AFAI®
Au service des professionnels
des systèmes d'information

COBIT®

4.1

Cadre de Référence

Objectifs de Contrôle

Guide de Management

Modèles de Maturité

IT GOVERNANCE INSTITUTE®

COBIT 4.1

L'IT Governance Institute
L'IT Governance Institute (ITGI, www.itgi.org) a été créé en 1998 pour faire progresser la réflexion et les standards internationaux qui se rapportent à la gestion et au contrôle des systèmes d'information (SI) dans les entreprises. Une gouvernance efficace des SI doit permettre de s'assurer que celles-ci vont dans le sens des objectifs de l'entreprise, qu'elles permettent d'optimiser les investissements informatiques et de gérer comme il convient les risques et les opportunités liés à leur existence. L'IT Governance Institute met à la disposition des dirigeants d'entreprises et des conseils d'administration des travaux de recherche originaux, des ressources en ligne et des études de cas pour les aider à faire face à leurs responsabilités dans le domaine de la gouvernance des SI.

Avertissement
L'IT Governance Institute (le « Propriétaire ») a conçu et rédigé ce document, intitulé COBIT ® V 4.1 (l' « Œuvre »), essentiellement comme une ressource pédagogique pour les directeurs de l'information, les directions générales, les professionnels de la gestion des SI et du contrôle. Le Propriétaire ne garantit pas que l'utilisation d'une partie quelconque de l'Œuvre produira de façon certaine un résultat positif. On ne doit pas considérer à priori que l'Œuvre contient toutes les informations, les procédures et les tests nécessaires, ni qu'elle exclut le recours à d'autres informations, procédures ou tests qui visent raisonnablement à produire des résultats semblables. Pour déterminer si une information, une procédure ou un test spécifique est approprié, les directeurs des systèmes d'information, les directions générales, les professionnels de la gestion des SI et du contrôle doivent appliquer leur propre jugement aux circonstances particulières qui se présentent dans leurs environnements informationnels et technologiques spécifiques.

.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 États-Unis
Tél :+1.847.590.7491
Fax :+1.847.253.1443
E-mail:info@itgi.org
Sites Internet : www.itgi.org
ISBN 1-933284-72-2

AFAI
Association Française de l'Audit et du Conseil Informatiques
171 bis, avenue Charles de Gaulle
92200 NEUILLY sur SEINE (France)
Tél. 33 (0)1 40 88 10 44
E-Mail : afai@afai.fr
Site Internet : www.afai.fr
ISBN 2-915007-09-8

Translated into French language from the English language version of COBIT ® *: Control Objectives for Information and related technology 4.1th Edition by AFAI the French Chapter of the Information Systems Audit and Control Association (ISACA) with the permission of the IT Governance Institute and the Information Systems Audit and Control Foundation. AFAI assumes sole responsibility for the accuracy and faithfulness of the translation.*

Traduction française de COBIT ® : Objectifs de contrôle de l'Information et des technologies associées Édition 4.1, réalisée par l'AFAI, chapitre français de l'Information Systems Audit and Control Association (ISACA), avec l'autorisation de l'IT Governance Institute et de la Information Systems Audit and Control Foundation. L'AFAI est seule responsable de l'exactitude et de la fidélité de la traduction.

REMERCIEMENTS

L'édition française de COBIT 4.1 est l'œuvre de la Commission COBIT de l'AFAI présidée par Jean-Louis BLEICHER, Administrateur de l'AFAI, Banque Fédérale des Banques Populaires.

Page volontairement laissée blanche

REMERCIEMENTS

L'IT Governance Institute tient à remercier :

Les experts, les réalisateurs et les réviseurs

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Ed Chavennes, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche LLP, South Africa
Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA
Philip Le Grand, Capita Education Services, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA

REMERCIEMENTS *(SUITE)*

Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., South Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Denmark
Jaco Sadie, Sasol, South Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgium
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

Le Conseil d'Administration de l'ITGI
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Trustee

Le Comité IT Governance
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Rómulo Lomparte, CISA, Banco de Crédito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

Le Comité de pilotage COBIT
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Rafael Eduardo Fabius, CISA, República AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

Les conseillers de l'ITGI
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

Les sponsors et membres affiliés de l'ITGI
ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
FIDA Inform
Information Security Forum
The Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Lte.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

TABLE DES MATIÈRES

SYNTHÈSE

SYNTHÈSE

Pour beaucoup d'entreprises, l'information et la technologie sur laquelle elle s'appuie constituent les actifs les plus précieux, même si elles sont souvent les moins bien perçues. Les entreprises qui réussissent connaissent les avantages des technologies de l'information et les utilisent pour apporter de la valeur à leurs parties prenantes. Ces entreprises comprennent et gèrent aussi les contraintes et les risques connexes, comme l'obligation de se soumettre à des règles de conformité de plus en plus contraignantes et la dépendance de plus en plus forte de nombreux processus métiers vis-à-vis des systèmes d'information (SI).

Le besoin de s'assurer de la valeur des SI, la gestion des risques qui leur sont liés et les exigences croissantes de contrôle sur l'information sont désormais reconnus comme des éléments clés de la gouvernance d'entreprise. Valeur, risque et contrôle constituent le cœur de la gouvernance des SI.

La gouvernance des SI est de la responsabilité des dirigeants et du conseil d'administration, et elle est constituée des structures et processus de commandement et de fonctionnement qui conduisent l'informatique de l'entreprise à soutenir les stratégies et les objectifs de l'entreprise, et à lui permettre de les élargir.

De plus, la gouvernance des SI intègre et institutionnalise les bonnes pratiques pour s'assurer qu'elles soutiennent la mise en œuvre des objectifs métiers. La gouvernance des SI permet à l'entreprise de tirer pleinement profit de ses données, maximisant ainsi ses bénéfices, capitalisant sur les opportunités qui se présentent et gagnant un avantage concurrentiel. Pour y parvenir, il convient d'utiliser un référentiel pour le contrôle des SI qui adopte les principes du Committee of Sponsoring Organisations of the Treadway Commission (COSO) *Internal Control-Integrated Framework*, référentiel de gouvernance d'entreprise et de gestion des risques largement reconnu, et d'autres référentiels semblables qui se conforment aux mêmes principes.

Les entreprises doivent satisfaire aux exigences fiduciaires ainsi qu'aux exigences de qualité et de sécurité, pour leur information comme pour tous leurs autres actifs. Les dirigeants doivent aussi optimiser l'utilisation des ressources informatiques disponibles : applications, données, infrastructures et personnels. Pour s'acquitter de ces responsabilités comme pour atteindre ces objectifs, ils doivent connaître la situation de leur architecture système et décider quelle gouvernance et quels contrôles informatiques ils doivent mettre en place.

Objectifs de Contrôle de l'Information et des technologies associées (Control Objectives for Information and related Technology, COBIT®) propose les bonnes pratiques dans un cadre de référence par domaine et par processus et présente les activités dans une structure logique facile à appréhender. Les bonnes pratiques de COBIT sont le fruit d'un consensus d'experts. Elles sont très axées sur le contrôle et moins sur l'exécution des processus. Elles ont pour but d'aider à optimiser les investissements informatiques, à assurer la fourniture des services et à fournir des outils de mesure (métriques) auxquels se référer pour évaluer les dysfonctionnements.

Pour que l'informatique réponde correctement aux attentes de l'entreprise, les dirigeants doivent mettre en place un système de contrôle ou un cadre de contrôle interne. Pour répondre à ce besoin, le cadre de référence de contrôle de COBIT :

- établit un lien avec les exigences métiers de l'entreprise,
- structure les activités informatiques selon un modèle de processus largement reconnu,
- identifie les principales ressources informatiques à mobiliser,
- définit les objectifs de contrôle à prendre en compte.

L'orientation métiers de COBIT consiste à lier les objectifs métiers aux objectifs informatiques, à fournir les métriques (ce qui doit être mesuré et comment) et les modèles de maturité pour faire apparaître leur degré de réussite et à identifier les responsabilités communes aux propriétaires de processus métiers et aux propriétaires de processus informatiques.

L'orientation processus de COBIT est illustrée par un modèle de processus qui subdivise la gestion des Systèmes d'Information en quatre domaines et 34 processus répartis entre les domaines de responsabilités que sont planifier, mettre en place, faire fonctionner et surveiller, donnant ainsi une vision complète de l'activité informatique. Les concepts d'architecture d'entreprise aident à identifier les ressources essentielles au bon déroulement des processus comme les applications, l'information, les infrastructures et les personnes.

En résumé, pour fournir les informations dont l'entreprise a besoin pour réaliser ses objectifs, les ressources informatiques doivent être gérées par un ensemble de processus regroupés selon une certaine logique.

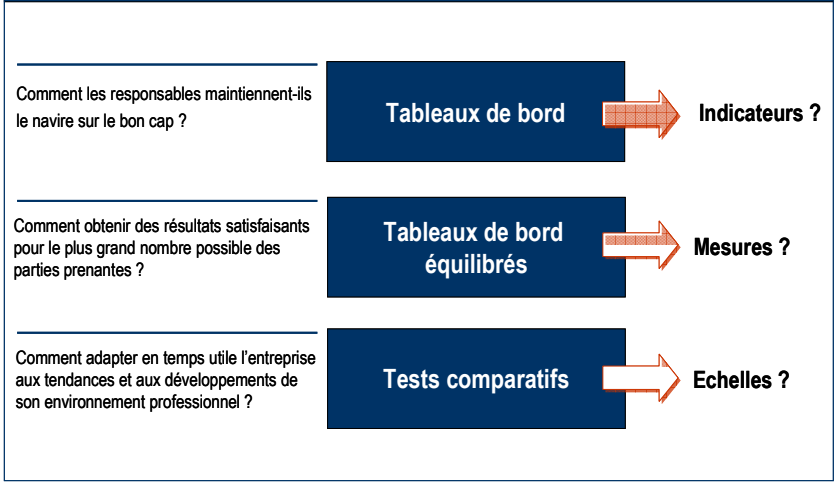
Mais comment contrôler les systèmes d'information pour qu'ils fournissent les données dont l'entreprise a besoin ? Comment gèrent-ils les risques liés aux ressources informatiques dont elles sont si dépendantes, et comment sécuriser celles-ci ? Comment l'entreprise peut-elle s'assurer que l'informatique atteint ses objectifs et concourt au succès des siens propres ?

Les dirigeants ont d'abord besoin d'objectifs de contrôle qui définissent les objectifs ultimes des politiques, des plans, des procédures et des structures organisationnelles de l'entreprise conçues pour fournir l'assurance raisonnable que :

- les objectifs de l'entreprise seront atteints,
- des dispositifs sont en place pour prévenir ou détecter et corriger les événements indésirables.

Ensuite, dans les environnements complexes d'aujourd'hui, le management est continuellement à la recherche d'informations condensées et disponibles en temps utile lui permettant de prendre rapidement des décisions difficiles en matière de valeur, de risque et de contrôle. Que doit-on mesurer, et comment ? Les entreprises ont besoin de pouvoir mesurer objectivement où elles en sont et où elles doivent apporter des améliorations, et elles ont besoin d'implémenter des outils de gestion pour surveiller ces améliorations. La **figure 1** montre certaines questions classiques et les outils de gestion de l'information utilisés pour trouver les réponses. Mais ces tableaux de bord nécessitent des indicateurs, les tableaux de bord équilibrés des mesures, et les tests comparatifs une échelle de comparaison.

Figure 1 Information du management



La réponse à ce besoin de déterminer et de surveiller les niveaux appropriés de contrôle et de performance de l'informatique est la définition donnée par COBIT des éléments suivants :

- **Tests comparatifs** de la capacité et des performances des processus informatiques présentés sous la forme de modèles de maturité inspirés du Capability Maturity Model (CMM) du Software Engineering Institute ;
- **Objectifs et métriques** des processus informatiques pour définir et mesurer leurs résultats et leurs performances, selon les principes du tableau de bord équilibré (Balanced Scorecard) de Robert Kaplan et David Norton ;
- **Objectifs des activités** pour mettre ces processus sous contrôle en se basant sur les objectifs de contrôle de COBIT.

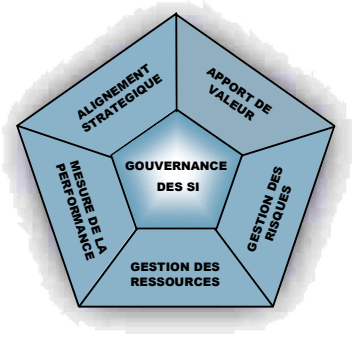
L'évaluation de la capacité des processus au moyen des modèles de maturité de COBIT est un élément clé de la mise en place d'une gouvernance des SI. Lorsqu'on a identifié les processus et les contrôles informatiques essentiels, le modèle de maturité permet de mettre en évidence les défauts de maturité et d'en faire la démonstration au management. On peut alors concevoir des plans d'action pour amener ces processus au niveau de maturité désiré.

COBIT concourt ainsi à la gouvernance des SI (**figure 2**) en fournissant un cadre de référence qui permet de s'assurer que :

- les SI sont alignés sur les métiers de l'entreprise,
- les SI apportent un plus aux métiers et maximisent ses résultats,
- les ressources des SI sont utilisées de façon responsable,
- les risques liés aux SI sont gérés comme il convient.

La mesure de la performance est essentielle à la gouvernance des SI. Elle est un élément de COBIT et consiste, entre autres, à fixer et à surveiller des objectifs mesurables pour ce que les processus informatiques sont censés fournir (résultat du processus) et pour la façon dont ils le fournissent (capacité et performance du processus). De nombreuses études ont montré que le manque de transparence des coûts, de la valeur et des risques des SI est l'une de motivations principales pour mettre en place une gouvernance des SI. Si d'autres domaines y contribuent, c'est essentiellement la mesure des performances qui permet la transparence.

Figure 2 Domaines de la Gouvernance des SI



- **L'Alignement Stratégique** consiste à s'assurer que les plans informatiques restent alignés sur les plans des métiers ; à définir, tenir à jour et valider les propositions de valeur ajoutée de l'informatique ; et à aligner le fonctionnement de l'informatique sur le fonctionnement de l'entreprise.
- **L'Apport de valeur** consiste à mettre en œuvre la proposition de valeur ajoutée tout au long du cycle de fourniture du service, à s'assurer que l'informatique apporte bien les bénéfices attendus sur le plan stratégique, à s'attacher à optimiser les coûts et à prouver la valeur intrinsèque des SI.
- **La Gestion des ressources** consiste à optimiser l'investissement dans les ressources informatiques vitales et à bien les gérer : applications, informations, infrastructures et personnes. Les questions clés concernent l'optimisation des connaissances et de l'infrastructure.
- **La Gestion des risques** exige une conscience des risques de la part des cadres supérieurs, une vision claire de l'appétence de l'entreprise pour le risque, une bonne connaissance des exigences de conformité, de la transparence à propos des risques significatifs encourus par l'entreprise, et l'attribution des responsabilités en matière de gestion des risques au sein de l'entreprise.
- **La Mesure de la performance** consiste en un suivi et une surveillance de la mise en œuvre de la stratégie, de l'aboutissement des projets, de l'utilisation des ressources, de la performance des processus et de la fourniture des services, en utilisant par exemple des tableaux de bord équilibrés qui traduisent la stratégie en actions orientées vers l'atteinte d'objectifs mesurables autrement que par la comptabilité conventionnelle.

Ces domaines de la gouvernance des SI présentent les questions que les dirigeants doivent examiner pour mettre en place cette gouvernance dans leur entreprise. La direction informatique utilise des processus pour organiser et gérer les activités informatiques au quotidien. COBIT propose un modèle de processus générique qui représente tous les processus que l'on trouve normalement dans les fonctions informatiques, ce qui permet aux responsables informatiques comme aux responsables métiers de disposer d'un modèle de référence commun. COBIT propose dans l'annexe II (Relations des processus informatiques avec les domaines de la gouvernance des SI, le COSO, les ressources informatiques de COBIT et les critères d'information COBIT) un tableau qui met en regard les processus informatiques et les domaines de gouvernance pour faire le lien entre les tâches des responsables informatiques et les objectifs de gouvernance de la direction générale.

Pour que cette gouvernance soit efficace, les dirigeants doivent exiger des directions informatiques qu'elles mettent en place des contrôles dans un cadre de référence défini pour tous les processus informatiques. Les objectifs de contrôle de COBIT sont organisés par processus informatique ; le cadre établit donc des liens clairs entre les exigences de la gouvernance des SI, les processus et les contrôles des SI.

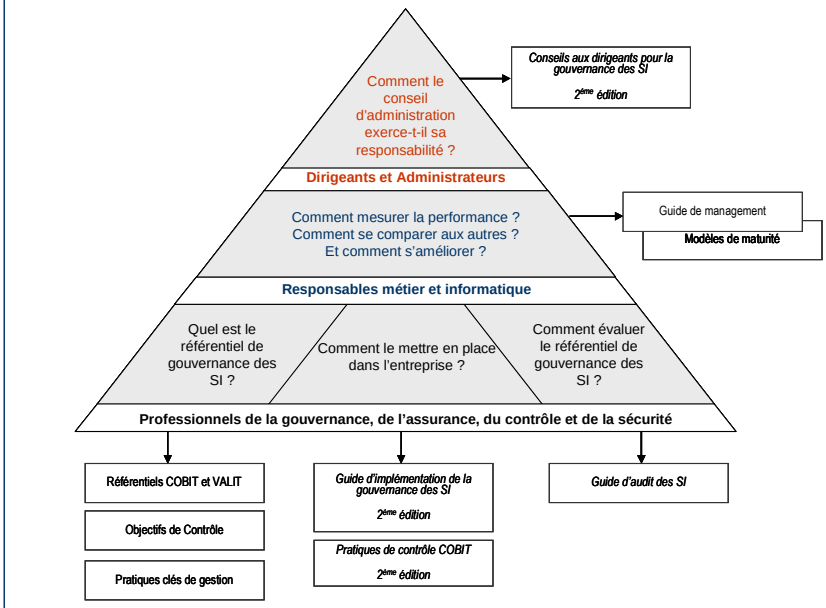
COBIT s'intéresse à ce qui est nécessaire pour une gestion et un contrôle adéquats des SI au niveau général. COBIT se conforme à d'autres standards informatiques plus détaillés et aux bonnes pratiques (voir annexe IV, Documents de référence de COBIT 4.1). COBIT agit comme intégrateur de ces différents guides en réunissant les objectifs clés dans un même cadre de référence général qui fait aussi le lien avec les exigences de gouvernance et les exigences opérationnelles.

COSO (comme d'autres référentiels compatibles semblables) est couramment accepté comme le cadre de référence du contrôle interne des entreprises. COBIT est la référence généralement acceptée du contrôle interne des SI.

Les produits COBIT s'organisent en trois niveaux (**figure 3**) conçus pour apporter leur aide :

- aux dirigeants et administrateurs,
- aux directions opérationnelles et informatiques,
- aux professionnels de la gouvernance, de l'assurance, du contrôle et de la sécurité.

Figure 3 Schéma du contenu de COBIT



Ce schéma de produit basé sur COBIT présente les produits généralement applicables et leur public principal. Il existe également des produits dérivés pour des fonctions particulières (*Objectifs de contrôle des SI pour Sarbanes-Oxley, 2ème édition*), dans des domaines comme la sécurité (*Bases de sécurité* COBIT et *Gouvernance de la sécurité de l'information : Recommandations destinées aux conseils d'administration et aux directions générales*) ou pour des entreprises spécifiques (COBIT *Quickstart* pour les petites et moyennes entreprises ou pour les grandes entreprises qui souhaitent accélérer la mise en œuvre d'un programme plus large de gouvernance des SI)

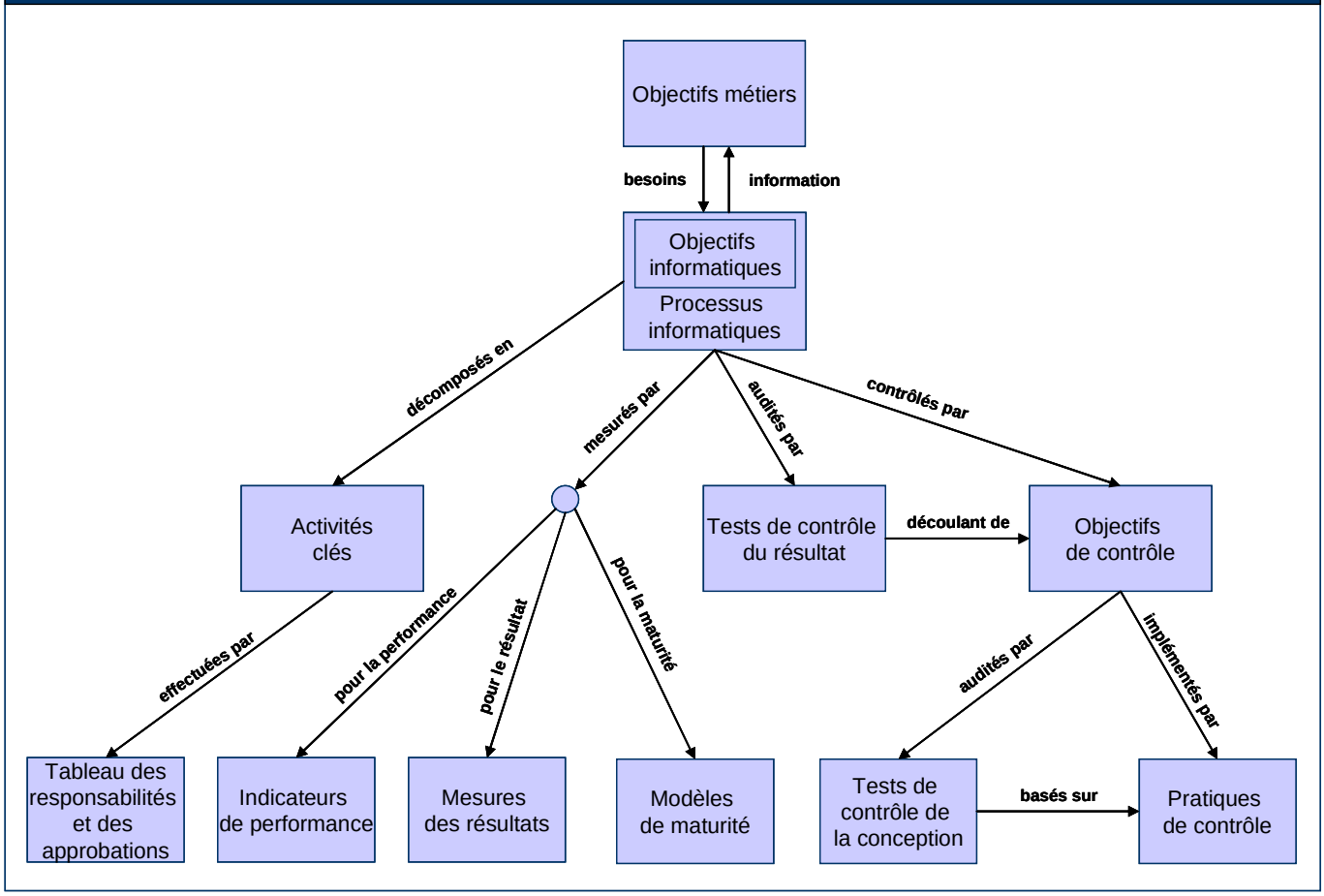
En quelques mots, les produits COBIT sont composés des éléments suivants :

- *Conseils aux dirigeants d'entreprises pour la gouvernance des SI, 2e édition* : ce document aide les dirigeants à comprendre l'importance de la gouvernance des SI, quels sont ses enjeux et quel est leur rôle dans sa mise en œuvre.
- Guide de management/modèles de maturité : ces outils permettent de répartir les responsabilités, de mesurer la performance, de tester la capacité et de trouver des réponses aux insuffisances dans ce domaine.
- Cadres de référence : ils permettent de structurer les objectifs de la gouvernance des SI et les bonnes pratiques, par domaine informatique et par processus, et de les relier aux exigences métiers.
- Objectifs de contrôle : ils fournissent un large éventail d'exigences élevées dont la direction doit tenir compte pour mettre en œuvre un contrôle efficace de chaque processus informatique.
- *Guide de mise en place de la gouvernance informatique : Utilisation de COBIT ® et Val IT™, 2ème Édition* : ce guide fournit une feuille de route générique pour mettre en place la gouvernance des SI en utilisant les ressources de COBIT et Val IT™.
- *Pratiques de contrôle COBIT® : Recommandations pour atteindre les objectifs de contrôle et réussir la gouvernance des SI, 2ème édition* : conseils sur l'importance des contrôles et sur la façon de les mettre en place.
- *Guide d'Audit de l'informatique : Utilisation de COBIT ®* : ce guide fournit des conseils sur la façon d'utiliser COBIT pour favoriser différentes types d'audit ainsi que des propositions de procédures d'évaluation pour tous les processus informatiques et les objectifs de contrôle.

Le schéma de contenu COBIT de la **figure 3** présente les principaux publics, leurs questions sur la gouvernance des SI et les produits qui permettent généralement d'y apporter des réponses. Il existe également des produits dérivés pour des fonctions particulières, dans des domaines comme la sécurité ou pour des entreprises spécifiques.

Tous ces composants COBIT sont reliés entre eux et visent à répondre aux besoins de gouvernance, de gestion, de contrôle et d'assurances de différents acteurs, comme le montre la **figure 4**.

Figure 4 Relations entre les composants de COBIT



COBIT est un cadre de référence et un ensemble d'outils permettant aux dirigeants de faire le lien entre les exigences du contrôle, les problématiques techniques et les risques métiers et de communiquer avec les parties prenantes sur ce niveau de contrôle. COBIT permet d'élaborer des politiques claires et des bonnes pratiques pour la maîtrise des SI dans toutes les entreprises. COBIT est en permanence tenu à jour et harmonisé avec les autres standards et recommandations. COBIT est ainsi devenu l'intégrateur des bonnes pratiques en technologies de l'information et le référentiel général de la gouvernance des SI qui aide à comprendre et à gérer les risques et les bénéfices qui leur sont associés. COBIT est organisé par processus et sa façon d'aborder l'entreprise par les métiers apporte une vision des SI qui couvre l'ensemble de leur champ d'application et des décisions à prendre pour ce qui les concerne.

L'adoption de COBIT comme cadre de gouvernance des SI offre les avantages suivants :

- un meilleur alignement de l'informatique sur l'activité de l'entreprise du fait de son orientation métiers ;
- une vision compréhensible par le management de ce que fait l'informatique ;
- une attribution claire de la propriété et des responsabilités, du fait de l'approche par processus ;
- un préjugé favorable de la part des tiers et des organismes de contrôle ;
- une compréhension partagée par toutes les parties prenantes grâce à un langage commun ;
- le respect des exigences du COSO pour le contrôle de l'environnement informatique.

Le reste de ce document propose une description du Cadre de Référence de COBIT et tous les composants essentiels de COBIT présentés par domaine (les 4 domaines informatiques) et par processus (les 34 processus informatiques) de COBIT. L'ensemble constitue un manuel de référence facile à consulter des principaux constituants de COBIT. Plusieurs annexes proposent également des références utiles.

Les informations les plus complètes et les plus récentes sur COBIT et les produits connexes (outils en ligne, guides de mise en œuvre, études de cas, lettres d'information, matériel pédagogique, etc.) sont disponibles sur *www.isaca.org/cobit*.

CADRE DE RÉFÉRENCE

CADRE DE RÉFÉRENCE COBIT

La mission de COBIT :

Elle consiste à imaginer, mettre au point, publier et promouvoir un cadre de référence de contrôle de la gouvernance des SI, actualisé, reconnu dans le monde entier et faisant autorité. Ce cadre de référence devra être adopté par les entreprises et utilisé quotidiennement par les dirigeants, les professionnels de l'informatique et les professionnels de l'assurance.

LE BESOIN D'UN CADRE DE RÉFÉRENCE POUR LA GOUVERNANCE DES SI

Le cadre de référence pour la gouvernance des SI définit les raisons pour lesquelles la gouvernance des SI est nécessaire, les différentes parties prenantes et sa mission.

Pourquoi

Les dirigeants ont de plus en plus conscience de l'impact significatif de l'information sur le succès de l'entreprise. Ils s'attendent à ce que l'on comprenne de mieux en mieux comment sont utilisées les technologies de l'information et la probabilité qu'elles contribuent avec succès à donner un avantage concurrentiel à l'entreprise. Ils veulent savoir en particulier si la gestion des SI peut leur permettre :

- d'atteindre leurs objectifs ;
- d'avoir assez de résilience pour apprendre et s'adapter ;
- de gérer judicieusement les risques auxquels ils doivent faire face ;
- de savoir bien identifier les opportunités et d'agir pour en tirer parti.

Les entreprises qui réussissent comprennent les risques, exploitent les avantages des SI et trouvent comment :

- aligner la stratégie de l'informatique sur celle de l'entreprise ;
- assurer aux investisseurs et aux actionnaires que l'entreprise respecte une "norme de prudence et de diligence" relative à la réduction des risques informatiques ;
- répercuter la stratégie et les objectifs de l'informatique dans l'entreprise ;
- faire en sorte que l'investissement informatique produise de la valeur ;
- apporter les structures qui faciliteront la mise en œuvre de cette stratégie et de ces objectifs ;
- susciter des relations constructives entre les métiers et l'informatique, et avec les partenaires externes ;
- mesurer la performance des SI.

Les entreprises ne peuvent pas répondre efficacement à ces exigences métiers et à celles de la gouvernance sans adopter et mettre en œuvre un cadre de référence pour la gouvernance et pour les contrôles qui permette aux directions des SI :

- d'établir un lien avec les exigences métiers de l'entreprise ;
- de rendre leurs performances transparentes par rapport à ces exigences ;
- d'organiser leurs activités selon un modèle de processus largement reconnu ;
- d'identifier les principales ressources informatiques à mobiliser ;
- de définir les objectifs de contrôle de management à envisager.

Par ailleurs les référentiels de gouvernance et de contrôle font désormais partie des bonnes pratiques de gestion des SI ; ils sont aussi un moyen de faciliter la mise en place de la gouvernance des SI et de se conformer aux exigences réglementaires toujours plus nombreuses.

Les bonnes pratiques informatiques ont gagné leurs galons grâce à un certain nombre de facteurs :

- l'exigence du meilleur retour sur investissements de leurs SI par les dirigeants et les administrateurs ; autrement dit, il convient de faire en sorte que l'informatique fournisse à l'entreprise ce dont elle a besoin pour apporter une valeur accrue aux parties prenantes ;
- la préoccupation de voir le niveau de dépenses informatiques augmenter assez systématiquement ;
- le besoin de répondre aux exigences réglementaires de contrôle des SI dans des domaines comme le respect de la vie privée et la publication des résultats financiers (par exemple la loi américaine Sarbanes-Oxley, Bâle II) et dans des secteurs spécifiques comme la finance, les produits pharmaceutiques et la santé ;
- la sélection de fournisseurs de services, la gestion de services externalisés et la gestion des achats ;
- la complexité croissante des risques informatiques comme la sécurité des réseaux ;
- les initiatives de la gouvernance des SI qui font une place aux référentiels de contrôle et aux bonnes pratiques pour aider à la surveillance et à l'amélioration des activités informatiques stratégiques, de façon à augmenter la valeur et réduire les risques pour l'entreprise ;
- le besoin d'optimiser les coûts en adoptant, chaque fois que c'est possible, des approches standardisées plutôt qu'individualisées ;
- une plus grande maturité caractérisée par l'adoption de référentiels réputés comme COBIT, ITIL (IT Infrastructure Library), la série ISO 27000 sur les normes liées à la sécurité de l'information, la norme ISO 9001:2000 *Systèmes de management de la qualité - Exigences*, le CMMI (Capability Maturity Model® Integration), PRINCE2 (Projects in Controlled Environments 2) et PMBOK (A *Guide to the Project Management Body of Knowledge*) ;
- le besoin qu'éprouvent les entreprises d'évaluer leurs performances par rapport aux normes communément acceptées et vis-à-vis de leurs pairs (analyse comparative - *benchmarking*).

Qui

Un référentiel de gouvernance et de contrôle sert les intérêts de diverses parties prenantes internes et externes dont chacune a des besoins spécifiques :

- Les parties prenantes internes à l'entreprise qui ont intérêt à voir les investissements informatiques générer de la valeur sont :
  - celles qui prennent les décisions d'investissements,
  - celles qui définissent les exigences,
  - celles qui utilisent les services informatiques.
- Les parties prenantes internes et externes qui fournissent les services informatiques sont :
  - celles qui gèrent l'organisation et les processus informatiques,
  - celles qui en développent les capacités,
  - celles qui exploitent les systèmes d'information au quotidien.
- Les parties prenantes internes et externes qui ont des responsabilités dans le contrôle et le risque sont :
  - celles qui sont en charge de la sécurité, du respect de la vie privée et/ou des risques,
  - celles qui sont en charge des questions de conformité,
  - celles qui fournissent des services d'assurance ou qui en ont besoin.

Quoi

Pour faire face à ces exigences, un cadre de référence pour la gouvernance et le contrôle des SI doivent respecter les spécifications générales suivantes :

- Fournir une vision métiers qui permette d'aligner les objectifs de l'informatique sur ceux de l'entreprise.
- Établir un schéma par processus qui définisse ce que chacun d'eux recouvre, avec une structure précise qui permette de s'y retrouver facilement.
- Faire en sorte que l'ensemble puisse être généralement accepté, en se conformant aux meilleures pratiques et aux standards informatiques, et en restant indépendant des technologies spécifiques.
- Fournir un langage commun, avec son glossaire, qui puisse être généralement compris par toutes les parties prenantes.
- Aider à remplir les obligations réglementaires en se conformant aux standards généralement acceptés de la gouvernance des entreprises (ex. COSO) et du contrôle informatique tels que les pratiquent les régulateurs et les auditeurs externes.

COMMENT COBIT RÉPOND À CES BESOINS

Le cadre de référence de COBIT répond à ces besoins par quatre caractéristiques principales : il est centré sur les métiers de l'entreprise, organisé par processus, basé sur des contrôles et s'appuie systématiquement sur des mesures.

Centré sur les métiers

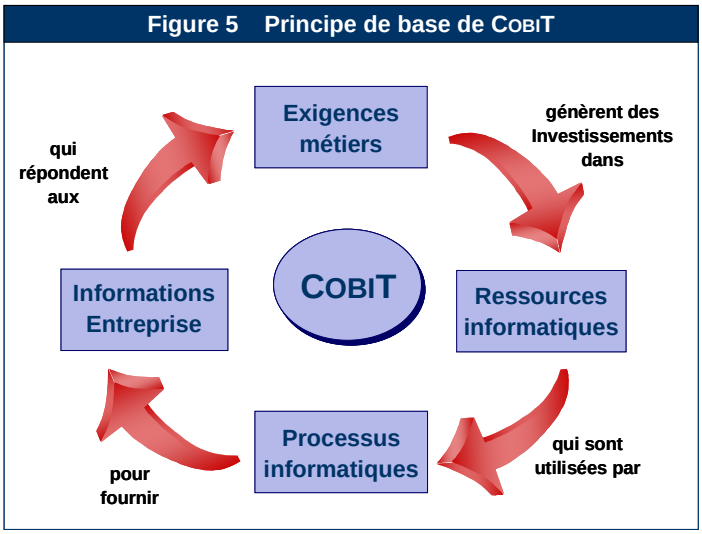
L'orientation métiers est l'idée centrale de COBIT. Il est conçu non seulement pour être employé par les fournisseurs de services informatiques, les utilisateurs et les auditeurs, mais également, ce qui est le plus important, comme un guide compréhensible par le management et par les propriétaires de processus métiers.

Le cadre de référence de COBIT se base sur le principe suivant **(figure 5)** :

> Pour fournir l'information dont elle a besoin pour atteindre ses objectifs, l'entreprise doit investir dans des ressources informatiques, les gérer et les contrôler, au moyen d'un ensemble de processus structuré pour fournir les services qui transmettent les données dont l'entreprise a besoin.

La gestion et le contrôle des informations sont au cœur du cadre de référence de COBIT et permettent de s'assurer que l'informatique est alignée sur les exigences métiers de l'entreprise.

Figure 5 Principe de base de COBIT



CRITÈRES D'INFORMATION DE COBIT

Pour satisfaire aux objectifs métiers l'entreprise, l'information doit se conformer à certains critères de contrôle que COBIT définit comme les exigences de l'entreprise en matière d'information. À partir des impératifs plus larges de qualité, fiduciaires et de sécurité, on définit sept critères d'information distincts dont certains se recoupent :

- **L'Efficacité** qualifie toute information pertinente utile aux processus métiers, livrée au moment opportun, sous une forme correcte, cohérente et utilisable.
- **L'Efficience** qualifie la mise à disposition de l'information grâce à l'utilisation optimale (la plus productive et la plus économique) des ressources.
- **La Confidentialité** concerne la protection de l'information sensible contre toute divulgation non autorisée.

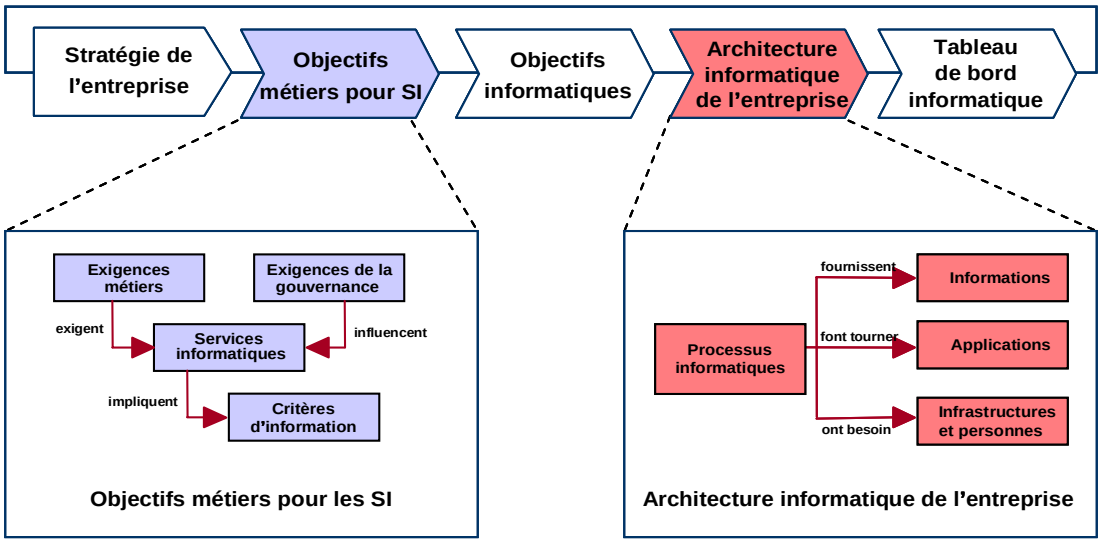
- **L'Intégrité** touche à l'exactitude et à l'exhaustivité de l'information ainsi qu'à sa validité au regard des valeurs de l'entreprise et de ses attentes.
- **La Disponibilité** qualifie l'information dont peut disposer un processus métier tant dans l'immédiat qu'à l'avenir. Elle concerne aussi la sauvegarde des ressources nécessaires et les moyens associés.
- **La Conformité** consiste à se conformer aux lois, aux réglementations et aux clauses contractuelles auxquelles le processus métier est soumis, c'est-à-dire aux critères professionnels imposés par l'extérieur comme par les politiques internes.
- **La Fiabilité** concerne la fourniture d'informations appropriées qui permettent au management de piloter l'entreprise et d'exercer ses responsabilités fiduciaires et de gouvernance.

OBJECTIFS MÉTIERS ET OBJECTIFS INFORMATIQUES

Si les critères d'information constituent un moyen générique de définir les exigences métiers, établir un ensemble générique d'objectifs métiers et informatiques constitue une base plus détaillée, liée à l'activité de l'entreprise, pour définir les exigences métiers et pour développer les métriques qui permettent de mesurer les résultats par rapport à ces objectifs. Chaque entreprise utilise l'informatique pour favoriser les initiatives métiers et celles-ci peuvent être considérées comme des objectifs métiers pour l'informatique. L'annexe I propose un tableau qui croise objectifs métiers, objectifs informatiques et critères d'information. On peut utiliser ces exemples génériques comme guide pour déterminer les exigences métiers, les objectifs et les métriques spécifiques à l'entreprise.

Si on veut que l'informatique réussisse à fournir les services qui favoriseront la stratégie de l'entreprise, le métier (le client) doit être clairement responsable de fixer ses exigences, et l'informatique (le fournisseur) doit avoir une bonne compréhension de ce qui doit être livré et comment. La **figure 6** illustre comment la stratégie de l'entreprise doit être traduite en objectifs liés aux initiatives qui s'appuient sur les SI (les objectifs métiers des SI). Ces objectifs doivent conduire à une définition claire des objectifs propres aux SI (les objectifs informatiques) qui, à leur tour, définissent les ressources et les capacités informatiques (l'architecture informatique de l'entreprise) requises pour le succès de la partie de la stratégie qui leur incombe[1].

Figure 6 Définir les objectifs informatiques et l architecture de l entreprise pour les SI



Une fois les objectifs alignés définis, il faut les surveiller pour s'assurer que ce qui est effectivement fourni correspond bien aux attentes. Cela est rendu possible par les métriques conçues à partir des objectifs et répercutées dans un tableau de bord informatique.

Pour que le client puisse comprendre les objectifs informatiques et le tableau de bord informatique, tous ces objectifs et les métriques connexes doivent être exprimés en termes métiers compréhensibles par le client. Et ceci, combiné à un alignement efficace de la hiérarchie des objectifs, permettra à l'entreprise de confirmer que ses objectifs seront probablement soutenus par les SI.

L'annexe I (Établissement de liens entre les objectifs et les processus) montre dans un tableau global comment les objectifs métiers génériques sont liés aux objectifs informatiques, aux processus informatiques et aux critères d'information. Ce tableau aide à comprendre quel est le champ d'action de COBIT et quelles sont les relations générales entre COBIT et les inducteurs de l'entreprise. Comme l'illustre la **figure 6**, ces inducteurs proviennent du métier et de la strate de gouvernance de l'entreprise, le premier étant plus axé sur la fonctionnalité et la vitesse de livraison tandis que la deuxième porte davantage sur la rentabilité, le retour sur investissement et la conformité.

[1] Remarque : La définition et la mise en œuvre d'une architecture informatique de l'entreprise entraîneront également la création d'objectifs informatiques internes qui contribuent aux objectifs métier (mais n'en découlent pas directement)

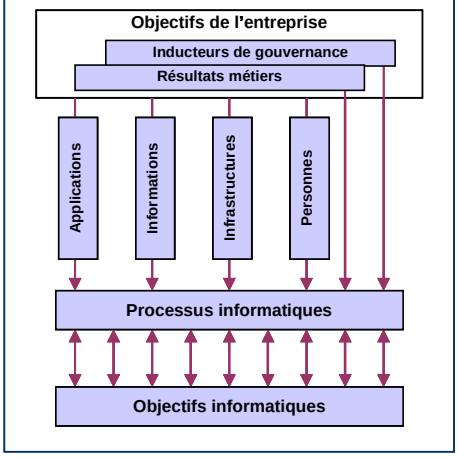
RESSOURCES INFORMATIQUES
L'informatique fournit ses services en fonction de ces objectifs au moyen d'un ensemble défini de processus qui utilisent les capacités des personnes et l'infrastructure informatique pour faire fonctionner des applications métiers automatisées tout en tirant parti des informations d'entreprise. Ces ressources constituent, avec les processus, une architecture d'entreprise pour les SI, comme le montre la **figure 6**.

Pour répondre aux exigences métiers des SI, l'entreprise doit investir dans les ressources nécessaires pour créer une capacité technologique appropriée (par exemple, un progiciel de gestion intégré (PGI- *ERP*)) capable d'assister un secteur opérationnel (par exemple, mettre en place une chaîne d'approvisionnement) qui produise le résultat désiré (par exemple, une augmentation des ventes et des bénéfices financiers).

On peut définir ainsi les ressources informatiques identifiées par COBIT :
- **Les applications** sont, entre les mains des utilisateurs, les ressources logicielles automatisées et les procédures manuelles qui traitent l'information.
- **L'information** est constituée des données sous toutes leurs formes, saisies, traitées et restituées par le système informatique sous diverses présentations, et utilisées par les métiers.
- **L'infrastructure** est constituée de la technologie et des équipements (machines, systèmes d'exploitation, systèmes de gestion de bases de données, réseaux, multimédia, ainsi que l'environnement qui les héberge et en permet le fonctionnement) qui permettent aux applications de traiter l'information.
- **Les personnes** sont les ressources qui s'occupent de planifier, d'organiser, d'acheter, de mettre en place, de livrer, d'assister, de surveiller et d'évaluer les systèmes et les services informatiques. Ces personnes peuvent être internes, externes ou contractuelles selon les besoins.

La **figure 7** montre schématiquement comment les objectifs métiers pour les SI influencent la gestion des ressources informatiques par les processus informatiques pour atteindre les objectifs informatiques.

Figure 7 Gérer les ressources informatiques pour remplir les objectifs informatiques



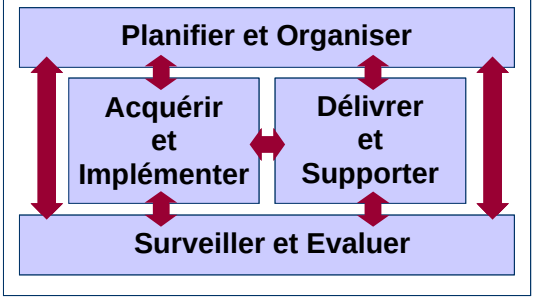
Orienté processus

COBIT regroupe les activités informatiques dans un modèle générique de processus qui se répartissent en quatre domaines. Ces domaines sont Planifier et Organiser, Acquérir et Implémenter, Délivrer et Supporter, Surveiller et Évaluer. Ils correspondent aux domaines de responsabilités traditionnels des SI, que sont planifier, mettre en place, faire fonctionner et surveiller.

Le cadre COBIT propose un modèle de processus de référence et un langage commun pour tous ceux qui, dans une entreprise, doivent utiliser ou gérer les activités informatiques. Adopter un modèle opérationnel et un langage commun à toutes les parties de l'entreprise impliquées dans les SI est l'une des étapes initiales les plus importantes vers une bonne gouvernance. COBIT propose aussi un cadre de référence pour mesurer et surveiller la performance des SI, communiquer avec les fournisseurs de services et intégrer les meilleures pratiques de gestion. Un modèle de processus encourage la propriété des processus, ce qui favorise la définition des responsabilités opérationnelles et des responsabilités finales (responsabilité de celui qui agit et responsabilité de celui qui est comptable du résultat).

Pour une gouvernance efficace des SI, il est important d'apprécier les activités et les risques propres aux SI qui nécessitent d'être pris en compte. Ils sont généralement ordonnés dans les domaines de responsabilité que sont planifier, mettre en place, faire fonctionner et surveiller. Dans le cadre de COBIT, ces domaines porte les appellations suivantes, comme le montre la **figure 8** :
- **Planifier et Organiser (PO)** : fournit des orientations pour la fourniture de solutions (AI) et la fourniture de services (DS).
- **Acquérir et Implémenter (AI)** : fournit les solutions et les transmets pour les transformer en services.
- **Délivrer et Supporter (DS)** : reçoit les solutions et les rend utilisables par les utilisateurs finals.
- **Surveiller et Evaluer (SE)** : surveille tous les processus pour s'assurer que l'orientation fournie est respectée.

Figure 8 Les quatre domaines interdépendants de COBIT



PLANIFIER ET ORGANISER (PO)
Ce domaine recouvre la stratégie et la tactique et vise à identifier la meilleure manière pour les SI de contribuer à atteindre les objectifs métiers de l'entreprise. La mise en œuvre de la vision stratégique doit être planifiée, communiquée et gérée selon différentes perspectives. Il faut mettre en place une organisation adéquate ainsi qu'une infrastructure technologique. Ce domaine s'intéresse généralement aux problématiques de management suivantes :
- Les stratégies de l'entreprise et de l'informatique sont-elles alignées ?
- L'entreprise fait-elle un usage optimum de ses ressources ?
- Est-ce que tout le monde dans l'entreprise comprend les objectifs de l'informatique ?
- Les risques informatiques sont-ils compris et gérés ?
- La qualité des systèmes informatiques est-elle adaptée aux besoins métiers ?

ACQUÉRIR ET IMPLÉMENTER (AI)
Le succès de la stratégie informatique nécessite d'identifier, de développer ou d'acquérir des solutions informatiques, de les mettre en œuvre et de les intégrer aux processus métiers. Ce domaine recouvre aussi la modification des systèmes existants ainsi que leur maintenance afin d'être sûr que les solutions continuent d'être en adéquation avec les objectifs métiers. Ce domaine s'intéresse généralement aux problématiques de management suivantes :
- Est-on sûr que les nouveaux projets vont fournir des solutions qui correspondent aux besoins métiers ?
- Est-on sûr que les nouveaux projets aboutiront en temps voulu et dans les limites budgétaires ?
- Les nouveaux systèmes fonctionneront-ils correctement lorsqu'ils seront mis en œuvre ?
- Les changements pourront-ils avoir lieu sans perturber les opérations en cours ?

DÉLIVRER ET SUPPORTER (DS)
Ce domaine s'intéresse à la livraison effective des services demandés, ce qui comprend l'exploitation informatique, la gestion de la sécurité et de la continuité, le service d'assistance aux utilisateurs et la gestion des données et des équipements. Il s'agit généralement des problématiques de management suivantes :
- Les services informatiques sont-ils fournis en tenant compte des priorités métiers ?
- Les coûts informatiques sont-ils optimisés ?
- Les employés sont-ils capables d'utiliser les systèmes informatiques de façon productive et sûre ?
- La confidentialité, l'intégrité et la disponibilité sont-elles mises en œuvre pour la sécurité de l'information ?

SURVEILLER ET ÉVALUER (SE)
Tous les processus informatiques doivent être régulièrement évalués pour vérifier leur qualité et leur conformité par rapport aux spécifications de contrôle. Ce domaine s'intéresse à la gestion de la performance, à la surveillance du contrôle interne, au respect des normes réglementaires et à la gouvernance. Il s'agit généralement des problématiques de management suivantes :
- La performance de l'informatique est-elle mesurée de façon à ce que les problèmes soient mis en évidence avant qu'il ne soit trop tard ?
- Le management s'assure-t-il que les contrôles internes sont efficaces et efficients ?
- La performance de l'informatique peut-elle être reliée aux objectifs métiers ?
- Des contrôles de confidentialité, d'intégrité et de disponibilité appropriés sont-ils mis en place pour la sécurité de l'information ?

À travers ces quatre domaines, COBIT a identifié 34 processus informatiques généralement utilisés (pour obtenir la liste complète, reportez-vous à la **figure 22**). La plupart des entreprises ont défini des responsabilités visant à planifier, mettre en place, faire fonctionner et surveiller les activités informatiques et la plupart disposent des mêmes processus clés. En revanche, peu d'entre elles auront la même structure de processus ou appliqueront la totalité des 34 processus COBIT. COBIT fournit la liste complète des processus qui peuvent permettre de vérifier l'exhaustivité des activités et des responsabilités. Toutefois, il n'est pas nécessaire de les appliquer tous et, en outre, ils peuvent être combinés selon les besoins de chaque entreprise.

Chacun de ces 34 processus est lié aux objectifs métiers et aux objectifs informatiques qui sont pris en charge. Des informations sont également fournies sur la façon dont les objectifs peuvent être mesurés, sur les activités clés et les principaux livrables et sur les personnes qui en sont responsables.

Basé sur des contrôles

COBIT définit les objectifs de contrôle pour les 34 processus, ainsi que des contrôles métiers et des contrôles applicatifs prédominants.

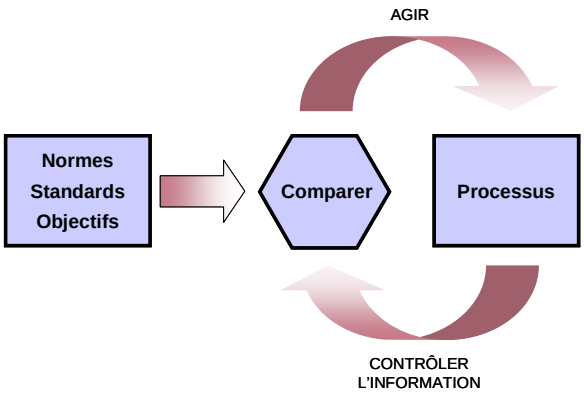
LES PROCESSUS ONT BESOIN DE CONTRÔLES
On définit le contrôle comme les politiques, les procédures, les pratiques et les structures organisationnelles conçues pour fournir l'assurance raisonnable que les objectifs métiers seront atteints et que les événements indésirables seront prévenus ou détectés et corrigés.

Les objectifs de contrôle des SI fournissent un large éventail d'exigences élevées dont la direction doit tenir compte pour mettre en œuvre un contrôle efficace de chaque processus informatique. Ces exigences :
- prennent la forme d'annonces de la direction visant à accroître la valeur ou à réduire le risque ;
- se composent de politiques, procédures, pratiques et structures organisationnelles ;
- sont conçues pour fournir l'assurance raisonnable que les objectifs métiers seront atteints et que les événements indésirables seront prévenus ou détectés et corrigés.

La direction de l'entreprise doit faire des choix concernant ces objectifs de contrôle, en :
- sélectionnant ceux qui sont applicables ;
- désignant ceux qui seront mis en œuvre ;
- choisissant la façon de les mettre en œuvre (fréquence, durée, automatisation, etc.) ;
- acceptant le risque de ne pas mettre en œuvre des objectifs qui pourraient s'appliquer.

On peut s'appuyer sur le modèle de contrôle standard illustré par la **figure 9**. Il suit les principes évidents de l'analogie suivante : Après réglage du thermostat d'ambiance (standard) du système de chauffage (processus), le système vérifie en permanence (comparer) la température de la pièce (information de contrôle) et déclenche éventuellement l'action d'adapter la température (agir).

Figure 9 Modèle de contrôle



La direction informatique utilise des processus pour organiser et gérer les activités informatiques au quotidien. COBIT propose un modèle de processus générique qui représente tous les processus que l'on trouve normalement dans les fonctions informatiques, ce qui permet aux responsables informatiques comme aux responsables commerciaux de disposer d'un modèle de référence commun. Pour que cette gouvernance soit efficace, la direction informatique doit mettre en place des contrôles dans un cadre de référence défini pour tous les processus informatiques. Puisque les objectifs de contrôle de COBIT sont organisés par processus informatique, le cadre établit donc des liens clairs entre les exigences de la gouvernance des SI, les processus informatiques et les contrôles informatiques.

Chacun des processus informatiques de COBIT est associé à une description et à un certain nombre d'objectifs de contrôle. Tous ensemble, ils sont caractéristiques d'un processus bien géré.

Les objectifs de contrôle sont identifiés par un domaine de référence à deux caractères (PO, AI, DS et SE), plus un numéro de processus et un numéro d'objectif de contrôle. En plus des objectifs de contrôle, chaque processus COBIT se réfère à des exigences de contrôle génériques désignées par PCn, pour Processus de Contrôle numéro n. Il faut les prendre en compte en même temps que les objectifs de contrôle du processus pour avoir une vision complète des exigences de contrôle.

PC1 Buts et objectifs du processus
Définir et communiquer des buts et objectifs spécifiques, mesurables, incitatifs, réalistes, axés sur les résultats et opportuns (SMARRT, Specific, Measurable, Actionable, Realistic, Results-oriented and Timely) pour l'exécution efficace de chaque processus informatique. S'assurer qu'ils sont reliés aux objectifs métiers et soutenus par des métriques adaptées.

PC2 Propriété des processus
Affecter un propriétaire à chaque processus informatique et définir clairement les rôles et les responsabilités du propriétaire du processus. Inclure, par exemple, la charge de conception du processus, d'interaction avec les autres processus, la responsabilité du résultat final, l'évaluation des performances du processus et l'identification des possibilités d'amélioration.

PC3 Reproductibilité du processus
Définir et mettre en place chaque processus informatique clé de façon à ce qu'il soit reproductible et qu'il produise invariablement les résultats escomptés. Fournir un enchaînement logique, flexible et évolutif d'activités qui conduiront aux résultats souhaités et suffisamment souple pour gérer les exceptions et les urgences. Si possible, utiliser des processus cohérents et personnaliser uniquement si c'est inévitable.

PC4 Rôles et Responsabilités
Définir les activités clés et les livrables finaux du processus. Attribuer et communiquer des rôles et responsabilités non ambigus, pour une exécution efficace et efficiente des activités clés et de leur documentation, ainsi que la responsabilité des livrables finaux du processus.

PC5 Politique, Plans et Procédures
Déterminer et indiquer comment tous les plans, les politiques et les procédures qui génèrent un processus informatique sont documentés, étudiés, gérés, validés, stockés, communiqués et utilisés pour la formation. Répartir les responsabilités pour chacune de ces activités et, au moment opportun, vérifier si elles sont correctement effectuées. S'assurer que les politiques, plans et procédures sont accessibles, corrects, compris et à jour.

PC6 Amélioration des performances du processus
Identifier un ensemble de métriques fournissant des indications sur les résultats et les performances du processus. Définir des cibles reflétant les objectifs du processus et des indicateurs de performance permettant d'atteindre les objectifs du processus. Définir le mode d'obtention des données. Comparer les mesures réelles et les objectifs et, si nécessaire, prendre des mesures pour corriger les écarts. Aligner les métriques, les objectifs et les méthodes avec l'approche globale de surveillance des performances des SI.

Des contrôles efficaces réduisent les risques, améliorent la probabilité de fournir de la valeur et améliorent l'efficience. En effet, les erreurs seront moins nombreuses et l'approche managériale sera plus cohérente.

COBIT y ajoute des exemples pour chaque processus ; ces exemples ont pour but d'illustrer, mais pas de prescrire ni d'être exhaustifs :
- entrées et sorties génériques de données/informations ;
- activités et conseils sur les rôles et les responsabilités dans un tableau RACI (Responsable, Approuve, est Consulté, est Informé) ;
- objectifs des activités clés (les choses les plus importantes à faire) ;
- métriques.

Outre la nécessité de savoir quels contrôles leur sont nécessaires, les propriétaires de processus doivent pouvoir dire de quels éléments ils ont besoin en entrée de la part des autres processus et ce que leurs processus doivent être capables de fournir aux autres processus. COBIT propose des exemples génériques d'entrées et de sorties essentiels pour chaque processus, qui concernent aussi les services informatiques externes. Certaines sorties sont des entrées pour tous les autres processus, et sont repérés par la mention TOUS dans les tableaux de sorties, mais ils ne sont pas mentionnés comme des entrées dans tous les processus ; cela concerne généralement les standards de qualité et les impératifs de mesure, le cadre de référence des processus informatiques, les rôles et responsabilités détaillés, le cadre de contrôle de l'informatique de l'entreprise, la politique informatique et les rôles et responsabilités du personnel.

Comprendre les rôles et responsabilités pour chaque processus est fondamental pour une gouvernance efficace. COBIT propose un tableau RACI pour chaque processus. Garant s'applique au responsable en dernier ressort : celui qui donne les orientations et qui autorise une activité. Responsable s'applique à celui qui fait exécuter la tâche. Les deux autres rôles (Consulté et Informé) s'appliquent à tous ceux qui doivent savoir ce qui se passe et qui doivent soutenir le processus.

CONTRÔLES MÉTIERS ET CONTRÔLES INFORMATIQUES

Le système de contrôle interne de l'entreprise a un impact sur les SI à trois niveaux :

- Au niveau de la direction générale, on fixe les objectifs métiers, on établit les politiques et on prend les décisions sur la façon de déployer les ressources de l'entreprise pour mettre en œuvre sa stratégie. C'est le conseil d'administration qui définit l'approche de gouvernance et de contrôle et qui les diffuse dans l'ensemble de l'entreprise. Ce sont ces ensembles de politiques et d'objectifs généraux qui orientent l'environnement de contrôle des SI.
- Au niveau des processus métiers, les contrôles s'appliquent à des activités spécifiques de l'entreprise. La plupart des processus métiers sont automatisés et intégrés à des applications informatiques, ce qui entraîne que de nombreux contrôles sont eux aussi automatisés à ce niveau. On les appelle des contrôles applicatifs. Certains contrôles de processus métiers restent cependant des procédures manuelles comme les autorisations de transactions, la séparation des tâches et les rapprochements manuels. Les contrôles au niveau des processus métiers sont donc une combinaison de contrôles manuels effectués par l'entreprise et de contrôles métiers et applicatifs automatisés. La responsabilité de ces deux types de contrôles appartient donc aux métiers, même si les contrôles applicatifs ont besoin de la fonction informatique pour permettre leur conception et leur développement.
- Pour assister les processus métiers, l'informatique fournit des services, habituellement au sein d'un service commun à de nombreux processus métiers, puisqu'une grande partie du développement et des processus informatiques sont fournis à l'ensemble de l'entreprise, et que la majeure partie de l'infrastructure informatique constitue un service commun (par ex. réseaux, bases de données, systèmes d'exploitation et archivage). On appelle "contrôles généraux informatiques" les contrôles qui s'appliquent à toutes les activités de services informatiques. La fiabilité de ces contrôles généraux est nécessaire pour que l'on puisse se fier aux contrôles applicatifs. Par exemple, une mauvaise gestion des changements pourrait mettre en péril (accidentellement ou volontairement) la fiabilité des vérifications d'intégrité automatiques.

CONTRÔLES GÉNÉRAUX INFORMATIQUES ET CONTRÔLES APPLICATIFS

Les contrôles généraux sont ceux qui sont intégrés aux processus et aux services informatiques. Ils concernent, par exemple :

- le développement des systèmes,
- la gestion des changements,
- la sécurité,
- l'exploitation.

On appelle communément "contrôles applicatifs" les contrôles intégrés aux applications des processus métiers. Ils concernent, par exemple :

- l'exhaustivité,
- l'exactitude,
- la validité,
- l'autorisation,
- la séparation des tâches.

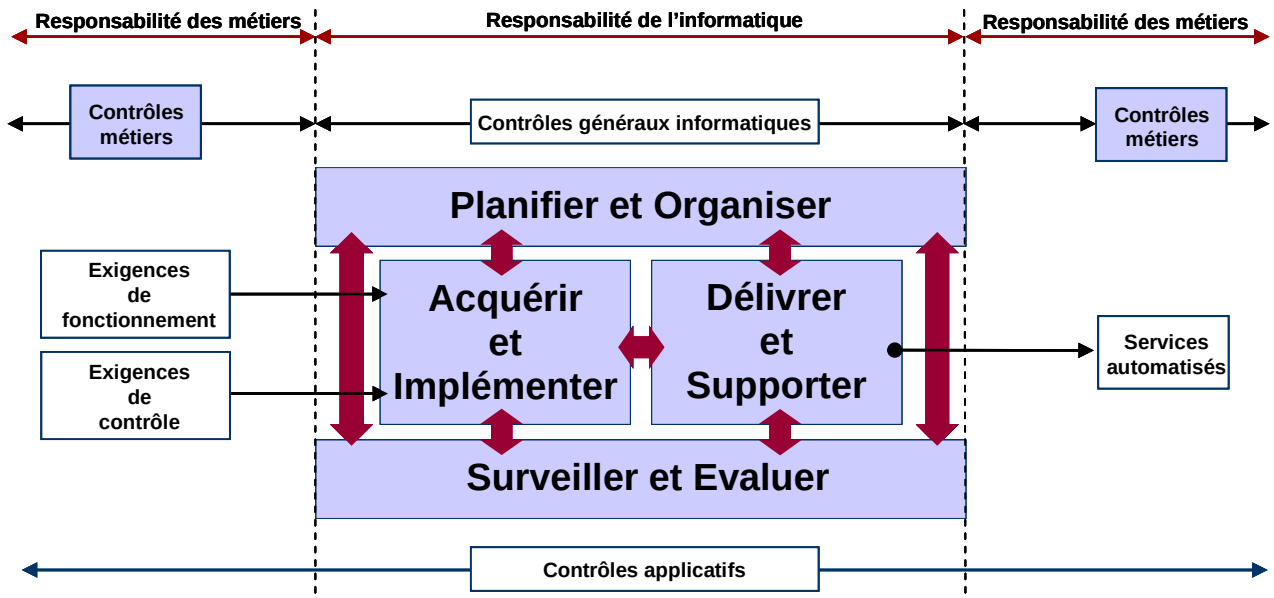
COBIT considère que la conception et la mise en place de contrôles applicatifs automatisés sont de la responsabilité de l'informatique. Elles relèvent du domaine Acquérir et Implémenter et se basent sur les exigences métiers définies selon les critères d'information de COBIT, comme l'indique la **figure 10**. La gestion opérationnelle et la responsabilité des contrôles applicatifs ne relèvent pas de l'informatique mais des propriétaires des processus métiers.

De ce fait, les contrôles applicatifs relèvent d'une responsabilité commune de bout en bout entre métiers et informatique, mais la nature des responsabilités se différencie comme suit :

- La partie métiers est chargée :
  - de définir correctement les exigences de fonctionnement et de contrôle ;
  - d'utiliser les services automatisés à bon escient.
- La partie informatique est chargée :
  - d'automatiser et de mettre en œuvre les exigences métiers de fonctionnement et de contrôle,
  - de mettre en place des contrôles pour maintenir l'intégrité des contrôles applicatifs.

Par conséquent, les processus informatiques de COBIT englobent les contrôles généraux informatiques, mais uniquement les aspects liés au développement des contrôles applicatifs. Les processus métiers sont chargés de la définition et de l'exploitation.

Figure 10 Contrôles métiers, généraux et applicatifs : limites



La liste suivante fournit un ensemble d'objectifs de contrôle applicatifs recommandés. Ils sont identifiés par un numéro CAn pour "Contrôle Applicatif numéro n".

CA1 Autorisation et préparation des données source
S'assurer que les documents source sont préparés par le personnel qualifié et autorisé, en respectant les procédures établies, en tenant compte de la séparation adéquate des tâches entre la génération/création et la validation de ces documents. La bonne conception des masques de saisie permet de réduire les erreurs et omissions. Détecter les erreurs et les anomalies de façon à pouvoir les signaler et les corriger.

CA2 Collecte et saisie des données source
Prévoir que la saisie des données sera effectuée en temps utile, par le personnel autorisé et qualifié. La correction et la ressaisie des données erronées doivent être effectuées sans compromettre le niveau d'origine d'autorisation des transactions. Si la reconstruction des données le requiert, conserver les documents source d'origine pendant un laps de temps adéquat.

CA3 Vérifications d'exactitude, d'exhaustivité et d'authenticité
S'assurer que les transactions sont exactes, complètes et valides. Valider les données saisies et modifier ou renvoyer pour correction aussi près que possible du point de création.

CA4 Intégrité et validité du traitement
Maintenir l'intégrité et la validité des données tout au long du cycle de traitement. La détection des transactions erronées n'interrompt pas le traitement des transactions valides.

CA5 Vérification des sorties, rapprochement et traitement des erreurs
Établir des procédures et les responsabilités connexes pour s'assurer que le traitement des données en sortie est dûment effectué, que ces données sont transmises au destinataire approprié et protégées lors de leur transmission ; que la vérification, la détection et la correction de l'exactitude des données en sortie a lieu et que les informations fournies dans ces données sont utilisées.

CA6 Authentification et intégrité des transactions
Avant d'échanger des données de transaction entre les applications internes et les fonctions métiers/fonctions opérationnelles (dans l'entreprise ou en dehors), vérifier l'exactitude des destinataires, l'authenticité de l'original et l'intégrité du contenu. Maintenir l'authenticité et l'intégrité lors de la transmission ou du transport.

Fondé sur la mesure

Toute entreprise a un besoin vital d'appréhender l'état de ses propres systèmes informatiques et de décider quel niveau de management et de contrôle elle doit assurer. Pour déterminer le bon niveau, le management doit se demander : jusqu'où doit-on aller et les bénéfices justifient-ils les coûts ?

Obtenir une vue objective du niveau de performance d'une entreprise n'est pas chose aisée. Que doit-on mesurer et comment ? Les entreprises ont besoin de pouvoir mesurer où elles en sont et où il faut apporter des améliorations, et il leur faut des outils de gestion pour surveiller ces améliorations. COBIT traite ces questions en fournissant :

- des modèles de maturité pour permettre de se comparer et de définir l'amélioration nécessaire des capacités ;
- des objectifs de performances et des métriques pour les processus informatiques, qui montrent jusqu'à quel point les processus permettent d'atteindre les objectifs métiers et les objectifs informatiques ; ils servent à mesurer la performance des processus internes selon les principes du tableau de bord équilibré ;
- des objectifs d'activité pour favoriser une performance efficace des processus.

MODÈLES DE MATURITÉ

On demande de plus en plus aux directions générales des entreprises publiques et privées de s'interroger sur la bonne gestion de leur informatique. Pour répondre à cette attente, des analyses d'optimisation de rentabilité concluent à la nécessité d'améliorer cette gestion et d'atteindre le niveau approprié de gestion et de contrôle de l'infrastructure informatique. Comme peu d'entre elles oseraient dire que ce n'est pas une bonne chose, elles doivent analyser l'équilibre coûts/bénéfices et se poser les questions suivantes :

- Que font nos confrères/concurrents et comment sommes-nous positionnés par rapport à eux ?
- Quelles sont les bonnes pratiques acceptables du marché et comment nous situons-nous par rapport à elles ?
- D'après ces comparaisons, peut-on dire que nous en faisons assez ?
- Comment identifie-t-on ce qu'il y a à faire pour atteindre un niveau approprié de gestion et de contrôle de nos processus informatiques ?

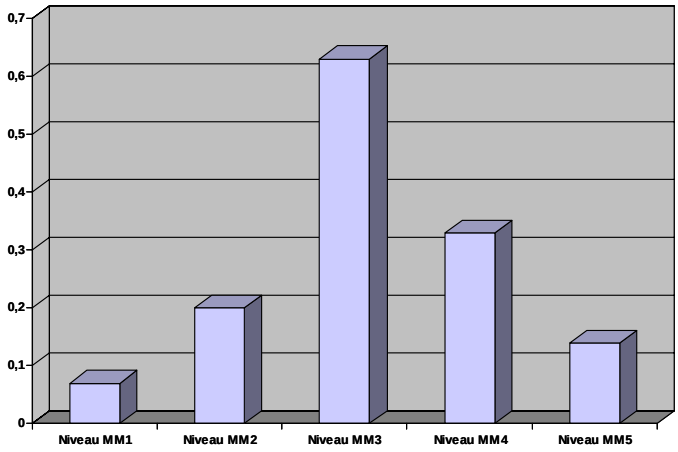
Il peut être difficile d'apporter des réponses directes à ces questions. La direction informatique est sans cesse à la recherche d'outils d'autoévaluation et de tests comparatifs pour répondre à la nécessité d'identifier les actions efficaces à entreprendre et la façon de les mener efficacement. À partir des processus COBIT, le propriétaire d'un processus doit être en mesure de se comparer sur une échelle vis-à-vis de cet objectif de contrôle. Ceci répond à trois besoins :

1. une mesure relative de la situation actuelle de l'entreprise ;
2. une manière efficace de désigner le but à atteindre ;
3. un outil permettant de mesurer la progression vers l'objectif.

L'utilisation des modèles de maturité pour la gestion et le contrôle des processus informatiques se base sur une méthode d'évaluation permettant de noter une entreprise selon un niveau de maturité gradué de 0 à 5 (d'Inexistant à Optimisé). Cette approche est basée sur le Modèle de Maturité que le Software Engineering Institute (SEI) a conçu pour mesurer la capacité à développer des logiciels. Même si les concepts de la méthode du SEI ont été respectés, la mise en œuvre de COBIT présente des différences importantes par rapport à la démarche initiale du SEI, qui était axée sur les principes d'ingénierie logicielle, les entreprises s'efforçant d'atteindre un niveau d'excellence dans ces domaines et l'évaluation officielle des niveaux de maturité de façon à pouvoir "certifier" les développeurs de logiciels. COBIT fournit une définition générique de l'échelle de maturité COBIT, qui est similaire au CMM mais interprétée en tenant compte des processus de gestion informatique de COBIT. Un modèle spécifique est fourni à partir de cette échelle générique, pour chacun des 34 processus COBIT. Quel que soit le modèle, les échelles ne doivent pas être trop fines au risque de rendre le système difficile à utiliser en requérant une précision inutile. En effet, le but est généralement de trouver où se situent les problèmes et comment établir des priorités pour les résoudre. Le but n'est pas d'évaluer le niveau d'adhésion aux objectifs de contrôle.

Les niveaux de maturité sont conçus comme des profils de processus informatiques que l'entreprise peut reconnaître comme des situations existantes ou futures. Ils ne sont pas conçus pour être utilisés comme des modèles par seuils qui exigeraient que toutes les conditions du niveau inférieur soient remplies pour accéder au niveau suivant. Avec les modèles de maturité COBIT, contrairement à la démarche CMM initiale du SEI, l'intention n'est pas de mesurer précisément les niveaux ni d'essayer de certifier qu'un niveau a été précisément atteint. Une évaluation de maturité COBIT est susceptible de générer un profil dans lequel les conditions relatives à plusieurs niveaux de maturité seront remplies, comme le montre le graphique de la **figure 11**.

Figure 11 Niveau de maturité possible d un processus informatique



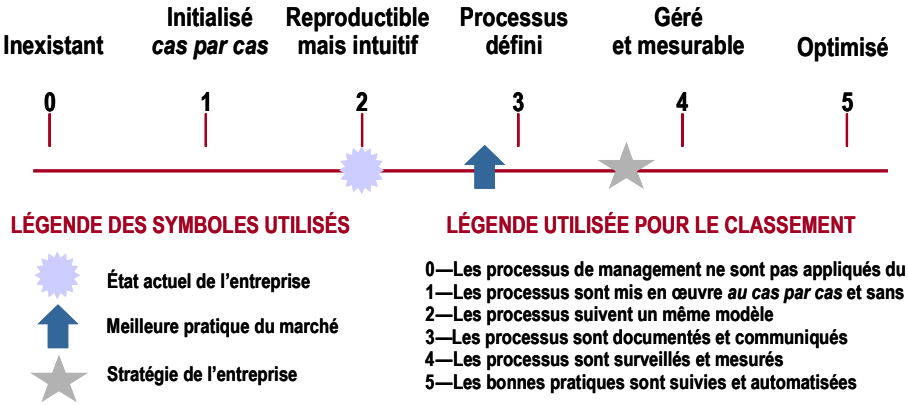
Niveau de maturité possible d'un processus informatique : l'exemple illustre un processus qui atteint largement le niveau 3 mais qui présente encore des problèmes de conformité avec les exigences des niveaux les moins élevés, tout en investissant déjà dans la mesure de la performance (niveau 4) et l'optimisation (niveau 5).

En effet, en cas d'évaluation de la maturité à l'aide des modèles COBIT, il arrive souvent qu'une mise en œuvre soit en place à différents niveaux même si elle est incomplète ou insuffisante. Ces atouts peuvent être mis à profit pour améliorer encore davantage la maturité. Par exemple, certains éléments du processus peuvent être bien définis et, même s'il est incomplet, il serait trompeur de dire que le processus n'est pas du tout défini.

En utilisant les modèles de maturité définis pour chacun des 34 processus informatiques de COBIT, le management peut mettre en évidence :
- l'état actuel de l'entreprise : où elle se situe aujourd'hui ;
- l'état actuel du marché : la comparaison ;
- l'ambition de l'entreprise : où elle veut se situer ;
- la trajectoire de croissance requise entre les situations en cours et les situations cibles.

Pour exploiter facilement ces résultats dans les réunions de direction où ils seront présentés comme une aide à la décision pour des plans futurs, il convient d'utiliser une méthode de présentation graphique **(figure 12)**.

Figure 12 Représentation graphique des modèles de maturité



L'élaboration de cette représentation graphique s'inspire du modèle de maturité générique présenté dans la **figure 13**.

COBIT est un cadre de référence conçu pour la gestion des processus informatiques et très axé sur le contrôle. Ces échelles doivent être commodes à utiliser et faciles à comprendre. La question de la gestion des processus informatiques est complexe par nature et subjective ; on l'approche par conséquent mieux en favorisant une prise de conscience au moyen d'outils d'évaluation faciles à utiliser qui entraîneront un large consensus et une motivation pour progresser. Ces évaluations peuvent se faire soit par comparaison avec les intitulés généraux des niveaux de maturité, soit de façon plus rigoureuse en examinant chaque proposition individuelle de ces descriptifs. Dans les deux cas, il est nécessaire d'utiliser l'expertise de l'entreprise pour le processus évalué.

L'avantage d'une approche basée sur les modèles de maturité est qu'elle permet assez facilement au management de se situer lui-même sur l'échelle et d'apprécier les moyens à mettre en œuvre pour améliorer les performances. L'échelle commence par le degré zéro parce qu'il est très possible qu'il n'existe aucun processus. Elle est basée sur une échelle de maturité simple, qui montre comment évolue un processus, d'inexistant (0) à optimisé (5).

Cependant, la capacité à gérer les processus est différente de la performance des processus. La capacité requise, déterminée par les métiers et les objectifs informatiques, n'a pas toujours besoin d'être appliquée au même niveau dans tout l'environnement informatique, c'est-à-dire pas systématiquement, ou seulement à un nombre limité de systèmes ou d'unités. La mesure de performance, expliquée dans les paragraphes qui suivent, est essentielle pour déterminer la véritable performance de l'entreprise pour ses processus informatiques.

Figure 13 Modèle de Maturité Générique

0 Inexistant : Absence totale de processus identifiables. L'entreprise n'a même pas pris conscience qu'il s'agissait d'un problème à étudier.

1 Initialisé/Cas par cas : On constate que l'entreprise a pris conscience de l'existence du problème et de la nécessité de l'étudier. Il n'existe toutefois aucun processus standardisé, mais des démarches dans ce sens tendent à être entreprises individuellement ou cas par cas. L'approche globale du management n'est pas organisée.

2 Reproductible mais intuitif : Des processus se sont développés jusqu'au stade où des personnes différentes exécutant la même tâche utilisent des procédures similaires. Il n'y a pas de formation organisée ni de communication des procédures standard et la responsabilité et laissée à l'individu. On se repose beaucoup sur les connaissances individuelles, d'où un risque d'erreurs.

3 Processus défini : On a standardisé, documenté et communiqué des processus *via* des séances de formation. Ces processus doivent impérativement être suivis ; toutefois, des écarts seront probablement constatés. Concernant les procédures elles-mêmes, elles ne sont pas sophistiquées mais formalisent des pratiques existantes.

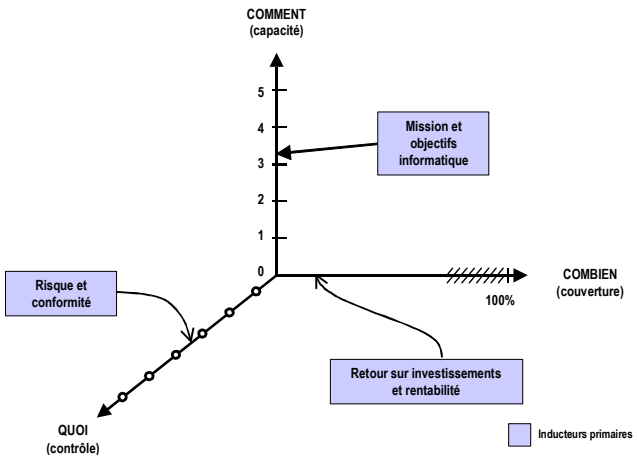
4 Géré et mesurable : La direction contrôle et mesure la conformité aux procédures et agit lorsque certains processus semblent ne pas fonctionner correctement. Les processus sont en constante amélioration et correspondent à une bonne pratique. L'automatisation et les outils sont utilisés d'une manière limitée ou partielle.

5 Optimisé : Les processus ont atteint le niveau des bonnes pratiques, suite à une amélioration constante et à la comparaison avec d'autres entreprises (Modèles de Maturité). L'informatique est utilisée comme moyen intégré d'automatiser le flux des tâches, offrant des outils qui permettent d'améliorer la qualité et l'efficacité et de rendre l'entreprise rapidement adaptable.

Même si une capacité correctement mise en œuvre réduit déjà les risques, une entreprise a tout de même besoin d'analyser les contrôles nécessaires pour être sûre que les risques sont limités et que la valeur est obtenue en tenant compte de l'appétence pour le risque et des objectifs métiers. Le choix de ces contrôles est facilité par les objectifs de contrôle de COBIT. L'annexe III propose un modèle de maturité qui illustre la maturité d'une entreprise en ce qui concerne la mise en place et la performance du contrôle interne. Cette analyse constitue souvent une réponse à des facteurs externes, mais idéalement elle devrait être instituée et documentée par les processus COBIT PO6 *Faire connaître les buts et les orientations du management* et SE2 *Surveiller et évaluer le contrôle interne.*

Capacité, couverture et contrôle sont les trois dimensions de la maturité d'un processus, comme le montre la **figure 14**.

Figure 14 Les trois dimensions de la maturité



Le modèle de maturité est un moyen de mesurer le niveau de développement des processus de management, autrement dit leur capacité réelle. Leur niveau de développement ou de capacité dépend essentiellement des objectifs informatiques et des besoins métiers sous-jacents qu'ils sont supposés satisfaire. La capacité réellement déployée dépend largement du retour qu'une entreprise attend de ses investissements. Par exemple, il y a des processus et des systèmes stratégiques qui nécessitent une gestion de la sécurité plus importante et plus stricte que d'autres qui sont moins essentiels. D'autre part, le degré et la sophistication des contrôles à appliquer à un processus sont davantage induits par l'appétence pour le risque de l'entreprise et par les impératifs de conformité applicables.

Les échelles des modèles de maturité aideront les professionnels à expliquer aux dirigeants où se situent les points faibles de la gestion des processus informatiques et à désigner le niveau que ceux-ci doivent atteindre. Le bon niveau de maturité dépendra des objectifs métiers de l'entreprise, de l'environnement opérationnel et des pratiques du secteur. En particulier, le niveau de maturité de la gestion dépendra de la dépendance de l'entreprise vis-à-vis de l'informatique, du niveau de sophistication de ses technologies et, avant tout, de la valeur de ses informations.

Une entreprise désireuse d'améliorer la gestion et le contrôle de ses processus informatiques peut trouver des références stratégiques en s'intéressant aux standards internationaux émergents et aux meilleures pratiques. Les pratiques émergentes actuelles peuvent devenir le niveau de performance attendu de demain et, par conséquent, être utiles pour planifier les objectifs de positionnement d'une entreprise dans le temps.

Les modèles de maturité sont créés à partir du modèle qualitatif général (voir **figure 13**) auquel on ajoute progressivement, de niveau en niveau, des principes issus des attributs suivants :
- sensibilisation et communication,
- politiques, plans et procédures,
- outils et automatisation,
- compétences et expertise,
- responsabilité opérationnelle et responsabilité finale,
- désignation des objectifs et métriques.

Le tableau des attributs de maturité de la **figure 15** répertorie les caractéristiques de la façon dont les processus informatiques sont gérés et montre comment ils évoluent d'inexistant à optimisé. On peut utiliser ces attributs pour une évaluation plus complète, pour l'analyse des écarts et pour la planification des améliorations.

En résumé, les modèles de maturité proposent un profil générique des étapes au travers desquelles évoluent les entreprises dans la gestion et le contrôle des processus informatiques. Ils constituent :
- un ensemble d'exigences et les facteurs d'application aux différents niveaux de maturité ;
- une échelle qui permet de mesurer facilement les écarts ;
- une échelle qui se prête à des comparaisons pragmatiques ;
- la base pour positionner les situations en cours et les situations cibles ;
- une aide pour déterminer, par l'analyse des écarts, les actions à entreprendre pour atteindre le niveau choisi ;
- pris tous ensemble, une vision de la façon dont l'informatique est gérée dans l'entreprise.

Les modèles de maturité COBIT se focalisent sur la maturité, mais pas nécessairement sur la couverture et l'ampleur du contrôle. Ils ne constituent pas un record à égaler, ni une base pour se préparer à une certification par petites étapes avec des seuils difficiles à franchir. Ils sont conçus pour être toujours applicables, avec des niveaux qui décrivent ce qu'une entreprise peut identifier comme le mieux adapté à ses processus. Le juste niveau est déterminé par le type d'entreprise, l'environnement et la stratégie.

La couverture, l'ampleur du contrôle et la façon dont la capacité est utilisée et déployée constituent des décisions coût/bénéfice. Par exemple, la gestion de la sécurité à un échelon élevé peut n'avoir à se focaliser que sur les systèmes de l'entreprise les plus sensibles. Un autre exemple serait le choix entre un examen manuel hebdomadaire et un contrôle automatisé permanent.

Finalement, même si de plus hauts niveaux de maturité augmentent le contrôle des processus, l'entreprise a toujours besoin d'analyser, en fonction des inducteurs de risque et de valeur, quels mécanismes de contrôle elle doit mettre en œuvre. Les objectifs métiers et les objectifs informatiques génériques définis dans ce cadre de référence aideront à faire cette analyse. Les mécanismes de contrôle sont guidés par les objectifs de contrôle de COBIT et s'intéressent en priorité aux actions entreprises au cours du processus ; les modèles de maturité se focalisent d'abord sur l'appréciation de la qualité de gestion d'un processus. L'annexe III propose un modèle de maturité générique qui montre la situation de l'environnement de contrôle interne et l'établissement de contrôles internes dans une entreprise.

On peut considérer qu'un environnement de contrôle est bien adapté lorsqu'on a traité les trois aspects de la maturité : capacité, couverture et contrôle. Améliorer la maturité réduit les risques et améliore l'efficience, ce qui induit moins d'erreurs, des processus plus prévisibles et une utilisation rentable des ressources.

MESURE DE LA PERFORMANCE

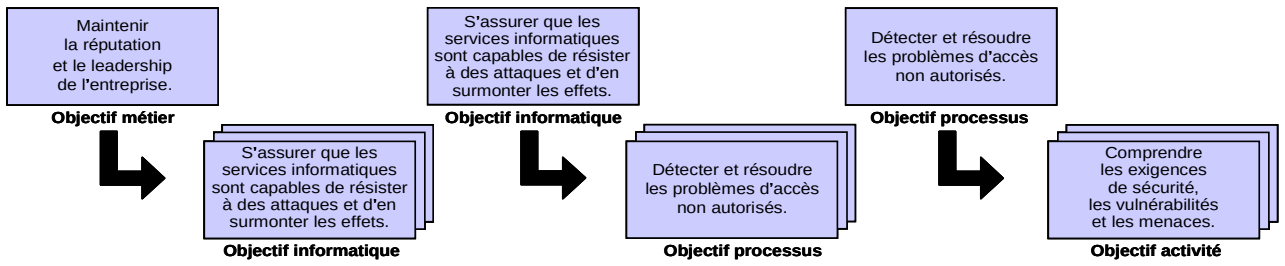
Les objectifs et les métriques sont définis à trois niveaux dans COBIT :
- les objectifs et les métriques informatiques, qui définissent les attentes de l'entreprise vis-à-vis de l'informatique et comment les mesurer ;
- les objectifs et les métriques des processus, qui définissent ce que le processus informatique doit fournir pour répondre aux objectifs informatiques et comment mesurer ces exigences ;
- les objectifs et les métriques de l'activité, qui déterminent les actions à entreprendre au sein du processus pour atteindre la performance requise et comment les mesurer.

Figure 15 Tableau des attributs de maturité

	Sensibilisation et communication	Politiques, plans et procédures	Outils et automatisation	Compétences et expertise	Responsabilité opérationnelle et responsabilité finale	Définition des objectifs et métriques
1	On commence à reconnaître la nécessité des processus. On communique de temps en temps sur ces questions.	L'approche par processus et les pratiques sont envisagées au cas par cas. Les processus et les politiques ne sont pas définis.	Il peut exister certains outils ; la pratique se base sur les outils de bureautique standards. Il n'y a pas d'approche planifiée de l'utilisation des outils.	On n'a pas identifié quelles compétences étaient nécessaires au fonctionnement du processus. Il n'existe pas de plan de formation et aucune formation n'est officiellement organisée.	Les responsabilités opérationnelles et les responsabilités finales ne sont pas définies. Les gens s'attribuent la propriété des problèmes à résoudre de leur propre initiative en fonction des situations.	Les objectifs ne sont pas clairs et rien n'est mesuré.
2	On a conscience du besoin d'agir. Le management communique sur les questions générales.	On commence à utiliser des processus semblables mais ils sont largement intuitifs car basés sur l'expertise individuelle. Certains aspects des processus sont reproductibles grâce à l'expertise individuelle, et il peut exister une forme de documentation et de compréhension informelle de la politique et des procédures.	Il existe des approches communes de certains outils, mais elles sont basées sur des solutions développées par des individus clés. Des outils ont pu être achetés chez des fournisseurs, mais ils ne sont sans doute pas utilisés correctement, et sont peut-être même des produits imparfaitement adaptés.	On a identifié les compétences minimales requises pour les domaines stratégiques. On fournit une formation en cas de besoin plutôt que selon un plan approuvé, et certaines formations informelles ont lieu "sur le tas".	Une personne assume ses responsabilités et en est habituellement tenue pour responsable (garante), même si cela n'a pas été formellement convenu. Lorsque des problèmes surviennent, on ne sait plus qui est responsable et une culture du blâme a tendance à s'installer.	On fixe certains objectifs ; on mesure certains flux financiers mais seul le management est au courant. On surveille certains secteurs isolés mais pas de façon organisée.
3	On a compris le besoin d'agir. Le management communique de façon plus formelle et plus rigoureuse.	On commence à utiliser les bonnes pratiques. On a défini et documenté les processus, les politiques et les procédures pour toutes les activités clés.	On a défini un plan d'utilisation et de standardisation des outils pour automatiser les processus. Les outils sont utilisés pour leurs fonctions de base, mais ne correspondent peut-être pas tous au plan adopté, et ne sont peut-être pas capables de fonctionner les uns avec les autres.	On a défini et documenté les besoins en compétences pour tous les secteurs. On a élaboré un plan de formation officiel, mais la formation reste basée sur des initiatives individuelles.	Les responsabilités opérationnelles et finales sont définies et les propriétaires de processus sont identifiés. Le propriétaire de processus n'a vraisemblablement pas toute autorité pour exercer ses responsabilités.	On fixe certains objectifs d'efficacité et on mesure cette efficacité, mais on ne communique pas dessus ; ces objectifs sont clairement reliés aux objectifs métiers. Des processus de mesures commencent à être utilisés, mais pas de façon systématique. On adopte les idées du tableau de bord équilibré informatique et on utilise parfois l'analyse causale de manière intuitive
4	On a pleinement compris les impératifs. On utilise des techniques abouties et des outils standards pour communiquer.	Les processus sont sains et complets ; on applique les meilleures pratiques internes. Tous les aspects des processus sont documentés et reproductibles. Les politiques ont été approuvées et avalisées par le management. On a adopté des standards pour le développement et la gestion des processus et des procédures et on les applique.	Les outils sont mis en place selon un plan standardisé et certains fonctionnent avec d'autres outils dans le même environnement. On utilise certains outils dans les domaines principaux pour automatiser la gestion des processus et pour surveiller les activités et les contrôles critiques.	Les besoins en compétences sont régulièrement réajustés pour tous les secteurs ; on apporte des compétences spécialisées à tous les secteurs critiques et on encourage la certification. On applique des techniques de formation éprouvées conformes au plan de formation et on encourage le partage des connaissances. On implique tous les experts des domaines internes et on évalue l'efficacité du plan de formation.	Les responsabilités opérationnelles et finales des processus sont acceptées et fonctionnent d'une façon qui permet au propriétaire de processus de s'acquitter pleinement de ses responsabilités. Il existe une culture de la récompense qui motive un engagement positif dans l'action.	On mesure l'efficacité et l'efficience, on communique sur ces questions qu'on lie aux objectifs métiers et au plan informatique stratégique. On met en œuvre le tableau de bord équilibré informatique dans certains secteurs sauf dans certains cas connus du management, et on est en train de standardiser l'analyse causale. L'amélioration continue commence à exister.
5	On comprend tout à fait les impératifs et on anticipe sur les évolutions. Il existe une communication proactive sur les tendances du moment, on applique des techniques éprouvées et des outils intégrés pour la communication.	On applique les meilleures pratiques et standards externes. La documentation des processus a évolué en workflow automatisé. On a standardisé et intégré les processus, les politiques et les procédures pour permettre une gestion et des améliorations de tous les maillons de la chaîne.	On utilise des progiciels standardisés dans l'ensemble de l'entreprise. Les outils sont pleinement intégrés entre eux pour supporter le processus de bout en bout. On utilise des outils pour favoriser l'amélioration des processus et pour détecter automatiquement les cas d'exception au contrôle.	L'entreprise encourage formellement l'amélioration continue des compétences, selon des objectifs personnels et d'entreprise clairement définis. La formation et l'enseignement s'appuient sur les meilleures pratiques externes et utilisent des concepts et des techniques de pointe. Le partage des connaissances est une culture d'entreprise et on déploie des systèmes à base de connaissances. On s'appuie sur l'expérience d'experts externes et d'entreprises leaders de la branche.	Les propriétaires de processus ont le pouvoir de prendre des décisions et d'agir. Le fait d'accepter des responsabilités a été déployé de façon cohérente à tous les échelons de l'entreprise.	Il existe un système de mesure de la performance intégré qui lie la performance de l'informatique aux objectifs métiers par l'application générale du tableau de bord équilibré informatique. Le management prend systématiquement note des exceptions et on applique l'analyse causale. L'amélioration continue fait désormais partie de la culture d'entreprise.

Les objectifs sont définis dans le sens descendant en ce sens que les objectifs métiers détermineront un certain nombre d'objectifs informatiques pour favoriser leur réalisation. Un objectif informatique est atteint par un processus ou par l'interaction de différents processus. Par conséquent, les objectifs informatiques aident à définir les différents objectifs de processus. D'autre part, chaque objectif de processus requiert un certain nombre d'activités, établissant ainsi les objectifs de l'activité. La **figure 16** fournit des exemples de liens entre les objectifs métiers, informatiques, des processus et de l'activité.

Figure 16 Exemple de relation entre les objectifs

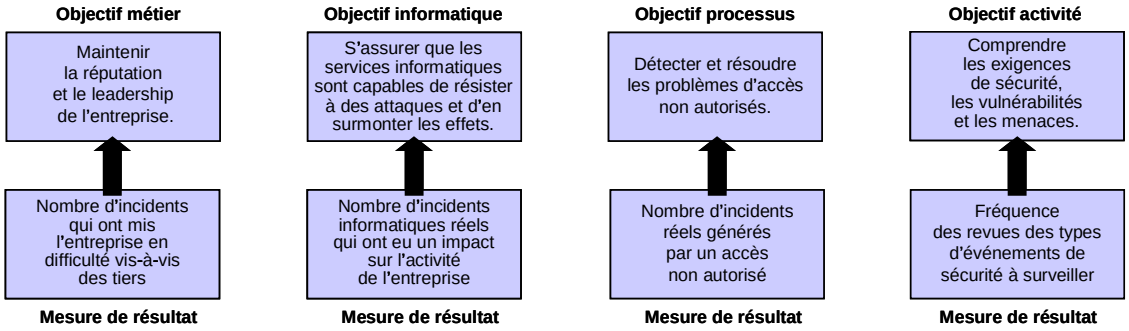


Les termes ICO (indicateurs clés d'objectif) et ICP (indicateurs clés de performance), utilisés dans les précédentes versions de COBIT, ont été remplacés par deux types de métriques :

- Les mesures de résultats (anciens ICO) indiquent si les objectifs ont été atteints. Elles ne peuvent être mesurées qu'après le résultat et sont correspondent donc à des "indicateurs a posteriori".
- Les indicateurs de performance (anciens ICP) indiquent si les objectifs ont des chances d'être atteints. Ils peuvent être mesurés avant la manifestation du résultat et correspondent donc à des "indicateurs a priori".

La **figure 17** fournit des mesures de résultats ou d'objectifs possibles pour l'exemple utilisé.

Figure 17 Mesures de résultats possibles pour l exemple de la figure 16



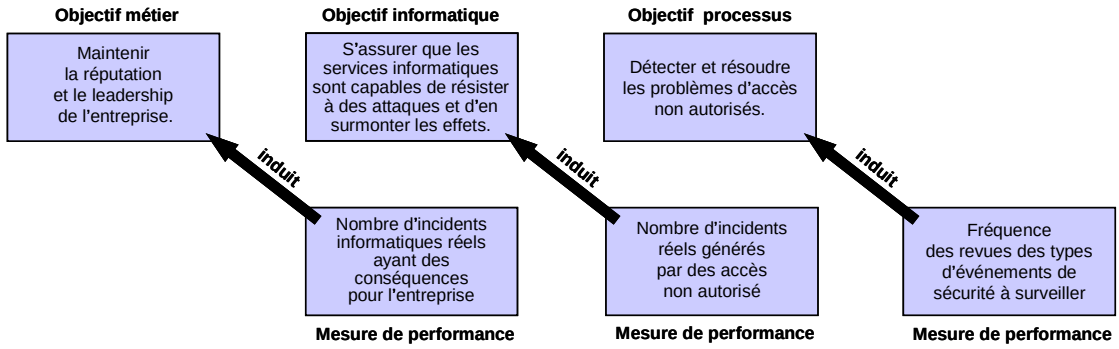
Les mesures de résultats du niveau inférieur deviennent les indicateurs de performance du niveau supérieur. Comme l'illustre l'exemple de la **figure 16**, une mesure de résultat indiquant que la détection et la résolution d'un accès non autorisé sont en bonne voie révèle également que les services informatiques seront très probablement capables de résister aux attaques. Ainsi, la mesure de résultat est devenue un indicateur de performance pour l'objectif de niveau supérieur. La **figure 18** montre comment les mesures de résultats deviennent des mesures de performance dans l'exemple employé.

Les mesures de résultats définissent des indicateurs qui, après les faits, révèlent à la direction si une activité, un processus ou une fonction informatique a atteint ses objectifs. Les mesures de résultats des fonctions informatiques sont souvent exprimées en termes de critères d'information :

- Disponibilité des informations requises pour répondre aux besoins métiers de l'entreprise
- Absence de risques vis-à-vis de l'intégrité et la confidentialité
- Rentabilité des processus et des opérations
- Confirmation de la fiabilité, de l'efficacité et de la conformité

Les indicateurs de performance définissent les mesures qui déterminent à quel point la performance de l'activité, de la fonction informatique ou du processus informatique lui donne des chances d'atteindre les objectifs. Ce sont des indicateurs essentiels pour savoir si un objectif a des chances d'être atteint ou non, conditionnant ainsi les objectifs du niveau supérieur. Ils mesurent généralement la disponibilité des capacités, des pratiques et des compétences appropriées et le résultat des activités sous-jacentes. Par exemple, un service fourni par les SI est un objectif pour les SI mais un indicateur de performance et une compétence pour l'entreprise. C'est la raison pour laquelle les indicateurs de performance sont parfois désignés sous le nom d'inducteurs de performance, notamment dans les tableaux de bord équilibrés.

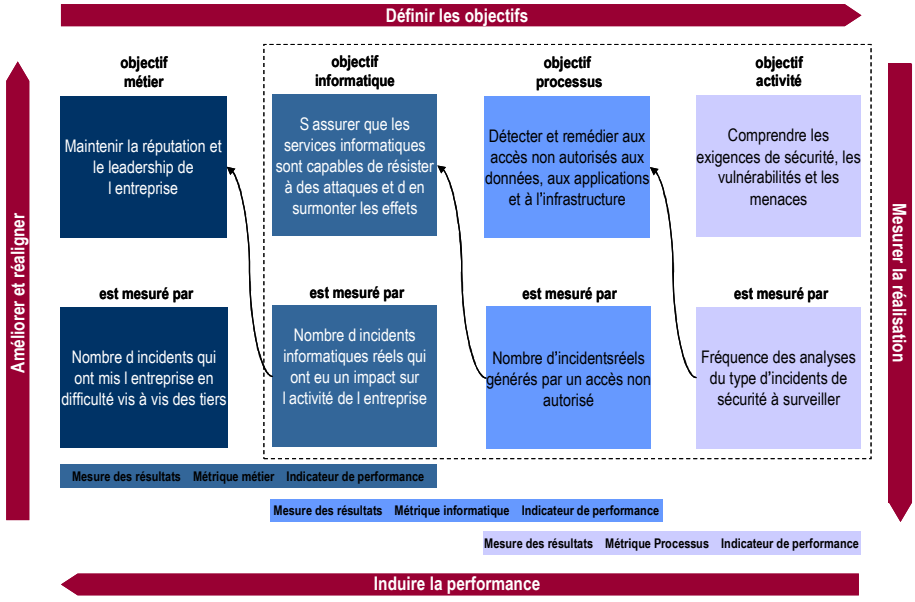
Figure 18 Inducteurs de performance possibles pour l'exemple de la figure 16



Par conséquent, les métriques fournies constituent une mesure des résultats de la fonction informatique, du processus informatique ou de l'objectif d'activité qu'elles évaluent, ainsi qu'un indicateur de performance induisant l'objectif de niveau supérieur en matière de fonction informatique, de processus informatique ou d'activité.

La **figure 19** illustre les relations entre les objectifs métiers, informatiques, des processus et de l'activité, et les différentes métriques. La déclinaison des objectifs est illustrée d'en haut à gauche à en haut à droite. Sous chaque objectif apparaît la mesure de résultat de l'objectif. La petite flèche indique que la même métrique est un indicateur de performance pour l'objectif de niveau supérieur.

Figure 19 Relations entre processus, objectifs et métriques (DS5)

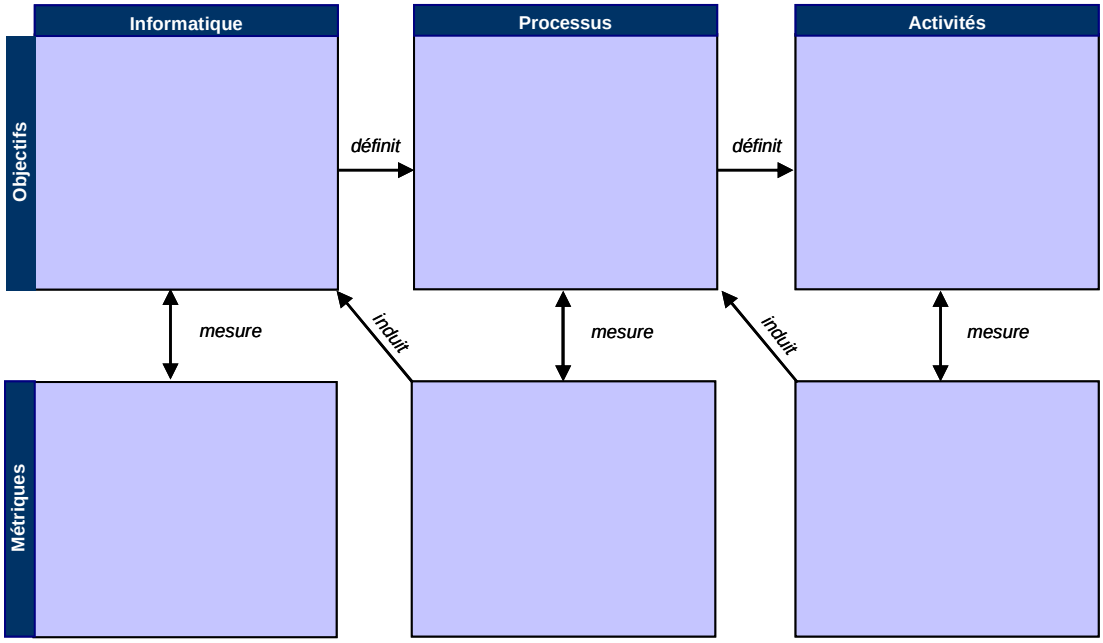


L'exemple fourni est tiré de DS5 *Assurer la sécurité des systèmes*. COBIT fournit uniquement des métriques jusqu'au résultat des objectifs informatiques, comme l'indique la délimitation en pointillés. Même s'il s'agit également d'indicateurs de performance pour les objectifs métiers des SI, COBIT ne fournit pas de mesures de résultat des objectifs métiers.

Les objectifs métiers et les objectifs informatiques utilisés dans la section des objectifs et métriques de COBIT, ainsi que les relations entre eux, sont fournis en Annexe I.
Pour chaque processus informatique de COBIT, les objectifs et les métriques sont présentés, comme l'illustre la **figure 20.**

Les métriques ont été mises au point en tenant compte des caractéristiques suivantes :
- un ratio perspicacité/effort élevé (c.-à-d. vision de la performance et du succès des objectifs par rapport à l'effort pour les atteindre) ;
- comparables en interne (par ex. pourcentage par rapport à une base ou à des chiffres dans le temps) ;
- comparables en externe quels que soient la taille ou le secteur d'activité ;
- quelques bonnes métriques (éventuellement même une seule très bonne sur laquelle agissent plusieurs paramètres) sont préférables à une longue liste de mauvaises métriques ;
- des mesures faciles à effectuer qui ne doivent pas être confondues avec les cibles à atteindre.

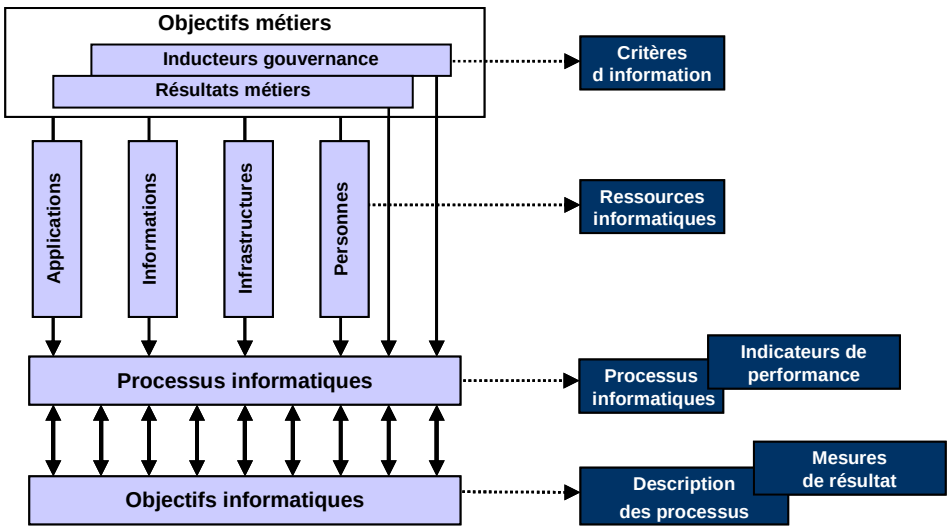
Figure 20 – Présentation des objectifs et des métriques



Le modèle du cadre de référence COBIT

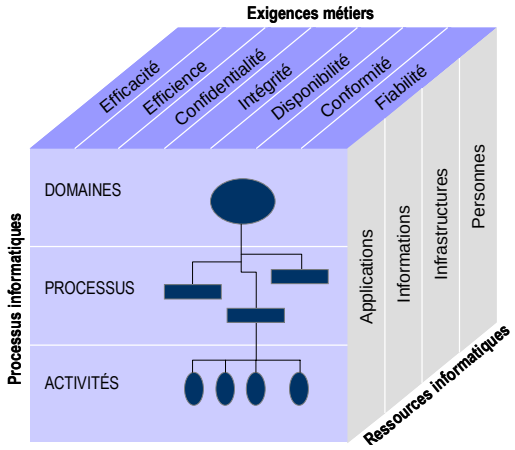
Le cadre de référence COBIT, par conséquent, lie les exigences d'information et de gouvernance métiers aux objectifs de l'informatique. Le modèle de processus COBIT permet aux activités informatiques et aux ressources qu'elles utilisent d'être correctement gérées et contrôlées sur la base des objectifs de contrôle de COBIT, et d'être alignées et surveillées en utilisant les objectifs et métriques de COBIT, comme l'illustre la **figure 21**.

Figure 21 – COBIT Gestion, Contrôle, Alignement et Surveillance



En résumé, les ressources informatiques sont gérées par des processus informatiques pour atteindre les objectifs informatiques qui répondent aux exigences métiers. C'est le principe de base du cadre de référence COBIT, comme l'illustre le cube COBIT **(figure 22)**.

Figure 22 Le cube COBIT



On peut représenter plus en détail le cadre de référence général de COBIT par le graphique de la **figure 23**, le modèle COBIT étant divisé en 4 domaines et en 34 processus génériques qui gèrent les ressources informatiques pour fournir l'information à l'entreprise en fonction des exigences métiers et de celles de la gouvernance.

Pourquoi COBIT est largement reconnu

COBIT se base sur l'analyse et l'harmonisation des standards informatiques existants comme sur les bonnes pratiques, et se conforme aux principes de gouvernance généralement acceptés. Il considère les exigences métiers au niveau le plus général et couvre l'ensemble des activités informatiques en se concentrant sur ce qui doit être accompli plutôt que sur la façon de réussir une gouvernance, une gestion et un contrôle efficaces des activités. Il agit donc comme un intégrateur des pratiques de gouvernance des SI et s'adresse aux directions générales, au management des métiers et de l'informatique, aux professionnels de la gouvernance, de l'assurance et de la sécurité comme à ceux de l'audit et du contrôle informatique. Il est conçu pour être complémentaire d'autres standards et des bonnes pratiques et pour être utilisé conjointement avec eux.

La mise en place des bonnes pratiques doit être cohérente avec la gouvernance de l'entreprise et avec le cadre de contrôle, appropriée à l'entreprise et intégrée aux autres méthodes et pratiques utilisées. Les standards et les bonnes pratiques ne sont pas la panacée. Leur efficacité dépend de la façon dont ils ont été mis en œuvre et dont ils sont tenus à jour. Ils sont plus utiles lorsqu'on les applique comme un ensemble de principes et comme point de départ pour l'élaboration de procédures spécifiques sur mesure. Pour éviter que les pratiques restent au niveau des bonnes intentions, le management et le personnel doivent comprendre quoi faire, comment le faire et pourquoi c'est important.

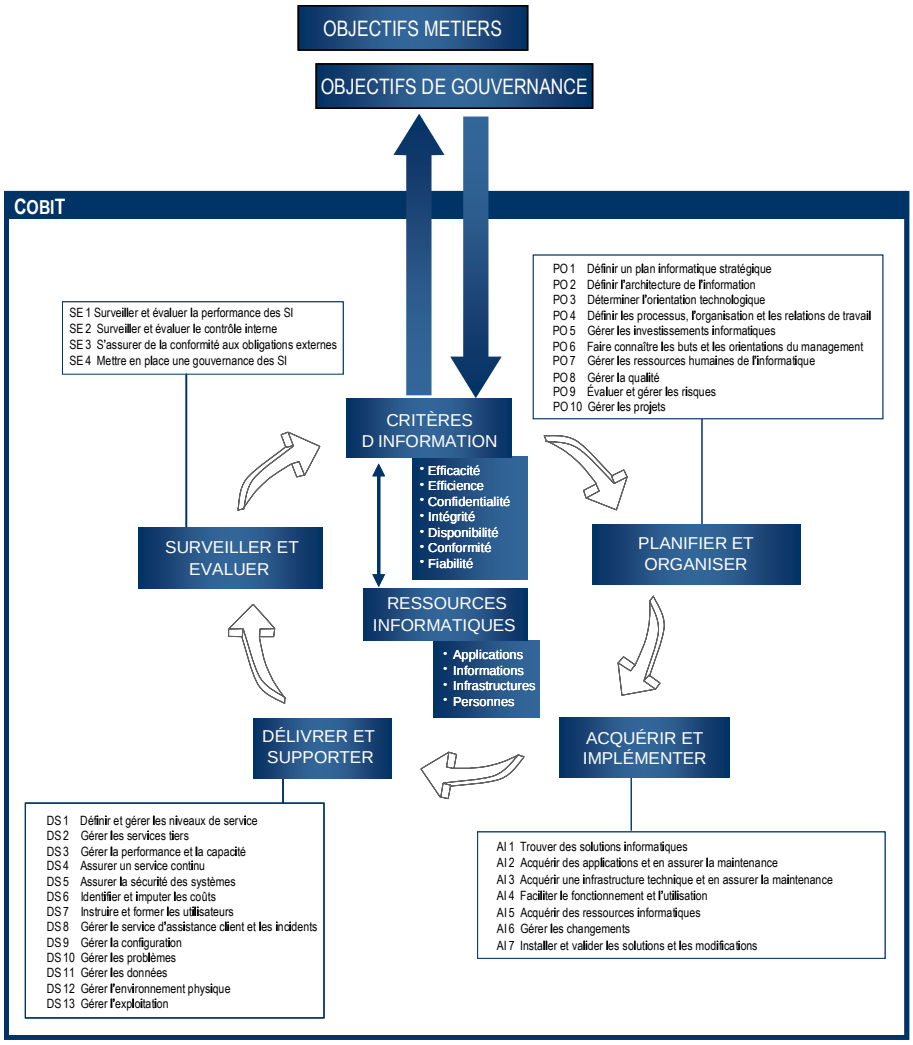
Pour réussir l'alignement des bonnes pratiques sur les exigences métiers, il est recommandé d'utiliser COBIT au niveau le plus général, ce qui fournira un cadre de contrôle global basé sur un modèle de processus informatiques génériques qui convient habituellement à toutes les entreprises. Les pratiques spécifiques et les standards qui intéressent des domaines particuliers peuvent être mis en regard du cadre de référence COBIT, fournissant ainsi un ensemble hiérarchisé de guides.

COBIT concerne différents types d'utilisateurs :
- **les directions générales :** pour que l'investissement informatique produise de la valeur et pour trouver le bon équilibre entre risques et investissements en contrôles, dans un environnement informatique souvent imprévisible ;
- **les directions métiers :** pour obtenir des assurances sur la gestion et le contrôle des services informatiques fournis en interne ou par des tiers ;
- **les directions informatiques :** pour fournir les services informatiques dont les métiers ont besoin pour répondre à la stratégie de l'entreprise, et pour contrôler et bien gérer ces services ;
- **les auditeurs :** pour justifier leurs opinions et/ou donner des conseils au management sur les dispositifs de contrôle interne.

COBIT a été développé et est maintenu à jour par un institut indépendant et sans but lucratif, puisant dans l'expertise des membres de ses associations affiliées, des experts du monde des affaires et des professionnels du contrôle et de la sécurité. Son contenu est basé sur une recherche permanente des bonnes pratiques de l'informatique et il est continuellement mis à jour, offrant ainsi un objectif et des ressources pratiques à tous les types d'utilisateurs.

COBIT est axé sur les objectifs et sur la perspective de la gouvernance des SI. Il s'assure que son cadre de référence en englobe bien tous les aspects, en accord avec les principes de la gouvernance d'entreprise et, par conséquent, qu'il peut être accepté par les administrateurs, dirigeants, auditeurs et régulateurs. Dans l'Annexe II, un tableau montre comment les objectifs de contrôle de COBIT se relient aux cinq domaines de la gouvernance des SI et aux activités de contrôle du COSO.

Figure 23 Le Cadre de référence général de COBIT



La **figure 24** présente les relations entre les différents éléments du cadre de référence de COBIT et les domaines d'action de la gouvernance des SI.

Figure 24 Cadre de référence COBIT et domaines de gouvernance des SI

	Objectifs	Métriques	Pratiques	Modèles de maturité
Alignement stratégique	P	P		
Apport de valeur		P	S	P
Gestion des risques		S	P	S
Gestion des ressources		S	P	P
Mesure de la performance	P	P		S

P = *inducteur Primaire* **S** = *inducteur Secondaire*

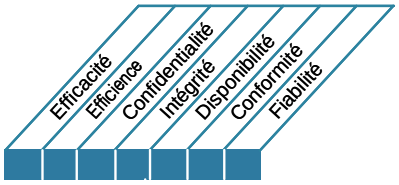
COMMENT UTILISER CE LIVRE

Navigation dans le cadre de référence COBIT

On trouvera une description de chacun des processus informatiques de COBIT, ainsi que des objectifs clés et des métriques, dans cette présentation en cascade **(figure 25)**.

Figure 25 Navigation dans COBIT

Pour chaque processus informatique, les objectifs de contrôle sont présentés comme les actions génériques des bonnes pratiques de gestion minimum nécessaires pour que le processus soit sous contrôle.



Le contrôle du processus informatique

nom du processus

qui répond à l'exigence des métiers vis-à-vis de l'informatique

liste des principaux objectifs métiers

en se concentrant sur

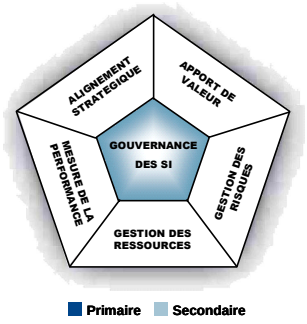
liste des principaux objectifs du processus

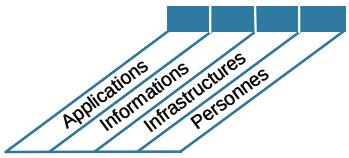
atteint son objectif grâce à

des objectifs liés à l'activité

et est mesuré par

des métriques clés





Présentation des composants essentiels de COBIT

Le cadre de référence COBIT est constitué d'un certain nombre de composants principaux que l'on retrouve dans le reste de cette publication et qui sont organisés en 34 processus, offrant ainsi une image complète de la façon de contrôler, de gérer et de mesurer chacun d'entre eux. Chaque processus est détaillé en quatre sections et chaque section occupe le plus souvent une page :

- La section 1 **(figure 25)** contient une description du processus qui résume ses objectifs, la description du processus étant présentée en éléments successivement décalés (en cascade). Cette page montre aussi sous forme schématique quels sont les critères d'information, les ressources informatiques et les domaines de la gouvernance des SI qui concernent ce processus, avec la précision P pour primaire ou S pour secondaire.
- La section 2 contient les objectifs de contrôle pour ce processus.
- La section 3 contient un tableau des éléments en entrée (entrées) et un autre des éléments en sortie (sorties) du processus, le tableau RACI, et un dernier tableau qui rapproche les objectifs et les métriques.
- La section 4 contient le modèle de maturité pour ce processus.

On peut présenter ainsi les éléments qui conditionnent la performance du processus :
- Les entrées du processus sont ce dont le propriétaire du processus a besoin que les autres lui fournissent.
- La description du processus et les objectifs de contrôle détaillés présentent ce que le propriétaire du processus doit faire.
- Les sorties du processus sont ce que le propriétaire du processus doit livrer.
- La partie objectifs et métriques montre comment il faut mesurer le processus.
- Le tableau RACI précise ce qui doit être délégué et à qui.
- Le modèle de maturité montre ce qu'il faut faire pour progresser.

Les rôles dans le tableau RACI sont désignés pour tous les processus par les expressions :
- Directeur général (DG).
- Directeur financier (DF).
- Direction métier.
- Directeur informatique (DSI).
- Propriétaire de processus métier.
- Responsable de l'exploitation.
- Responsable de l'architecture.
- Responsable des développements.
- Responsable administratif de l'informatique (dans les grandes entreprises, le responsable de fonctions telles que ressources humaines, budget ou contrôle interne).
- Responsable de la gestion des projets (PMO, Project Management Officer) ou fonction de gestion de projet.
- Conformité, audit, risque et sécurité (personnes qui ont des responsabilités de contrôle mais pas de responsabilités opérationnelles informatiques).

Certains processus spécifiques ont un rôle spécialisé supplémentaire propre au processus, par ex. Responsable service gestion des incidents pour le processus DS8.

Il faut bien noter que même si le présent contenu a été collecté auprès de centaines d'experts, selon des recherches et des vérifications rigoureuses, les entrées, sorties, responsabilités, mesures et objectifs sont des exemples et ne prétendent constituer ni des prescriptions ni une liste exhaustive. Ils proposent une base de connaissance et d'expertise dans laquelle chaque entreprise doit sélectionner ce qui sera efficace et efficient pour son activité en fonction de sa stratégie, de ses objectifs et de ses politiques.

Utilisateurs des composants de COBIT

Les dirigeants peuvent utiliser les supports COBIT pour évaluer les processus informatiques à l'aide des objectifs métier et des objectifs informatiques décrits en Annexe I, afin de clarifier les objectifs des processus informatiques et les modèles de maturité des processus pour évaluer les performances réelles.

Les responsables de la mise en œuvre et les auditeurs peuvent identifier les exigences de contrôle applicables à partir des objectifs de contrôle et les responsabilités à partir des activités et des tableaux RACI associés.

Tous les utilisateurs potentiels peuvent tirer parti du contenu COBIT et l'utiliser dans le cadre d'une méthode globale de gestion et de gouvernance des SI, conjointement à d'autres normes plus détaillées telles que :
- ITIL pour la prestation de services ;
- CMM pour la fourniture de solutions ;
- ISO 17799 pour la sécurité de l'information ;
- PMBOK ou PRINCE2 pour la gestion de projets.

Annexes

On trouvera à la fin du livre les sections de référence supplémentaires suivantes :

I Tableaux établissant les liens entre les objectifs et les processus (3 tableaux)

II. Relations des processus informatiques avec les domaines de la gouvernance des SI, le COSO, les ressources informatiques de COBIT et les critères d'information COBIT.

III. Modèle de maturité pour le contrôle interne.

IV. Documents de référence de COBIT 4.1.

V. Correspondance entre COBIT 3e édition et COBIT 4.1.

VI. Approche recherche et développement.

VII. Glossaire

VIII. COBIT et produits de la famille COBIT

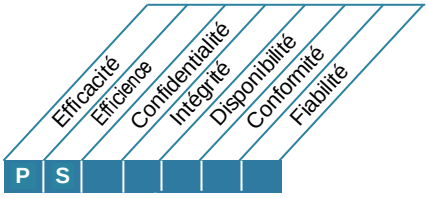
PLANIFIER ET ORGANISER

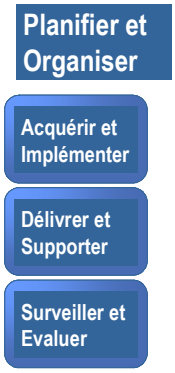
PO1 Définir un plan informatique stratégique
PO2 Définir l'architecture de l'information
PO3 Déterminer l'orientation technologique
PO4 Définir les processus, l'organisation et les relations de travail
PO5 Gérer les investissements informatiques
PO6 Faire connaître les buts et les orientations du management
PO7 Gérer les ressources humaines de l'informatique
PO8 Gérer la qualité
PO9 Évaluer et gérer les risques
PO10 Gérer les projets

DESCRIPTION DU PROCESSUS

PO1 Définir un plan informatique stratégique

Un plan de stratégie informatique est nécessaire pour gérer et orienter toutes les ressources informatiques vers les priorités stratégiques de l'entreprise. La DSI et les parties prenantes de l'entreprise ont la responsabilité de s'assurer que la meilleure valeur possible est obtenue des portefeuilles de projets et de services. Le plan stratégique doit permettre aux principales parties prenantes d'améliorer leur compréhension des potentialités et des limites des technologies de l'information (TI), d'évaluer la performance actuelle, d'identifier les besoins en capacité et en ressources humaines et de les éclairer sur le niveau d'investissement nécessaire. La stratégie et les priorités de l'entreprise doivent se refléter dans les portefeuilles de projets et doivent être mises en œuvre par le(s) plan(s) tactique(s) des SI qui précise(nt) succintement les objectifs, les plans et les tâches et qui sont compris et acceptés à la fois par les métiers et l'informatique.





Le contrôle du processus informatique

Définir un plan informatique stratégique

qui répond à l'exigence des métiers vis-à-vis de l'informatique

soutenir ou étendre les exigences de stratégie et de gouvernance de l'entreprise tout en maintenant la transparence des bénéfices, des coûts et des risques

en se concentrant sur

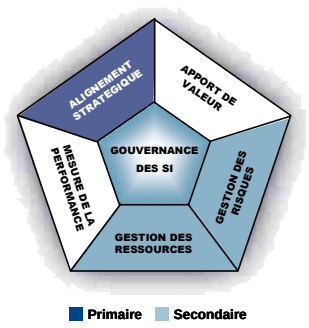
la convergence du management de l'entreprise et du management de l'informatique dans la traduction des exigences des métiers en offres de services, et sur le développement de stratégies pour fournir ces services en toute transparence et efficacité

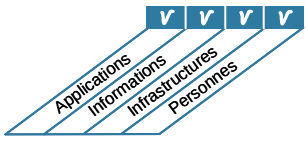
atteint son objectif en

- travaillant avec les métiers et la direction générale pour aligner la planification stratégique des SI avec les besoins actuels et futurs de l'entreprise
- ayant un bonne connaissance des capacités actuelles des technologies de l'information
- fournissant un schéma des priorités à appliquer aux objectifs des métiers qui quantifie les exigences des métiers

et est mesuré par

- le pourcentage des objectifs informatiques du plan informatique stratégique qui apporte un soutien au plan stratégique des métiers
- le pourcentage de projets informatiques dans le portefeuille de projets qui découle directement du plan tactique des SI
- le délai entre les mises à jour du plan stratégique des SI et celles du plan tactique





OBJECTIFS DE CONTRÔLE

PO1 Définir un plan informatique stratégique

PO1.1 Gestion de la valeur des SI
Travailler avec les métiers pour s'assurer que le portefeuille d'investissements informatiques de l'entreprise contient des programmes ou projets dont les analyses de rentabilité sont solides. Reconnaître qu'il y a des investissements obligatoires, indispensables et discrétionnaires qui diffèrent en complexité et en degré de liberté pour ce qui est de l'attribution des crédits. Les processus informatiques doivent fournir aux programmes des composants informatiques efficaces et efficients et des alertes, au plus tôt, pour tout écart par rapport au plan, par exemple en ce qui concerne les coûts, les délais et les fonctionnalités, susceptible d'avoir des conséquences sur les résultats attendus des programmes. Les services informatiques doivent être rendus sur la base de contrats de services *(CS ou Service Level Agreement SLA)* équitables et applicables. La responsabilité finale de l'obtention des bénéfices et du contrôle des coûts est clairement assignée et supervisée. Établir une évaluation juste, transparente, reproductible et comparable des analyses de rentabilité qui tient compte de la valeur financière, du risque de ne pas fournir une capacité et de ne pas réaliser les bénéfices attendus.

PO1.2 Alignement métiers-informatique
Instaurer des processus de formation bi-directionnelle et d'engagement réciproque dans le plan stratégique pour arriver à un alignement et une intégration de l'informatique et des métiers. Trouver un compromis entre les impératifs métiers et ceux de l'informatique de façon à ce que les priorités fassent l'objet d'un agrément mutuel.

PO1.3 Évaluation de la capacité et de la performance actuelle
Évaluer la capacité et la performance actuelle de la configuration et le servi fourni de façon à constituer une base d'évaluation de besoins à venir. Définir la performance en termes de contribution de l'informatique aux objectifs des métiers, de fonctionnalités, de stabilité, de complexité, de coûts, de forces et de faiblesses.

PO1.4 Plan informatique stratégique
Créer un plan stratégique qui définit, en coopération avec les parties prenantes, comment les objectifs de l'informatique vont contribuer aux objectifs stratégiques de l'entreprise et aux coûts et aux risques qui leur sont liés. Il doit inclure les programmes d'investissements informatiques, les services et les actifs informatiques. Il doit définir comment les objectifs seront atteints, les métriques à retenir et les procédures permettant d'obtenir un aval formel des parties prenantes. Le plan informatique stratégique doit couvrir les budgets d'investissement et de fonctionnement, les sources de financement, la stratégie de fourniture, la stratégie d'achat et les exigences légales et réglementaires. Le plan stratégique doit être suffisamment détaillé pour permettre de définir des plans informatiques tactiques.

PO1.5 Plans informatiques tactiques
Créer un portefeuille de plans informatiques tactiques qui découle du plan informatique stratégique. Ces plans tactiques doivent contenir les programmes d'investissements informatiques, les services et les actifs informatiques. Ces plans tactiques doivent décrire les initiatives informatiques nécessaires, des besoins en ressources, et comment l'utilisation des ressources et la réalisation de bénéfices seront surveillées et gérées. Les plans tactiques doivent être suffisamment détaillés pour permettre de définir des plans de projets. Gérer activement les plans tactiques informatiques et les initiatives au moyen de l'analyse de projets et des portefeuilles de services.

PO1.6 Gestion du portefeuille informatique
Gérer activement avec les métiers le portefeuille des programmes d'investissements informatiques qui sont nécessaires pour atteindre les objectifs métiers stratégiques spécifiques ; cela consiste à identifier, définir, évaluer, sélectionner, initier et contrôler ces programmes et à établir leurs priorités respectives. Cela inclut de clarifier les résultats métiers désirés, de s'assurer que les objectifs des programmes favorisent l'obtention de ces résultats, de comprendre l'ampleur des efforts nécessaires pour les obtenir, d'affecter clairement la responsabilité finale et de définir les mesures de soutien, de définir les projets qui font partie des programmes, d'allouer les ressources et les financements, de déléguer l'autorité, et de commander les projets nécessaires au moment du lancement des programmes.

GUIDE DE MANAGEMENT

PO1 Définir un plan informatique stratégique

De	Entrées
PO5	Rapports coûts/bénéfices
PO9	Évaluation des risques
PO10	Portefeuille actualisé des projets
DS1	Besoins de services nouveaux/actualisés ; portefeuille actualisé des services
*	Stratégie d'entreprise et priorités
*	Portefeuille de programmes
SE1	Entrée de la performance dans le planning SI
SE4	Etat de situation de la gouvernance des SI ; orientation stratégique de l'entreprise pour les SI

* Entrées externes à COBIT

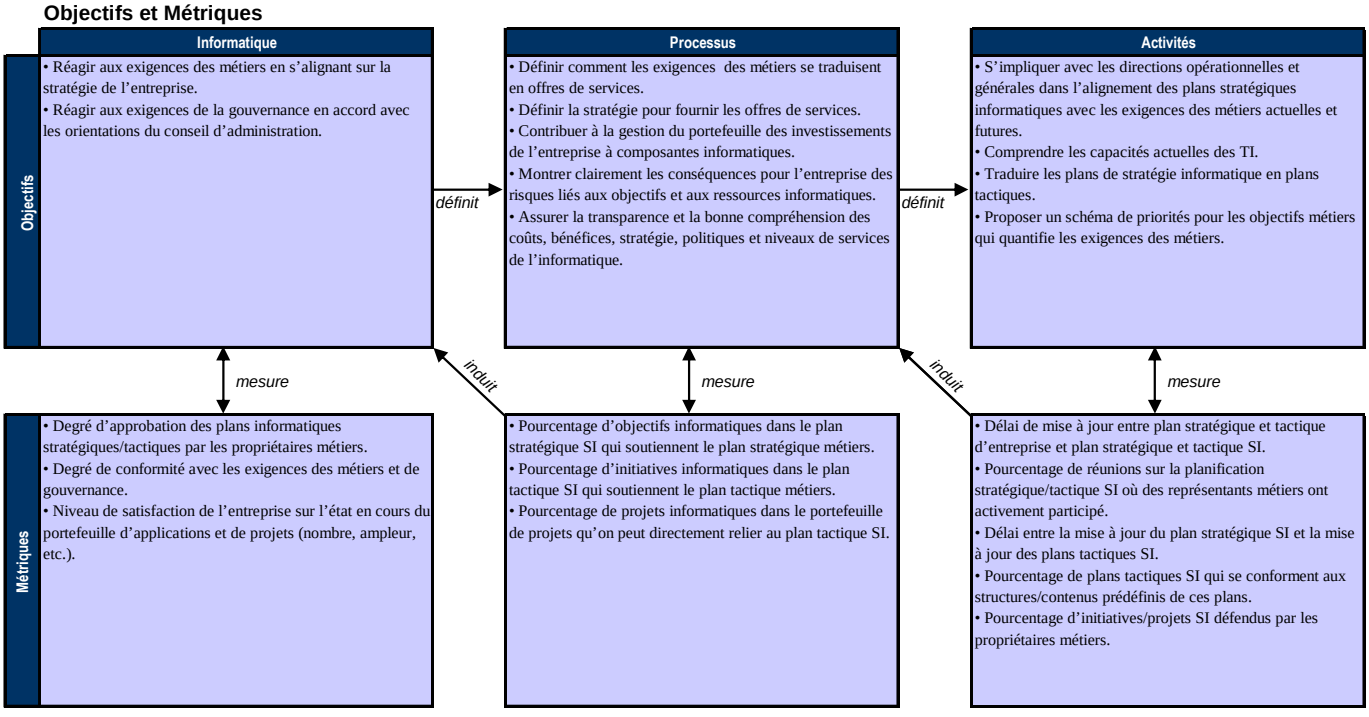
Sorties	Vers						
Plan informatique stratégique	PO2…PO6		PO8	PO9	AI1	DS1	
Plan informatique tactique	PO2…PO6			PO9	AI1	DS1	
Portefeuille de projets	PO5	PO6	PO10	AI6			
Portefeuille de services	PO5	PO6	PO9	DS1			
Stratégie de fourniture	DS2						
Stratégie d'achats	AI5						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Lier objectifs métiers et objectifs informatiques.	C	I	A/R	R	C						
Identifier les dépendances critiques et les performances actuelles.	C	C	R	A/R	C	C	C	C	C		C
Construire un plan informatique stratégique.	A	C	C	R	I	C	C	C	C	I	C
Élaborer des plans informatiques tactiques.	C	I		A	C	C	C	C	C	R	I
Analyser les portefeuilles de programmes et gérer les portefeuilles de projets et de services.	C	I	I	A	R	R	C	R	C	C	I

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO1 Définir un plan informatique stratégique

La gestion du processus *Définir un plan informatique stratégique* qui répond à l'exigence des métiers vis-à-vis de l'informatique *soutenir ou étendre les exigences de stratégie et de gouvernance de l'entreprise tout en maintenant la transparence des bénéfices, coûts et risques est* :

0 Inexistante quand

Il n'y a pas de planification informatique stratégique. Le management n'a pas conscience qu'un plan informatique stratégique est nécessaire à la réalisation des objectifs de l'entreprise.

1 Initialisée, au cas par cas quand

Le management connaît le besoin d'un plan informatique stratégique. La planification informatique s'effectue au cas par cas en réponse à des exigences métiers spécifiques. La planification informatique stratégique fait l'objet de discussions occasionnelles aux réunions de la DSI. L'alignement des exigences métiers, des applications et de l'informatique se fait d'une façon réactive plus que par une stratégie générale de l'entreprise. La position stratégique par rapport au risque est déterminée de façon informelle, projet par projet.

2 Reproductible mais intuitive quand

Le plan stratégique informatique n'est partagé avec la direction de l'entreprise qu'en réponse à des besoins spécifiques. On met à jour les plans informatiques en réponse à des demandes du management. On prend les décisions projet par projet, sans cohérence avec une stratégie globale d'entreprise. On connaît intuitivement les risques et les avantages des principales décisions stratégiques pour les utilisateurs.

3 Définie quand

Une politique définit quand et comment réaliser le plan informatique stratégique. Ce dernier adopte une approche structurée qui est documentée et connue de tout le personnel. Le processus de planification informatique est raisonnablement conçu et garantit une bonne probabilité de réalisation d'un plan approprié. Toutefois, la mise en œuvre du processus est laissée à l'initiative de responsables individuels et aucune procédure d'examen de ce processus n'est prévue. La stratégie informatique globale inclut une définition cohérente des risques acceptés par l'entreprise et précise si elle se voit en position d'innovateur ou de suiveur. Les stratégies informatiques en matière de finances, de techniques et de ressources humaines influencent de plus en plus l'acquisition de nouveaux produits et de nouvelles technologies. La planification informatique stratégique fait l'objet de discussions aux réunions de la direction de l'entreprise.

4 Gérée et mesurable quand

La planification informatique stratégique est une pratique standard et le management signale les anomalies. Elle correspond à une fonction de management comportant des responsabilités de cadre supérieur. Le management est capable de surveiller le processus de planification informatique stratégique, de prendre des décisions étayées en se basant sur lui, et de mesurer son efficacité. Il existe à la fois des plans informatiques à court et long terme qui sont diffusés à tous les échelons de l'entreprise, avec des mises à jour lorsque c'est nécessaire. La stratégie informatique et la stratégie globale de l'entreprise sont de mieux en mieux coordonnées grâce à l'utilisation de processus métiers et de capacités qui ajoutent de la valeur, et grâce à la mise en œuvre d'applications et de technologies qui induisent la ré-ingénierie des processus métiers. Il existe un processus bien défini assurant une bonne répartition entre les ressources internes et externes nécessaires au développement et à l'exploitation des systèmes.

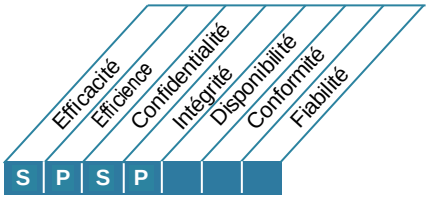
5 Optimisée quand

Le plan informatique stratégique est un processus documenté et vivant, toujours pris en compte dans la définition des objectifs métiers ; la valeur apportée par les investissements informatiques est patente. Les considérations risque/valeur ajoutée sont continuellement actualisées dans le processus de planification informatique stratégique. On développe et on actualise en permanence des plans informatiques à long terme réalistes pour refléter l'évolution des technologies et des activités de l'entreprise. On utilise des tests comparatifs avec les normes reconnues et fiables des métiers, et on les intègre au processus d'élaboration de la stratégie. Le plan informatique stratégique tient compte de la façon dont l'évolution des nouvelles technologies peut induire de nouvelles capacités métiers et améliorer l'avantage compétitif de l'entreprise.

DESCRIPTION DU PROCESSUS

PO2 Définir l'architecture de l'information

Les responsables des systèmes informatiques doivent créer et mettre régulièrement à jour un modèle d'information de l'entreprise et déterminer quels sont les systèmes appropriés susceptibles d'optimiser l'utilisation de cette information. Cela comprend l'élaboration d'un dictionnaire des données de l'entreprise, des règles de syntaxe de données propres à l'entreprise, d'un système de classification des données et de niveaux de sécurité. En assurant une information fiable et sûre, ce processus améliore la gestion de la prise de décision et permet de rationaliser les ressources informatiques pour être en phase avec les stratégies de l'entreprise. Ce processus informatique est aussi nécessaire pour étendre le champ de la responsabilité de l'intégrité et de la sécurité des données et pour améliorer l'efficacité et le contrôle du partage de l'information entre les applications et les différents départements de l'entreprise.



Le contrôle du processus informatique

Définir l'architecture de l'information

qui répond à l'exigence des métiers vis-à-vis de l'informatique

répondre intelligemment et rapidement aux exigences, fournir des informations fiables et cohérentes et intégrer en douceur les applications aux processus métiers

en se concentrant sur

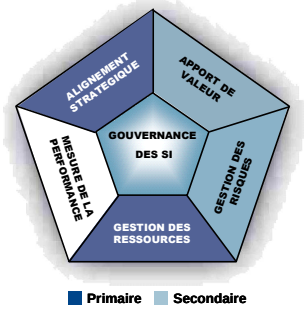
la constitution d'un modèle de données de l'entreprise intégrant un système de classification des informations pour assurer l'intégrité et la cohérence de toutes les données

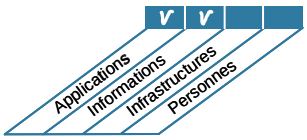
atteint son objectif en

- garantissant l'exactitude de l'architecture de l'information et du modèle de données
- attribuant la propriété des données
- classant l'information selon un système de classification approuvé

et est mesuré par

- le pourcentage d'éléments de données redondants/dupliqués
- le pourcentage d'applications qui ne se conforment pas à la méthodologie d'architecture de l'information de l'entreprise
- la fréquence des activités de validation des données.





OBJECTIFS DE CONTRÔLE

PO2 Définir l'architecture de l'information

PO2.1 Modèle d'architecture de l'information de l'entreprise
Établir et tenir à jour un modèle d'information de l'entreprise pour faciliter le développement d'applications et les activités d'aide à la décision, conforme aux plans informatiques décrits dans PO1. Ce modèle doit permettre d'optimiser la création, l'utilisation et le partage de l'information dans l'entreprise et d'en maintenir l'intégrité, la flexibilité, la fonctionnalité, la rentabilité, la disponibilité en temps opportun, la sécurité et la résistance aux pannes.

PO2.2 Dictionnaire et règles de syntaxe des données de l'entreprise
Maintenir opérationnel un dictionnaire des données qui utilise les règles de syntaxe des données de l'entreprise Ce dictionnaire doit faciliter le partage d'éléments de données par les applications et les systèmes, favoriser la compréhension commune des données entre l'informatique et les utilisateurs métiers et éviter la création d'éléments de données incompatibles.

PO2.3 Système de classification des données
Établir un système de classification basé sur les dimensions critiques et sensibles des données (par ex. publiques, confidentielles, secrètes) qui s'applique à toute l'entreprise. Ce système doit comprendre les détails sur la propriété des données, la définition des niveaux de sécurité et des contrôles de protection appropriés, une brève description des règles de conservation et de destruction des données, et de leurs dimensions critiques et sensibles. Il doit être utilisé comme base pour les contrôles, comme les contrôles d'accès, d'archivage ou de cryptage.

PO2.4 Gestion de l'intégrité
Définir et mettre en place des procédures qui assurent l'intégrité et la cohérence de toutes les données conservées sous forme électronique, comme les bases de données, les entrepôts de données et les archives de données.

GUIDE DE MANAGEMENT

PO2 Définir l'architecture de l'information

De	Entrées
PO1	Plans informatiques stratégiques et tactiques
AI1	Étude de faisabilité - exigences des métiers
AI7	Revue post-démarrage
DS3	Informations sur la performance et la capacité
SE1	Entrée de la performance dans le planning SI

Sorties	Vers						
Système de classification de données	AI2						
Plan optimisé des systèmes métiers	PO3	AI2					
Dictionnaire de données	AI2	DS11					
Architecture de l'information	PO3	DS5					
Classifications attribuées aux données	DS1	DS4	DS5	DS11	DS12		
Procédures et outils de classification	*						

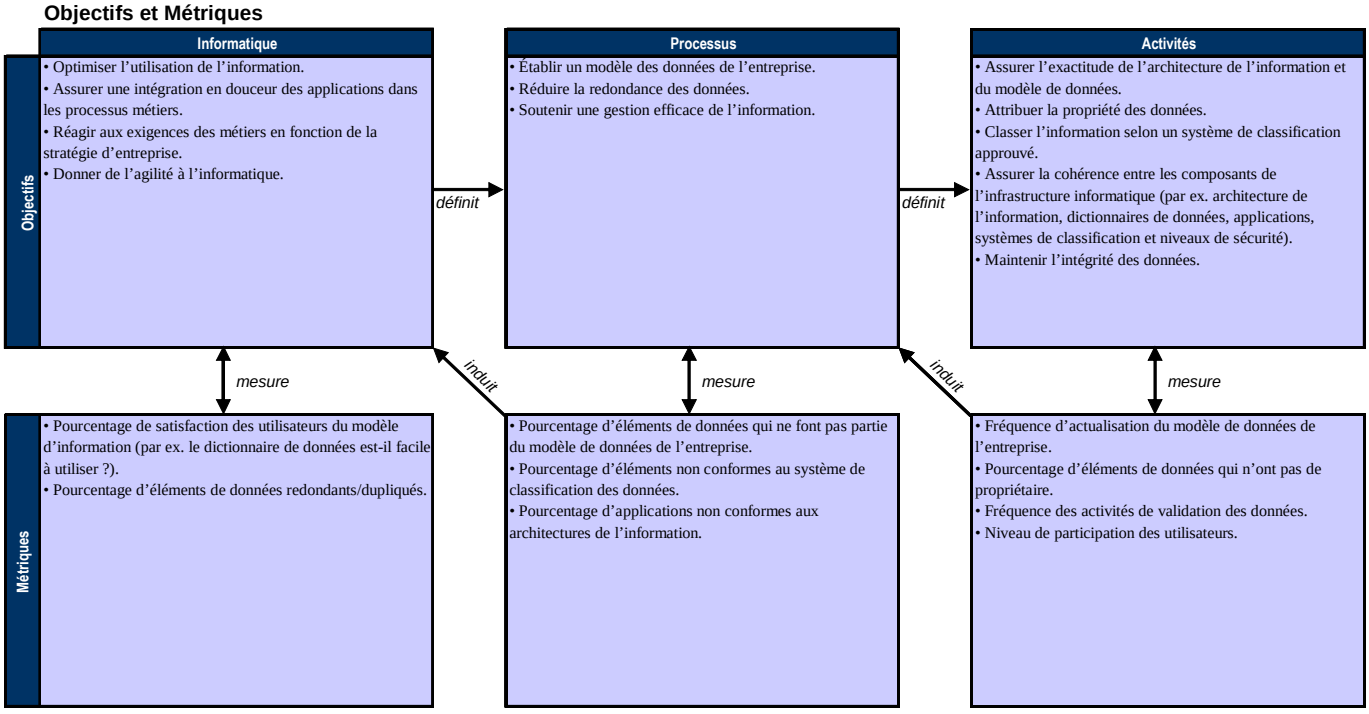
* Sorties externes à CobiT

Tableau RACI

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Créer et maintenir le modèle d'information de l'entreprise ou du groupe.		C	I	A	C		R	C	C		C
Créer et maintenir le(s) dictionnaire(s) de données de l'entreprise ou du groupe.				I	C		A/R	R			C
Élaborer et maintenir le système de classification de données.	I	C	A	C	C	I	C	C			R
Fournir aux propriétaires de données les procédures et les outils nécessaires aux systèmes de classification des données.	I	C	A	C	C	I	C	C			R
Utiliser le modèle d'information, le dictionnaire de données et le système de classification pour planifier des systèmes informatiques métiers optimisés.	C	C	I	A	C		R	C			I

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO2 Définir l'architecture de l'information

La gestion du processus *Définir l'architecture de l'information* qui répond à l'exigence des métiers vis-à-vis de l'informatique *répondre intelligemment et rapidement aux exigences, fournir des informations fiables et cohérentes et intégrer en douceur les applications aux processus métiers* est :

0 Inexistante quand

Il n'y a pas de prise de conscience de l'importance de l'architecture de l'information pour l'entreprise. Les connaissances, les compétences et les responsabilités nécessaires pour mettre en place cette architecture n'existent pas dans l'entreprise.

1 Initialisée, au cas par cas quand

Le management admet le besoin d'une architecture de l'information. L'élaboration de certains composants d'une architecture de l'information a lieu au cas par cas. Les définitions concernent les données, plutôt que les informations, et viennent des logiciels applicatifs disponibles sur le marché. La communication sur le besoin d'une architecture de l'information se fait au hasard, sans cohérence.

2 Reproductible mais intuitive quand

Un processus d'architecture de l'information se fait jour et différentes personnes dans l'entreprise suivent des procédures semblables, bien qu'informelles et intuitives. Les personnels acquièrent leurs compétences en architecture de l'information par la pratique et par la mise en œuvre de techniques répétitives. La nécessité tactique est à l'origine de la création de certains composants d'une architecture de l'information.

3 Définie quand

L'importance de l'architecture de l'information est comprise et acceptée et l'on sait clairement qui est responsable de sa mise en place. On a standardisé et documenté des procédures, outils et techniques liés à cette architecture ; ils sont encore simples et font partie d'activités de formation informelles. On a défini certaines politiques de base sur cette question en fonction de certaines nécessités stratégiques, mais la conformité avec les politiques, standards et outils n'est pas systématiquement respectée. On trouve une fonction d'administration des données formellement définie, qui met en place des standards à l'échelle de l'entreprise, et qui commence à faire des rapports sur la mise à disposition et l'utilisation de l'architecture de l'information. On commence à employer des outils automatisés, mais les processus et les règles utilisés sont définis par les offres commerciales de logiciels de bases de données. Un plan de formation formel a été élaboré mais les formations formelles sont encore basées sur l'initiative individuelle.

4 Gérée et mesurable quand

Des méthodes et des techniques précises soutiennent pleinement le développement et la mise en œuvre de l'architecture de l'information. On rend compte des performances du processus de développement de l'architecture de l'information et on mesure ses résultats. Des outils automatiques d'assistance sont largement répandus, mais pas encore intégrés. On a identifié les principaux éléments à mesurer, et un système de mesure est en place. Le processus de définition de l'architecture de l'information est proactif et conçu pour faire face aux besoins futurs de l'entreprise. Le personnel chargé de l'administration des données s'implique activement dans tous les efforts de développement des applications pour en assurer la cohérence. Un référentiel central automatisé est pleinement opérationnel. On utilise des modèles de données plus complexes pour bénéficier des informations contenues des bases de données. Les systèmes d'information à l'usage du management (EIS) et les systèmes d'aide à la décision utilisent pleinement les informations disponibles.

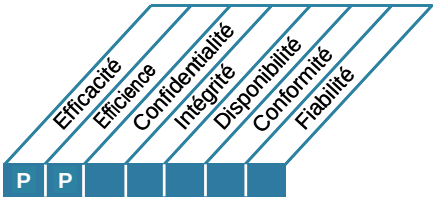
5 Optimisée quand

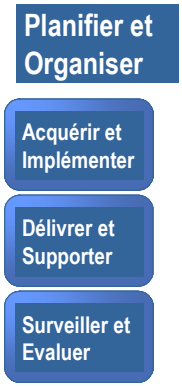
L'architecture de l'information est systématiquement utilisée à tous les niveaux. On met en permanence l'accent sur la valeur de l'architecture de l'information pour l'entreprise. Les informaticiens ont les connaissances et les compétences nécessaires pour développer et assurer la maintenance d'une architecture de l'information robuste et réactive qui s'intéresse à tous les besoins de l'entreprise. On utilise systématiquement et abondamment l'information fournie. On utilise largement les meilleures pratiques de la profession en matière de développement et de maintenance de l'architecture de l'information, y compris un processus d'amélioration permanente. On a défini une stratégie de mobilisation des informations en utilisant les technologies d'entrepôts de données et d'outils d'exploration des données (data mining). L'architecture de l'information s'améliore sans cesse, et elle prend en compte les informations non traditionnelles sur les processus, les organisations et les systèmes.

DESCRIPTION DU PROCESSUS

PO3 Déterminer l'orientation technologique

Le SI détermine l'orientation technologique susceptible de favoriser l'activité de l'entreprise. Cela exige la création et la maintenance d'un plan d'infrastructure technologique et d'un comité architecture des TI qui fixe et gère les attentes clairement exprimées et réalistes de ce que la technologie peut offrir en termes de produits, services et mécanismes de livraison. Ce plan est régulièrement actualisé et comprend des aspects comme l'architecture, l'orientation technologique, les plans d'acquisition, les standards, les stratégies de migration et les imprévus. Cela permet de réagir en temps utile aux modifications de l'environnement concurrentiel, cela permet aussi des économies d'échelle dans les effectifs et les investissements informatiques ainsi qu'une meilleure interopérabilité des plates-formes et des applications.





Le contrôle du processus informatique

Déterminer l'orientation technologique

qui répond à l'exigence des métiers vis-à-vis de l'informatique

posséder des systèmes applicatifs stables, rentables, intégrés et standardisés, et des ressources et des capacités qui répondent aux besoins actuels et futurs de l'entreprise

en se concentrant sur

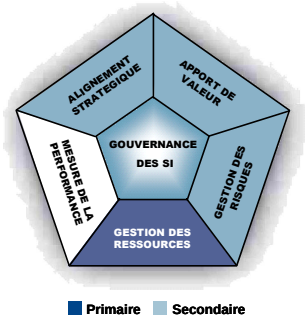
la définition et la mise en place d'un plan d'infrastructure informatique, d'une architecture et de standards qui savent identifier et mettre à profit les opportunités technologiques

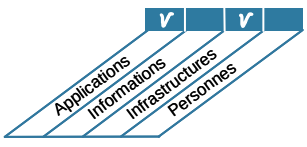
atteint son objectif en

- mettant en place un forum destiné à conseiller l'architecture et à vérifier la conformité
- mettant en place un plan d'infrastructure technologique qui trouve le bon équilibre entre coûts, risques et besoins
- définissant les standards d'infrastructure technologique en fonction des besoins de l'architecture informatique

et est mesuré par

- le nombre et le type d'écarts par rapport au plan d'infrastructure technologique
- la fréquence des révisions/actualisations du plan d'infrastructure technologique
- le nombre de plates-formes technologiques par service dans l'entreprise.





OBJECTIFS DE CONTRÔLE

PO3 Déterminer l'orientation technologique

PO3.1 Planification de l'orientation technologique
Analyser les technologies existantes et émergentes et décider quelle orientation technologique sera la plus favorable pour répondre à la stratégie informatique et pour l'architecture des systèmes de l'entreprise. Désigner aussi dans le plan les technologies qui permettront de créer des opportunités pour l'activité de l'entreprise. Entre autres composantes de l'infrastructure, le plan doit prendre en compte l'architecture des systèmes, l'orientation technologique, les stratégies de migration et les imprévus.

PO3.2 Plan d'infrastructure technologique
Créer et maintenir un plan d'infrastructure technologique en phase avec les plans stratégiques et tactiques des SI. Ce plan doit se baser sur les orientations technologiques et comporter une gestion des imprévus et des orientations pour l'acquisition de ressources informatiques. Il doit prendre en compte les modifications de l'environnement concurrentiel, des économies d'échelle dans les effectifs et les investissements informatiques ainsi qu'une meilleure interopérabilité des plates-formes et des applications.

PO3.3 Surveillance de l'évolution des tendances et de la réglementation
Mettre en place un processus pour surveiller les tendances de l'environnement du secteur d'activité, de la profession, de l'environnement informatique, légal et réglementaire. Introduire les conséquences de ces tendances dans le développement du plan d'infrastructure technologique des SI.

PO3.4 Standards informatiques
Pour proposer des solutions informatiques efficaces et sûres à l'ensemble de l'entreprise, constituer un forum informatique pour donner des lignes directrices en technologie de l'information, des avis sur les produits d'infrastructure et des conseils sur le choix technologique, mesurer la conformité par rapport à ces standards et à ces lignes directrices. Ce forum doit piloter les standards et les pratiques informatiques en fonction de leur pertinence vis-à-vis de l'activité de l'entreprise, des risques et de leur conformité aux exigences externes.

PO3.5 Comité d'architecture technologique
Créer un comité architecture des TI pour fournir les lignes directrices de cette architecture et les conseils pour leur application, et pour en vérifier la conformité. Ce comité doit piloter la conception de l'architecture des TI en s'assurant qu'elle favorise la stratégie de l'entreprise et qu'elle prend en compte les impératifs de conformité et de continuité. Ceci est relié au processus PO2 *Définir l'architecture de l'information.*

GUIDE DE MANAGEMENT

PO3 Déterminer l'orientation technologique

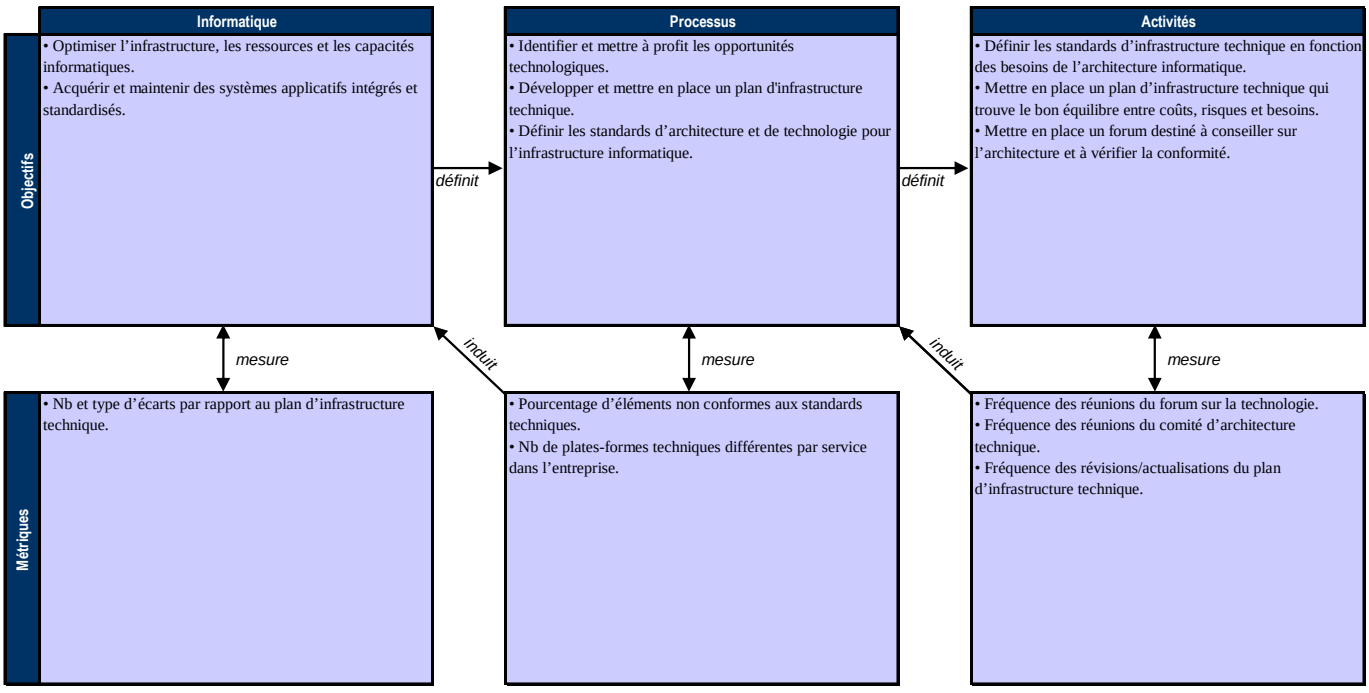
De	Entrées
PO1	Plans informatiques stratégiques et tactiques
PO2	Plan optimisé des systèmes métiers, architecture de l'information
AI3	Mises à jour des standards techniques
DS3	Information sur la performance et la capacité

Sorties	Vers						
Opportunités technologiques	AI3						
Standards techniques	AI1	AI3	AI7	DS5			
Mises à niveau régulières de l'état de la technologie	AI1	AI2	AI3				
Plan d'infrastructure technique	AI3						
Besoins en infrastructure	PO5						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Créer et maintenir à niveau un plan d'infrastructure technique.		I	I	A		C	R	C	C		C
Créer et maintenir à niveau des standards techniques.				A		C	R	C	I	I	I
Publier les standards techniques.		I	I	A		I	R	I	I	I	I
Surveiller l'évolution de la technologie.		I	I	A		C	R	C		C	C
Définir l'utilisation (future) (stratégique) des nouvelles technologies.		C	C	A		C	R	C		C	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.



MODÈLE DE MATURITÉ

PO3 Déterminer l'orientation technologique

La gestion du processus *Déterminer l'orientation technologique* qui répond à l'exigence des métiers vis-à-vis de l'informatique *posséder des systèmes applicatifs stables, rentables, intégrés et standardisés, et des ressources et des capacités qui répondent aux besoins actuels et futurs de l'entreprise* est :

0 Inexistante quand

Il n'y a pas de prise de conscience de l'importance d'un plan d'infrastructure technique pour l'entreprise. Les connaissances et compétences nécessaires pour développer un tel plan n'existent pas. Personne ne réalise qu'il est essentiel de prévoir des changements technologiques pour affecter les ressources de manière efficace.

1 Initialisée, au cas par cas quand

Le management admet le besoin de planifier l'architecture technique. Le développement de composants informatiques et la mise en place de nouvelles technologies se font isolément, au cas par cas. L'approche de la planification de l'infrastructure est réactive et poussée par les besoins opérationnels. Les choix techniques sont dictés par les plans produits souvent contradictoires des fournisseurs de matériels, de systèmes et de progiciels. Il y a peu de communication sur l'impact potentiel des changements technologiques.

2 Reproductible mais intuitive quand

On communique sur le besoin et l'importance d'une planification technologique. La planification reste tactique et orientée vers la recherche de solutions techniques à des problèmes techniques, plutôt que vers l'utilisation de l'informatique pour répondre aux besoins de l'entreprise. L'évaluation des changements technologiques est laissée à des personnes différentes qui suivent des processus intuitifs, mais similaires. Les personnels acquièrent leurs compétences en planification technologique par la pratique et par la mise en œuvre répétitive de techniques. On voit émerger des techniques et des normes communes pour le développement de composants d'infrastructure.

3 Définie quand

Le management a conscience de l'importance du plan d'infrastructure technique. Le processus de son développement est raisonnablement sain et en cohérence avec le plan stratégique informatique. Il existe un plan d'infrastructure technique défini, documenté et bien diffusé, mais il n'est pas toujours respecté. Les orientations de ce plan montrent quels sont les domaines technologiques où l'entreprise souhaite être en pointe, et ceux qui ont une moindre priorité en fonction des risques et de la stratégie générale de l'entreprise. Les fournisseurs principaux sont choisis en fonction de l'adéquation de leurs projets d'évolution technologiques et de leurs politiques produits à long terme avec les orientations de l'entreprise. Il existe un programme formel de formation et de répartition des rôles et des responsabilités.

4 Gérée et mesurable quand

Le management assure le développement et la maintenance du plan d'infrastructure technique. L'équipe informatique a les connaissances et les compétences nécessaires pour développer un plan d'infrastructure technique. L'impact potentiel de l'évolution des technologies et des technologies nouvelles est pris en compte. Le management peut mettre en évidence les écarts par rapport au plan et anticiper les problèmes. On a désigné des responsables du développement et de la maintenance d'un plan d'infrastructure technique. Le processus de développement du plan d'infrastructure technique est élaboré et réactif aux changements. Les bonnes pratiques internes ont été intégrées au processus. La stratégie des ressources humaines est en adéquation avec les orientations technologiques pour faire en sorte que les informaticiens soient en mesure de faire face aux changements technologiques. On a défini des plans de migration pour l'introduction de nouvelles technologies. L'externalisation et le partenariat sont mis en œuvre pour accéder aux connaissances et compétences nécessaires. Le management a analysé l'acceptation du risque vis-à-vis de l'utilisation audacieuse ou au contraire prudente des technologies lorsqu'il s'agit de créer de nouvelles opportunités professionnelles ou d'améliorer l'efficacité opérationnelle.

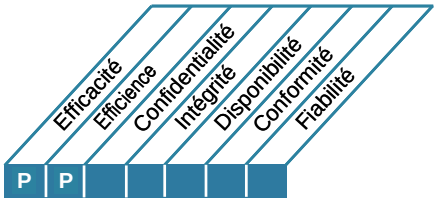
5 Optimisée quand

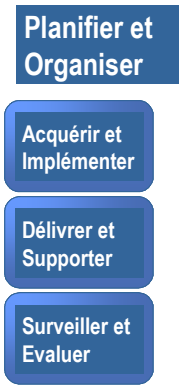
Une équipe de recherche évalue les technologies nouvelles ou en évolution et compare les pratiques de l'entreprise aux normes de la profession. Les orientations du plan d'infrastructure technique sont définies par rapport aux standards et développements internationaux et ceux de la branche, et non en fonction des technologies proposées par les fournisseurs. Les conséquences potentielles de changements technologiques sont analysées au niveau du management. Les dirigeants approuvent formellement les orientations technologiques nouvelles et les évolutions. L'entreprise a un plan d'infrastructure technique qui correspond à ses besoins, qui est robuste, réactif et susceptible de s'adapter à des modifications de l'environnement des métiers. On applique un processus continu d'amélioration du plan d'infrastructure technique. Les orientations technologiques sont largement inspirées des meilleures pratiques de la profession.

DESCRIPTION DU PROCESSUS

PO4 Définir les processus, l'organisation et les relations de travail

On définit l'organisation de l'informatique en prenant en compte les besoins en personnel et en compétences, en prévoyant les fonctions, les rôles et les responsabilités, la supervision, l'autorité, et en sachant qui rend des comptes à qui. Cette organisation fait partie d'un cadre de référence de processus informatiques qui assure la transparence et le contrôle ainsi que l'implication de la direction générale et de la direction opérationnelle. Un comité Stratégie assure la supervision des SI pour le compte du Conseil d'Administration (CA) et un ou plusieurs comité(s) de pilotage auxquel(s) participent les responsables des métiers et les responsables de l'informatique déterminent les priorités relatives aux ressources informatiques en fonction des besoins des métiers. Les processus, les politiques et les procédures administratives sont en place pour toutes les fonctions, en apportant une attention particulière au contrôle, à l'assurance qualité, à la gestion du risque, à la propriété des données et des systèmes et à la séparation des tâches. Pour assurer leur soutien aux exigences des métiers en temps voulu, l'informatique doit être impliquée dans les processus de décisions en cause.





Le contrôle du processus informatique

Définir les processus, l'organisation et les relations de travail

qui répondent à l'exigence suivante des métiers vis-à-vis de l'informatique

réagir avec rapidité et souplesse à la stratégie de l'entreprise tout en se conformant aux exigences de gouvernance et en proposant des interlocuteurs identifiés et compétents

en se concentrant sur

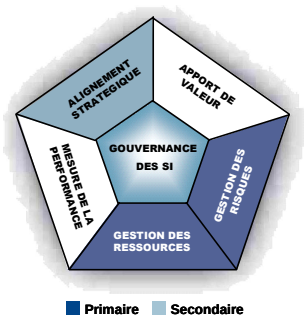
des structures organisationnelles informatiques transparentes, flexibles et réactives, des processus informatiques attribués à des propriétaires avec des rôles et des responsabilités intégrés aux processus métiers et aux processus de décision

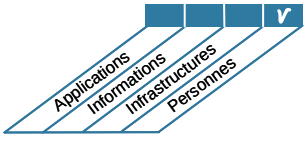
atteint son objectif en

- définissant un cadre de référence de processus informatiques
- mettant en place les entités et les structures organisationnelles appropriées
- définissant les rôles et les responsabilités

et est mesuré par

- le pourcentage de rôles dont la position et l'autorité sont décrits en détail
- le nombre d'unités métiers/processus qui ne sont pas pris en compte par l'organisation informatique mais qui devraient l'être, d'après la stratégie
- le nombre d'activités informatiques essentielles extérieures à l'organisation informatique et qui ne sont pas approuvées ou pas conformes aux standards organisationnels définis par l'informatique





OBJECTIFS DE CONTRÔLE

PO4 Définir les processus, l'organisation et les relations de travail

PO4.1 Cadre de référence des processus informatiques
Définir un cadre de référence des processus pour mettre en œuvre le plan stratégique des SI. Ce cadre doit définir la structure des processus informatiques et leurs liens (ex. gérer les lacunes et les recouvrements entre processus), la propriété, la maturité, la mesure de la performance, l'amélioration, la conformité, les objectifs qualité et les plans pour les faire aboutir. Il doit organiser l'intégration des processus spécifiques aux SI, la gestion du portefeuille de l'entreprise, les processus métiers et les processus de modification de l'activité de l'entreprise. Le cadre de référence des processus informatiques doit être intégré à un système de gestion de la qualité et au cadre de contrôle interne.

PO4.2 Comité stratégique informatique
Mettre en place un Comité stratégique informatique au niveau du conseil d'administration. Ce comité doit s'assurer que la gouvernance des SI, élément de la gouvernance d'entreprise, est bien traitée, donne des avis sur les orientations stratégiques et passe en revue les investissements majeurs pour le compte du conseil d'administration .

PO4.3 Comité de pilotage informatique
Mettre en place un comité de pilotage informatique (ou équivalent) composé de cadres exécutifs, métiers et informatiques pour :
- Déterminer les priorités des programmes d'investissements informatiques en accord avec la stratégie et les priorités des métiers de l'entreprise
- Assurer un suivi des projets et résoudre les conflits de ressources
- Surveiller les niveaux et l'amélioration des services.

PO4.4 Position de la fonction informatique au sein de l'entreprise
Positionner la fonction informatique dans la structure globale de l'entreprise selon un modèle lié à l'importance des technologies de l'information dans l'entreprise, en tenant en particulier compte de leur dimension critique pour la stratégie des métiers et du niveau de dépendance opérationnelle vis-à-vis d'elles. Le niveau hiérarchique du DSI doit être proportionnel à l'importance des SI dans l'entreprise.

PO4.5 Structure du service informatique
Mettre en place une structure interne et externe d'organisation de l'informatique qui reflète les exigences des métiers. En outre, mettre en place un processus pour réviser périodiquement la structure organisationnelle des SI de façon à ajuster les besoins en personnel et les stratégies de recrutement pour faire face aux objectifs des métiers définis et aux changements qui se produisent.

PO4.6 Établissement des rôles et responsabilités
Établir et communiquer les rôles et les responsabilités du personnel de l'informatique et des utilisateurs finaux. Ils définissent l'autorité, le niveau de responsabilité et d'approbation de chacun pour répondre aux besoins de l'entreprise.

PO4.7 Responsabilité de l'assurance qualité informatique
Attribuer la responsabilité de la performance de la fonction assurance qualité et doter la fonction assurance qualité des systèmes d'assurance qualité, des compétences en contrôle et en communication appropriés. La position au sein de l'entreprise, les responsabilités et la dimension du groupe assurance qualité doivent répondre aux besoins de l'entreprise.

PO4.8 Responsabilité des risques, de la sécurité et de la conformité
Situer la propriété et la responsabilité des risques liés aux SI dans l'entreprise au niveau de management approprié. Définir et attribuer les rôles cruciaux de gestion des risques informatiques en y incluant les responsabilités spécifiques de la sécurité de l'information, de la sécurité physique et de la conformité. Situer la responsabilité de la gestion de la sécurité au niveau de l'entreprise de façon à ce qu'elle soit concernée par les questions qui touchent l'ensemble de l'entreprise. On peut avoir besoin d'attribuer des responsabilités supplémentaires de gestion de la sécurité à certains niveaux des SI pour faire face à des problèmes de sécurité spécifiques. Obtenir des orientations de la part du management sur l'appétence pour le risque et sur l'approbation de tout risque informatique résiduel.

PO4.9 Propriété des données et du système
Doter l'entreprise de procédures et d'outils qui lui permettent de faire face à ses responsabilités de propriétaire des données et des systèmes d'information. Les propriétaires doivent prendre les décisions concernant la classification de l'information et la protection de cette information en fonction de cette classification.

PO4.10 Supervision
Mettre en place des pratiques adéquates de supervision dans la fonction informatique pour s'assurer que les rôles et les responsabilités sont bien exercés, pour évaluer si le personnel possède suffisamment d'autorité et de ressources pour accomplir ses tâches et responsabilités et pour procéder, de manière générale, à la révision des indicateurs clés de performance.

PO4.11 Séparation des tâches
Mettre en place une séparation des rôles et des responsabilités qui réduisent la possibilité qu'un seul individu puisse détourner un processus critique. Le management doit s'assurer que le personnel n'effectue que les tâches autorisées relevant de sa fonction et de ses attributions.

PO4.12 Recrutement informatique
Évaluer régulièrement les besoins en personnel, ou à l'occasion de changements majeurs au sein de l'entreprise, au niveau métiers ou informatique pour s'assurer que la fonction informatique a un nombre suffisant de collaborateurs pour apporter le support adéquat et approprié aux attentes et objectifs des métiers.

PO4.13 Personnel informatique clé
Recenser et identifier les personnels clés (par ex. les remplaçants ou les renforts) et limiter la dépendance vis-à-vis de personnes uniques en charge d'une fonction critique.

PO4.14 Procédures et règles applicables au personnel sous contrat
S'assurer que les consultants et le personnel sous contrat qui travaillent à la direction informatique connaissent les règles de protection de l'information de l'entreprise et s'y conforment et ce pour que les termes des contrats passés avec eux soient respectés.

PO4.15 Relations
Mettre en place et maintenir opérationnelle une structure de coordination, de communication et de liaison optimale entre la fonction informatique et divers autres professionnels à l'intérieur et à l'extérieur de cette fonction, comme le conseil d'administration, la direction générale, les unités opérationnelles, certains utilisateurs, les fournisseurs, les responsables de la sécurité, les responsables de la gestion des risques, le groupe responsable de la conformité dans l'entreprise et les responsables chargés des prestations externes (externalisation et sous-traitance).

Page volontairement laissée blanche

GUIDE DE MANAGEMENT

PO4 Définir les processus, l'organisation et les relations de travail

De	Entrées
PO1	Plans stratégiques et tactiques
PO7	Politiques et procédures RH des SI, tableau des compétences SI, descriptions des postes
PO8	Actions pour l'amélioration de la qualité
PO9	Plans d'actions pour remédier aux risques SI
SE1	Plans d'actions correctives
SE2	Rapport sur l'efficacité des contrôles SI
SE3	Recueil des exigences légales/réglementaires concernant la fourniture de services informatiques
SE4	Améliorations du référentiel des processus

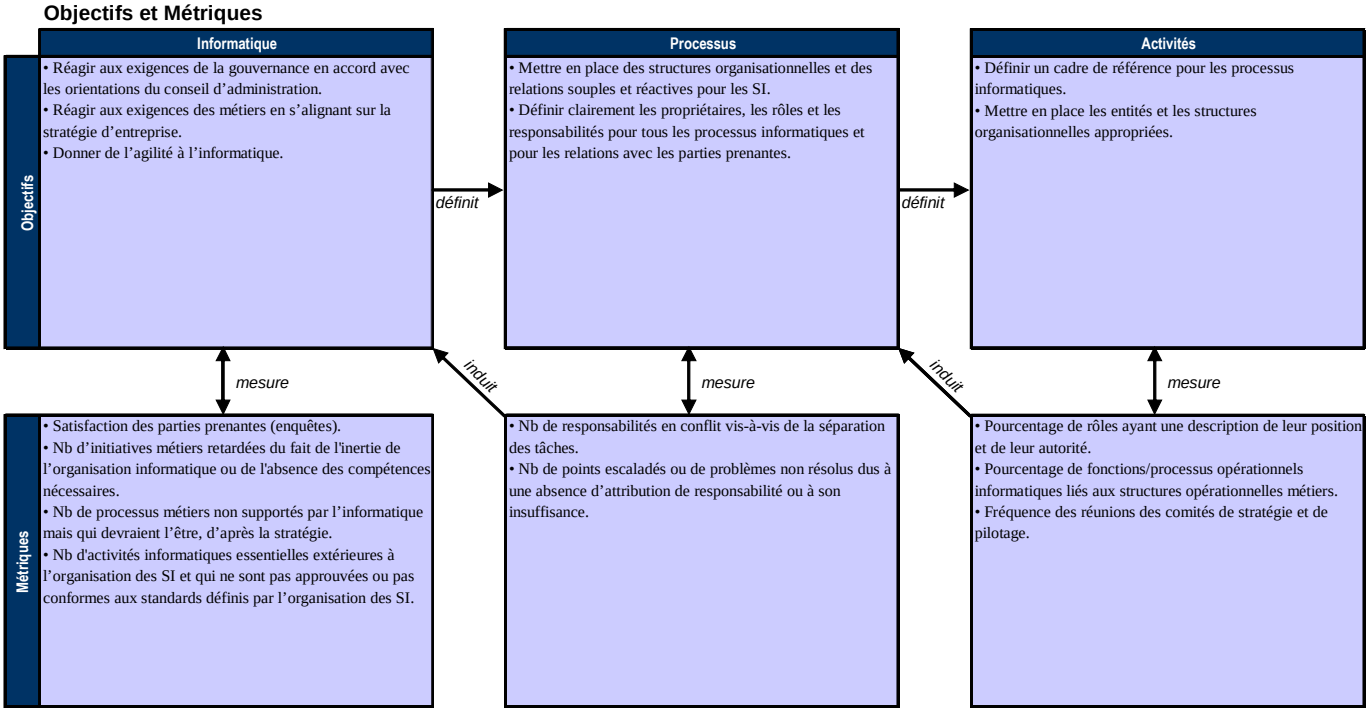
Sorties	Vers						
Référentiel des processus informatiques	SE4						
Documentation sur les propriétaires de systèmes	AI7	DS6					
Organisation et relations de travail de l'informatique	PO7						
Référentiel des processus informatiques, documentation des rôles et responsabilités	Tous						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Mettre en place une organisation des SI comprenant des comités et des liens vers les parties prenantes et les fournisseurs.	C	C	C	A		C	C	C	R	C	I
Élaborer le référentiel des processus informatiques.	C	C	C	A		C	C	C	R	C	C
Identifier les propriétaires des systèmes.		C	C	A	C	R	I	I	I	I	I
Identifier les propriétaires des données.		I	A	C	C	I	R	I	I	I	C
Mettre en place les rôles et les responsabilités des SI, en incluant supervision et séparation des tâches.		I	I	A	I	C	C	C	R	C	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO4 Définir les processus, l'organisation et les relations de travail

La gestion du processus *Définir les processus, l'organisation et les relations de travail* qui répond à l'exigence des métiers vis-à-vis de l'informatique *réagir avec rapidité et souplesse à la stratégie de l'entreprise tout en se conformant aux exigences de gouvernance et en proposant des interlocuteurs identifiés et compétents* est :

0 Inexistante quand

L'organisation de l'informatique n'est pas conçue de manière efficace pour contribuer au succès des objectifs des métiers.

1 Initialisée, au cas par cas quand

Les activités et fonctions informatiques viennent d'initiatives au cas par cas et sont mises en place sans cohérence. Les SI ne sont impliqués dans les processus métiers que dans les dernières étapes. La fonction informatique est considérée comme une fonction de support qui ne prend pas en compte l'organisation globale de l'entreprise. Le besoin d'une organisation informatique est implicitement compris, mais les rôles et les responsabilités ne sont ni formalisés ni appliqués.

2 Reproductible mais intuitive quand

La fonction informatique est organisée pour offrir des solutions tactiques aux besoins des clients et aux relations avec les fournisseurs, mais sans cohérence. On communique sur le besoin d'une organisation structurée et d'une gestion des fournisseurs, mais les décisions dépendent encore des connaissances et des compétences d'individus clés. On voit émerger des techniques communes de gestion de l'organisation informatique et des relations avec les fournisseurs.

3 Définie quand

On a défini les rôles et les responsabilités de l'informatique et des tiers. L'organisation informatique a été développée, documentée, communiquée et alignée sur la stratégie informatique. L'environnement de contrôle interne est défini. On a formalisé les relations avec les tiers, y compris les comités de pilotage, l'audit interne et la gestion des fournisseurs. L'organisation informatique possède toutes les fonctions nécessaires. Les fonctions à la charge du SI et celles à la charge des utilisateurs sont bien définies. Les besoins essentiels en personnel et en compétences informatiques sont satisfaits. Les relations avec les utilisateurs et les tiers sont formellement définies. On a défini et mis en place la répartition des rôles et des responsabilités.

4 Gérée et mesurable quand

L'informatique anticipe les changements, et dispose de tous les rôles nécessaires à la satisfaction des exigences des métiers. La direction des SI, la propriété des processus et les responsabilités opérationnelles et finales sont définies et équilibrées. Les bonnes pratiques internes sont mises en pratique dans l'organisation des fonctions du SI. La direction des SI a l'expertise et les compétences requises pour définir, mettre en œuvre et surveiller le type d'organisation et de relations retenu. On a standardisé les métriques à l'appui des objectifs des métiers ainsi que les facteurs clés de succès définis par les utilisateurs. On dispose d'un inventaire des compétences pour soutenir la constitution d'équipes de projets et le développement professionnel. La proportion de compétences et de ressources internes et de celles que l'on recherchera à l'extérieur est précisée et appliquée. La structure organisationnelle de l'informatique est un bon reflet des besoins de l'entreprise car elle fournit des services plus en ligne avec les processus métiers stratégiques qu'avec des technologies isolées.

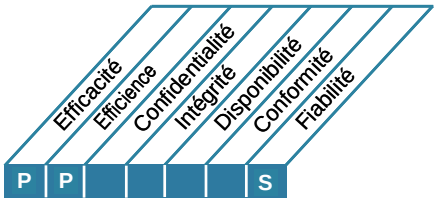
5 Optimisée quand

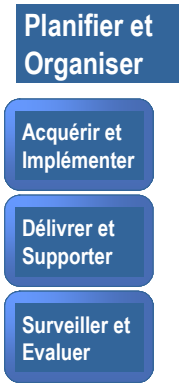
La structure organisationnelle de l'informatique est souple et capable de s'adapter. On a mis en place les meilleures pratiques de la profession. L'informatique est abondamment mise à contribution pour assurer la surveillance de la performance de l'organisation des SI et des processus. Les technologies servent de levier pour s'aligner et supporter la complexité et la répartition géographique de l'entreprise. Un processus d'amélioration continu est en place.

DESCRIPTION DU PROCESSUS

PO5 Gérer les investissements informatiques

Mettre en place et maintenir opérationnel, pour les programmes d'investissements informatiques, un cadre de référence qui couvre les coûts, les bénéfices, les priorités budgétaires, un processus de budgétisation formalisé et une gestion conforme au budget. Travailler avec les parties prenantes pour identifier et contrôler les coûts et bénéfices totaux dans le contexte des plans stratégiques et tactiques informatiques et initier des mesures correctives lorsque c'est nécessaire. Le processus favorise le partenariat entre l'informatique et les parties prenantes des métiers, facilite l'utilisation efficace et efficiente des ressources informatiques, et apporte transparence et responsabilité dans le coût total de propriété, la réalisation de bénéfices pour l'entreprise et le retour sur investissement des investissements informatiques.





Le contrôle du processus informatique

Gérer les investissements informatiques

qui répond à l'exigence des métiers vis-à-vis de l'informatique

améliorer constamment et de façon démontrable la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise avec des services intégrés et standardisés qui satisfont les attentes des utilisateurs finaux

en se concentrant sur

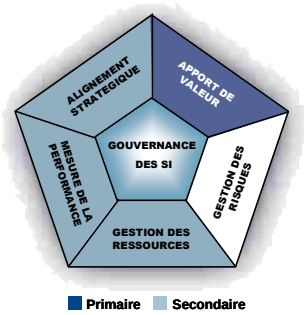
des décisions d'investissement et de gestion de portefeuille informatique efficaces et efficientes, et sur l'établissement et le suivi de budgets informatiques en ligne avec la stratégie et les décisions d'investissement informatique

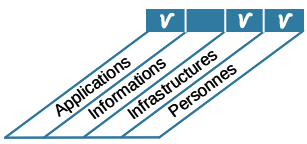
atteint son objectif en

- prévoyant et en attribuant des budgets
- définissant des critères d'investissements formels (ROI, durée d'amortissement, valeur nette actuelle)
- mesurant et en évaluant la valeur pour l'entreprise par rapport aux prévisions

et est mesuré par

- la réduction du coût unitaire des services informatiques fournis
- le pourcentage de l'écart budgétaire par rapport au budget total
- le pourcentage des dépenses informatiques exprimées en inducteurs de valeur métiers (ex. augmentation des ventes/services grâce à une plus grande connectivité)





OBJECTIFS DE CONTRÔLE

PO5 Gérer les investissements informatiques

PO5.1 Référentiel de gestion financière
Mettre en place un référentiel de gestion financière pour gérer les investissements et les coûts des actifs et services informatiques à l'aide de portefeuilles de programmes d'investissements, d'analyse de rentabilité et de budgets.

PO5.2 Définition des priorités dans le budget informatique
Mettre en place un processus de prise de décision pour définir les priorités dans l'attribution des ressources informatiques pour l'exploitation, les projets et la maintenance, dans le but de maximiser la contribution des SI à l'optimisation du retour sur investissement du portefeuille de l'entreprise qui gère les programmes d'investissements informatiques et des autres services et actifs informatiques.

PO5.3 Budget informatique
Définir et mettre en place des pratiques d'élaboration d'un budget qui reflète les priorités établies par le portefeuille de l'entreprise qui gère les programmes d'investissements informatiques, et qui prend en compte les coûts récurrents de fonctionnement et de maintenance de l'infrastructure actuelle. Ces pratiques doivent favoriser le développement d'un budget global informatique ainsi que celui de budgets de programmes individuels, avec une attention particulière pour les composantes informatiques de ces programmes. Ces pratiques doivent prévoir des révisions et des réajustements réguliers et l'approbation du budget global et des budgets des programmes individuels.

PO5.4 Gestion des coûts
Mettre en place un processus de gestion des coûts qui compare les coûts réels aux dépenses budgétées. Les coûts doivent être suivis et communiqués dans un rapport. Lorsqu'il y a des écarts il faut les mettre en évidence en temps voulu, évaluer leurs conséquences sur les programmes et, avec le responsable métier de ces programmes, prendre des mesures pour y remédier ; si nécessaire, il faut aussi réévaluer l'analyse de rentabilité du programme.

PO5.5 Gestion des bénéfices
Mettre en place un processus de surveillance des bénéfices attendus de la fourniture et du maintien de capacités informatiques appropriés. La contribution de l'informatique aux métiers, soit en tant que composante des programmes d'investissements à composantes informatiques, soit en tant que soutien opérationnel habituel, doit être identifiée, étayée par une analyse de rentabilité, approuvée, surveillée et faire l'objet de rapports. Il faut faire une analyse critique des rapports, et s'il est possible d'améliorer la contribution des SI, il faut déterminer des actions à entreprendre, et agir. Lorsque des changements dans la contribution des SI ont des conséquences sur un programme ou lorsque ces conséquences viennent de modifications d'autres projets, l'analyse de rentabilité du programme doit être réévaluée.

GUIDE DE MANAGEMENT

PO5 Gérer les investissements informatiques

De	Entrées
PO1	Plans informatiques stratégiques et tactiques, portefeuilles de projets et de services
PO3	Besoins en infrastructures
PO10	Portefeuille de projets informatiques actualisé
AI1	Étude de faisabilité des exigences des métiers
DS3	Plan performance et capacité (exigences)
DS6	Données financières informatiques
SE4	Résultats attendus des investissements informatiques des métiers

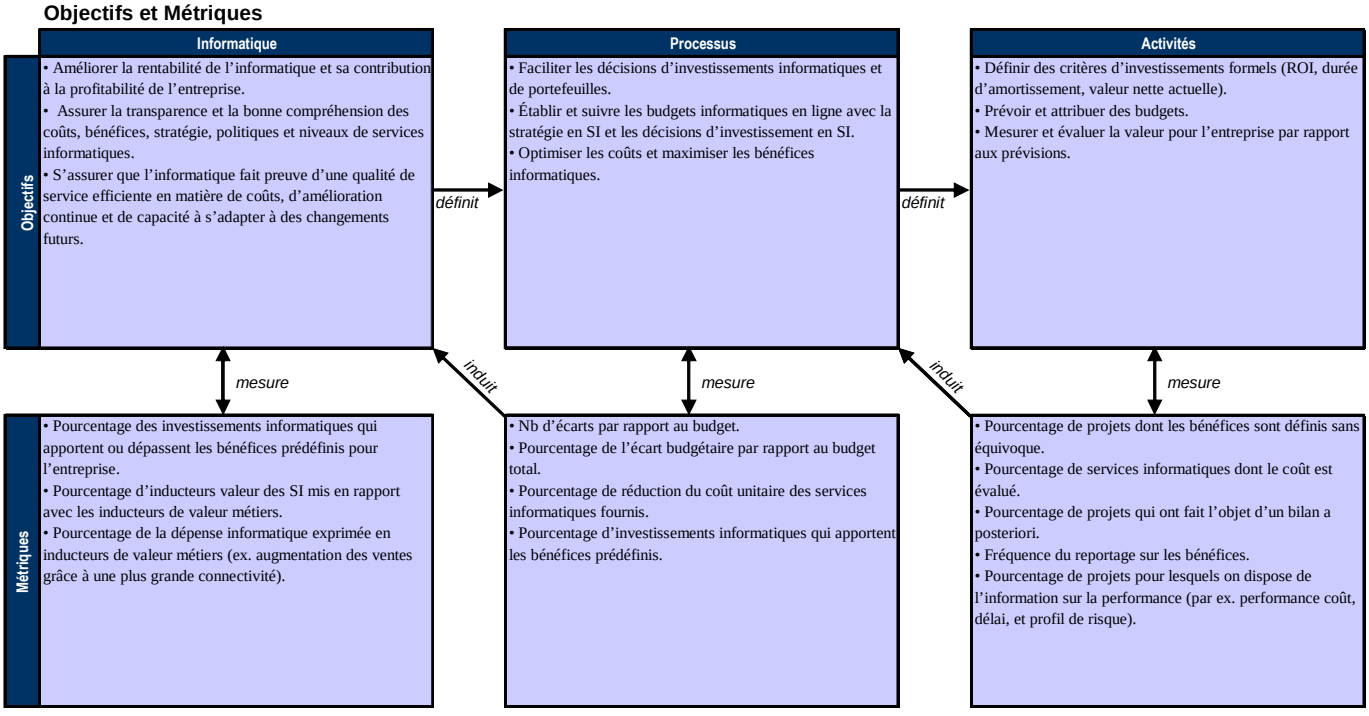
Sorties	Vers						
Rapports coûts/bénéfices	PO1	AI2	DS6	SE1	SE4		
Budgets informatiques	DS6						
Portefeuille actualisé des services SI	DS1						
Portefeuille actualisé des projets SI	PO10						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Tenir à jour le portefeuille de programmes.	A	R	R	R	C					I	I
Tenir à jour le portefeuille de projets.	I	C	A/R	A/R	C		C	C		C	I
Tenir à jour le portefeuille de services.	I	C	A/R	A/R	C	C				C	I
Mettre en place et tenir à jour le processus de budgétisation informatique.	I	C	C	A		C	C	C	R	C	
Identifier, communiquer et surveiller les investissements, les coûts et la valeur des SI pour l'entreprise.	I	C	C	A/R		C	C	C	R	C	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO5 Gérer les investissements informatiques

La gestion du processus *Gérer les investissements informatiques* qui répond à l'exigence des métiers vis-à-vis de l'informatique *améliorer constamment et de façon démontrable la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise avec des services intégrés et standardisés qui satisfont les attentes des utilisateurs finaux* est :

0 Inexistante quand

Il n'y a pas de prise de conscience de l'importance du choix des investissements informatiques et de leur budgétisation. Il n'y a ni suivi ni surveillance des investissements et des dépenses informatiques.

1 Initialisée, au cas par cas quand

L'entreprise reconnaît le besoin de gérer les investissements informatiques, mais ce besoin n'est pas régulièrement communiqué. L'attribution de la responsabilité du choix des investissements et de l'élaboration du budget informatique se fait au cas par cas. On trouve isolément des choix d'investissements et des budgets informatiques documentés de façon informelle. Les investissements informatiques sont justifiés au cas par cas. Certaines décisions budgétaires sont prises de façon circonstancielle pour répondre à des besoins opérationnels.

2 Reproductible mais intuitive quand

Le besoin de faire des choix d'investissements et d'établir un budget informatique est implicitement compris. On communique sur le besoin d'un processus de choix et de gestion budgétaire. La conformité dépend d'initiatives individuelles. On voit émerger des techniques communes pour développer des composantes du budget informatique. On prend des décisions budgétaires au coup par coup.

3 Définie quand

Les politiques et les processus d'investissements et de gestion budgétaire sont définis, documentés et communiqués, et prennent en compte les aspects métiers et technologiques essentiels. Le budget informatique est en ligne avec le plan stratégique informatique et avec celui de l'entreprise. Les processus d'établissement du budget et de choix des investissements informatiques sont formalisés, documentés et communiqués. Une formation formelle est mise en place mais elle reste principalement basée sur des initiatives individuelles. On formalise l'approbation des choix budgétaires et d'investissements informatiques. Le personnel informatique a les connaissances et les compétences nécessaires pour établir le budget informatique et recommander les investissements appropriés.

4 Gérée et mesurable quand

La responsabilité fonctionnelle et la responsabilité finale des choix d'investissements et du budget est confiée à une personne précise. On relève les écarts par rapport au budget et on y remédie. Une analyse formelle est effectuée et rend compte des coûts directs et indirects des opérations en cours aussi bien que des investissements proposés ; elle prend en compte tous les coûts du cycle de vie. On utilise un processus de gestion budgétaire normalisée et capable d'anticiper. On constate dans les plans d'investissement un glissement des coûts de développement et d'exploitation des des matériels et logiciels au profit de l'intégration des systèmes et des ressources humaines informatiques. On calcule les bénéfices et autres avantages en termes à la fois financiers et non financiers.

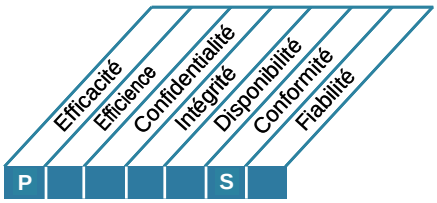
5 Optimisée quand

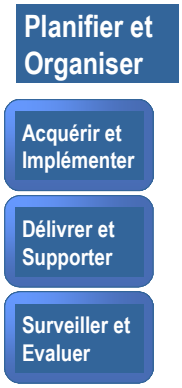
On utilise les meilleures pratiques de la profession pour étalonner les coûts et susciter des approches susceptibles d'améliorer l'efficacité des investissements. On analyse les nouveautés technologiques pour opérer les choix d'investissements et établir les budgets. Le processus de gestion des investissements est continuellement amélioré en fonction de l'analyse des performances réelles des investissements. Les décisions d'investissement tiennent compte des tendances à l'amélioration du rapport prix/performance. On cherche et on évalue méthodiquement des alternatives de financement dans le contexte existant de la structure du capital de l'entreprise, en utilisant des méthodes d'évaluation formelles. On indentifie les variations de façon proactive. On tient compte dans les décisions d'investissements d'une analyse à long terme des coûts et des bénéfices pour un cycle de vie complet

DESCRIPTION DU PROCESSUS

PO6 Faire connaître les buts et orientations du management

Le management développe un cadre de contrôle des SI pour l'entreprise, définit et communique les politiques. Il met en place un programme de communication permanent, approuvé et soutenu par le management, pour articuler la mission, les objectifs de fourniture de services, les politiques et les procédures, etc. Cette communication apporte son soutien aux objectifs informatiques et s'assure qu'on est attentif aux risques, aux objectifs et aux orientations métiers et informatique et qu'on les comprend. Ce processus s'assure de la conformité aux lois et règlements qui s'appliquent à lui.





Le contrôle du processus informatique

Faire connaître les buts et les orientations du management

qui répond à l'exigence des métiers vis-à-vis de l'informatique

obtenir des informations précises et en temps utile sur les services informatiques actuels et futurs, et sur les risques et les responsabilités associés

en se concentrant sur

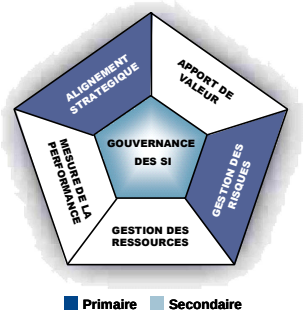
la fourniture aux parties prenantes de politiques, procédures, lignes directrices et autres éléments d'information compréhensibles et approuvés, à l'intérieur d'un cadre de contrôle des SI

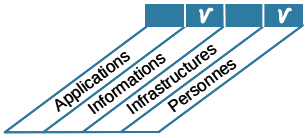
atteint son objectif en

- définissant un cadre de contrôle pour les processus informatiques
- développant et déployant des politiques informatiques
- appliquant les politiques informatiques

et est mesuré par

- le nombre de perturbations des activités du fait de perturbations des services informatiques
- le pourcentage de parties prenantes qui comprennent le cadre de contrôle des SI de l'entreprise
- le pourcentage de parties prenantes qui ne se conforment pas à la politique





OBJECTIFS DE CONTRÔLE

PO6 Faire connaître les buts et orientations du management

PO6.1 Politique informatique et environnement de contrôle
Définir les éléments d'un environnement de contrôle des SI en ligne avec la philosophie de management et le style de fonctionnement de l'entreprise. Parmi ces éléments on doit trouver les attentes/exigences d'apport de valeur des investissements informatiques, l'appétence pour le risque, l'intégrité, les valeurs éthiques, la compétence du personnel, les responsabilités opérationnelles et finales. L'environnement de contrôle est basé sur une culture dont les principes sont l'apport de valeur tout en gérant les risques significatifs, l'encouragement à la coopération entre services et au travail d'équipe, la promotion de la conformité et de l'amélioration permanente des processus, et la bonne prise en main des anomalies de fonctionnement (ou des échecs) des processus.

PO6.2 Risque informatique pour l'entreprise et cadre de contrôle
Développer et maintenir à jour un cadre de référence qui définit l'approche globale de l'entreprise vis-à-vis du risque informatique et de son contrôle. Ce cadre est aligné sur la politique informatique et son environnement de contrôle ainsi que sur le référentiel de risque et de contrôle de l'entreprise.

PO6.3 Gestion des politiques informatiques
Développer et tenir à jour un ensemble de politiques à l'appui de la stratégie SI. Ces politiques doivent préciser leurs objectifs, comporter des rôles et responsabilités, des processus de gestion des exceptions, une approche conformité et des références aux procédures, aux standards et aux lignes directrices. Leur pertinence doit être régulièrement confirmée et approuvée.

PO6.4 Déploiement des politiques, des standards et des procédures
Déployer et faire respecter par tout le personnel concerné des politiques informatiques. Elles font partie intégrante du fonctionnement de l'entreprise.

PO6.5 Communication des objectifs et des orientations informatiques
Sensibiliser et faire comprendre les objectifs et les orientations informatiques aux parties prenantes et utilisateurs concernés dans l'ensemble de l'entreprise.

GUIDE DE MANAGEMENT

PO6 Faire connaître les buts et orientations du management

De	Entrées
PO1	Plans informatiques stratégiques et tactiques, portefeuilles de projets et de services
PO9	Guide de gestion des risques liés aux SI
SE2	Rapport sur l'efficacité des contrôles des SI

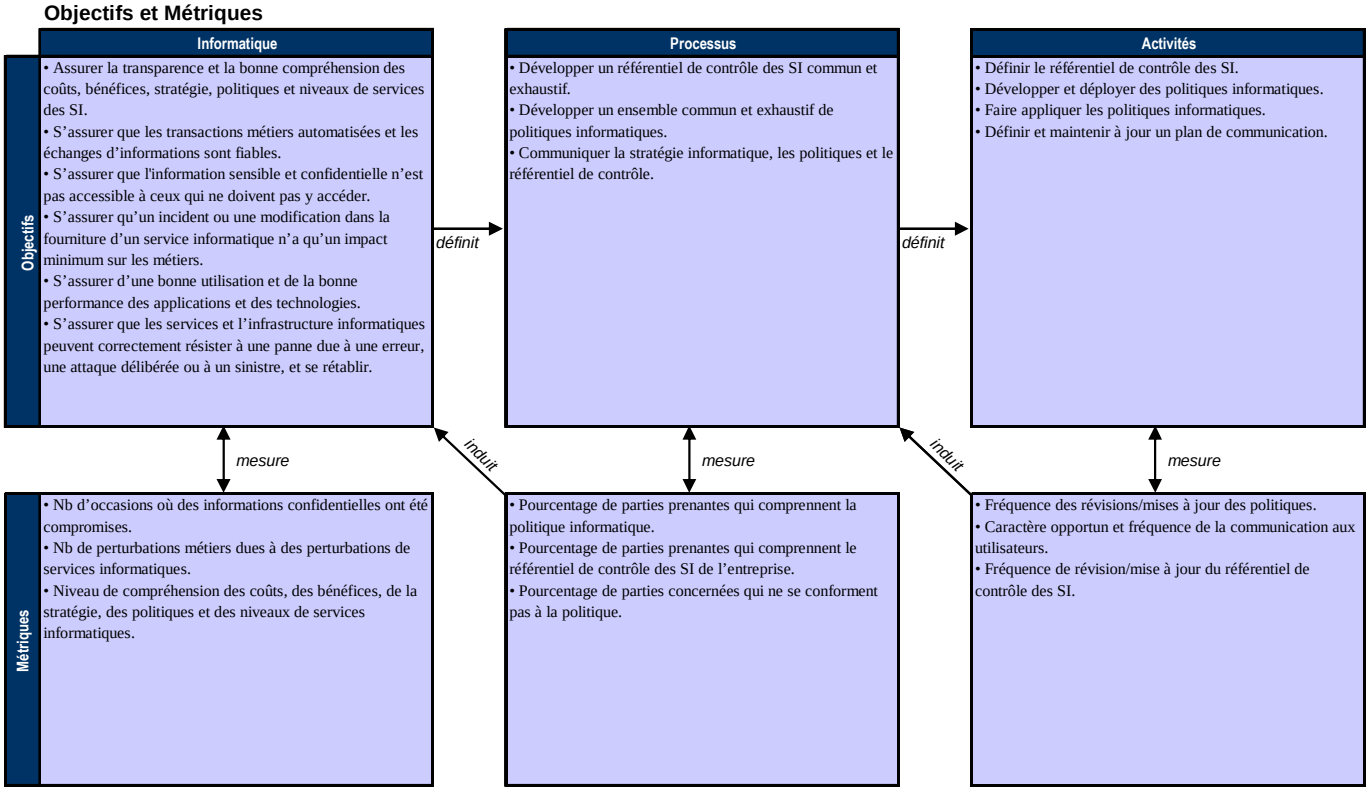
Sorties	Vers
Référentiel de contrôle des SI de l'entreprise	Tous
Politiques informatiques	Tous

Tableau RACI

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Mettre en place et maintenir opérationnels un environnement et un référentiel de contrôle informatique.	I	C	I	A/R	I	C		C	C		C
Développer et actualiser les politiques informatiques.	I	I	I	A/R		C	C	C	R		C
Communiquer le référentiel de contrôle, les objectifs et les orientations des SI.	I	I	I	A/R					R		C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO6 Faire connaître les buts et orientations du management

La gestion du processus *Faire connaître les buts et orientations du management* qui répond à l'exigence des métiers vis-à-vis de l'informatique *obtenir des informations précises et en temps utile sur les services informatiques actuels et futurs, et sur les risques et les responsabilités associés* est :

0 Inexistante quand

Le management n'a pas mis en place un environnement de contrôle de l'informatique positif. On ne reconnaît pas encore le besoin d'établir un ensemble de processus de mise en œuvre des politiques, des plans et procédures, et de la mise en conformité.

1 Initialisée, au cas par cas quand

Le management ne prend en compte les exigences d'un environnement de contrôle de l'information qu'en réaction aux circonstances. On établit et on communique les politiques, les procédures et les standards selon les besoins, au fur et à mesure qu'ils se font jour. Les processus de développement, de communication et de mise en conformité sont informels et incohérents.

2 Reproductible mais intuitive quand

Le management comprend implicitement les besoins et les exigences d'un environnement de contrôle de l'information efficace, mais les pratiques restent largement informelles. Le management a fait connaître le besoin de politiques, de plans et de procédures de contrôle, mais leur développement est laissé à l'initiative de chaque responsable et de certaines entités de l'entreprise. On reconnaît qu'une politique de qualité est philosophiquement souhaitable, mais les pratiques sont laissées à la discrétion de chaque responsable. La formation elle aussi se fait sur la base de besoins identifiés de façon individuelle.

3 Définie quand

Le management développe, documente et communique un environnement complet du contrôle de l'information et de la gestion de la qualité qui inclut un cadre de référence pour les politiques, les plans et procédures. Le processus de développement des politiques est structuré, tenu à jour, et connu du personnel, et les politiques, plans et procédures existants sont raisonnablement fiables et s'appliquent aux questions essentielles. Le management met l'accent sur l'importance de la sensibilisation à la sécurité des SI, et a lancé des programmes de sensibilisation sur ce thème. Une formation formelle pour soutenir l'environnement de contrôle de l'information existe, mais elle n'est pas mise en œuvre de façon rigoureuse. Lorsqu'il existe un cadre de référence général pour le développement de politiques et de procédures de contrôle, la surveillance de la conformité à ces politiques et à ces procédures n'est pas régulière. Il existe un cadre de référence général de développement. On a formalisé et standardisé des techniques pour promouvoir la sensibilisation à la sécurité.

4 Gérée et mesurable quand

Le management accepte la responsabilité de communiquer les politiques de contrôle interne, délègue les responsabilités et attribue suffisamment de ressources pour que l'environnement puisse s'adapter à des changements importants. On a créé un environnement de contrôle de l'information positif et proactif et on s'est engagé sur la voie de la sensibilisation aux questions de qualité et de sécurité de l'information. On développe, tient à jour et communique un ensemble complet de politiques, de plans et procédures constitué des bonnes pratiques internes. On établit un cadre de déploiement qui comporte les vérifications de conformité nécessaires.

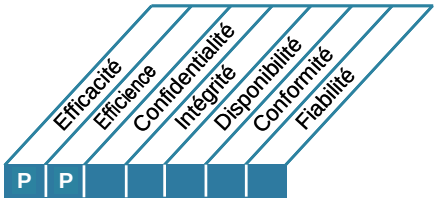
5 Optimisée quand

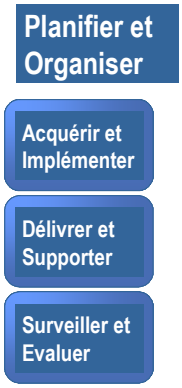
L'environnement de contrôle de l'information est en ligne avec la vision stratégique générale et avec le cadre de gestion de cette stratégie ; il est fréquemment révisé, mis à jour, et constamment amélioré. Des experts internes et externes sont désignés pour s'assurer qu'on utilise les meilleures pratiques de la profession en ce qui concerne la conduite du contrôle et les techniques de communication. Les processus de surveillance, d'auto évaluation, et de vérification de la conformité ont pénétré toute l'entreprise. On utilise l'informatique pour tenir à jour les bases de connaissances sur les politiques et sur la sensibilisation, et pour optimiser la communication grâce à la bureautique et aux outils de formation sur ordinateur.

DESCRIPTION DU PROCESSUS

PO7 Gérer les ressources humaines de l'informatique

Engager et conserver des collaborateurs compétents pour la création et la fourniture de services informatiques à l'entreprise. Pour y arriver il faut suivre des pratiques définies et approuvées en matière de recrutement, de formation, d'évaluation, de promotion, et de départ. Ce processus est critique car les personnes constituent un actif important, et la gouvernance et l'environnement de contrôle interne dépendent énormément de la motivation et de la compétence du personnel.





Le contrôle du processus informatique

Gérer les ressources humaines de l'informatique

qui répond à l'exigence des métiers vis-à-vis de l'informatique

disposer de personnes compétentes et motivées pour créer et fournir des services informatiques

en se concentrant sur

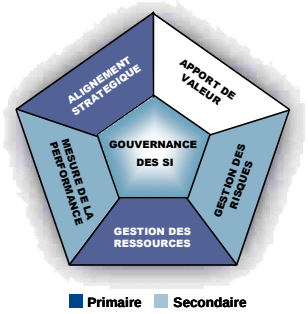
l'embauche et la formation du personnel, sa motivation par des plans de carrières clairs, l'attribution de rôles qui correspondent à sa compétence, l'établissement d'un processus d'évaluation défini, la création de fiches de postes et la surveillance à ne pas dépendre de personnes clés

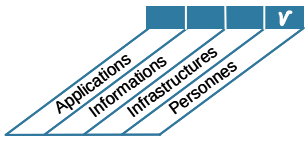
atteint son objectif en

- évaluant les performances du personnel
- embauchant et en formant du personnel informatique pour faire avancer les plans tactiques
- minimisant les risques d'une dépendance excessive vis-à-vis de ressources clés

et est mesuré par

- le niveau de satisfaction des parties prenantes de l'expertise et des compétences du personnel informatique
- le taux de turnover du personnel informatique
- le pourcentage d'informaticiens dont les diplômes sont en adéquation avec les besoins des différents postes





OBJECTIFS DE CONTRÔLE

PO7 Gérer les ressources humaines de l'informatique

PO7.1 Recrutement et maintien du personnel
Aligner les processus de recrutement du personnel informatique sur les politiques et les procédures globales de l'entreprise (ex. embauche, environnement de travail favorable, orientation). Mettre en place des processus pour s'assurer que le personnel informatique est déployé comme il convient dans l'entreprise et qu'il a les compétences nécessaires pour permettre à l'entreprise d'atteindre ses objectifs.

PO7.2 Compétences du personnel
Vérifier régulièrement que le personnel a les compétences nécessaires pour remplir son rôle en fonction de son instruction, formation et/ou expérience. Définir les besoins en compétences informatiques fondamentales et vérifier qu'ils sont satisfaits en utilisant des programmes de qualification et de certification si c'est utile.

PO7.3 Affectation des rôles
Définir, surveiller et superviser des référentiels pour les rôles, les responsabilités et la rémunération du personnel, en incluant l'obligation d'adhérer aux procédures et politiques de l'entreprise, à son code d'éthique et à ses pratiques professionnelles. Le niveau de supervision doit être fonction de l'importance du poste et de l'étendue des responsabilités attribuées.

PO7.4 Formation
Bien orienter les employés des SI à l'embauche et leur dispenser la formation permanente nécessaire pour tenir à jour leurs connaissances, compétences, capacités et leur sensibilisation au contrôle interne et à la sécurité au niveau nécessaire pour permettre à l'entreprise d'atteindre ses objectifs.

PO7.5 Dépendance à l'égard d'individus
Dépendre le moins possible d'individus clés dans les secteurs essentiels grâce à l'acquisition de connaissances (documentation), au partage des connaissances, aux plans d'évolution de carrière et aux personnels de remplacement.

PO7.6 Procédures de sécurité concernant le personnel
Inclure des vérifications d'antécédents dans le processus de recrutement du personnel informatique. L'étendue et la fréquence de ces vérifications doivent être fonction du niveau de criticité et/ou de sensibilité de la fonction et s'appliquer aux employés, aux contractuels et aux fournisseurs.

PO7.7 Évaluation des performances
Exiger des évaluations appropriées et régulières par rapport à des objectifs individuels établis d'après les objectifs de l'entreprise, les standards en vigueur et les responsabilités spécifiques du poste. Les performances et le comportement des employés doivent être activement stimulés par l'accompagnement lorsque c'est approprié.

PO7. 8 Changements de postes et départs
Agir avec détermination en ce qui concerne les mouvements de personnels, en particulier les départs. Il faut organiser le transfert des connaissances, réattribuer les responsabilités et supprimer les droits d'accès, de façon à minimiser les risques et à garantir la continuité de la fonction.

GUIDE DE MANAGEMENT

PO7 Gérer les ressources humaines de l'informatique

De	Entrées
PO4	Documentation relative à l'organisation, aux relations, aux rôles et responsabilités des SI
AI1	Étude de faisabilité des exigences des métiers

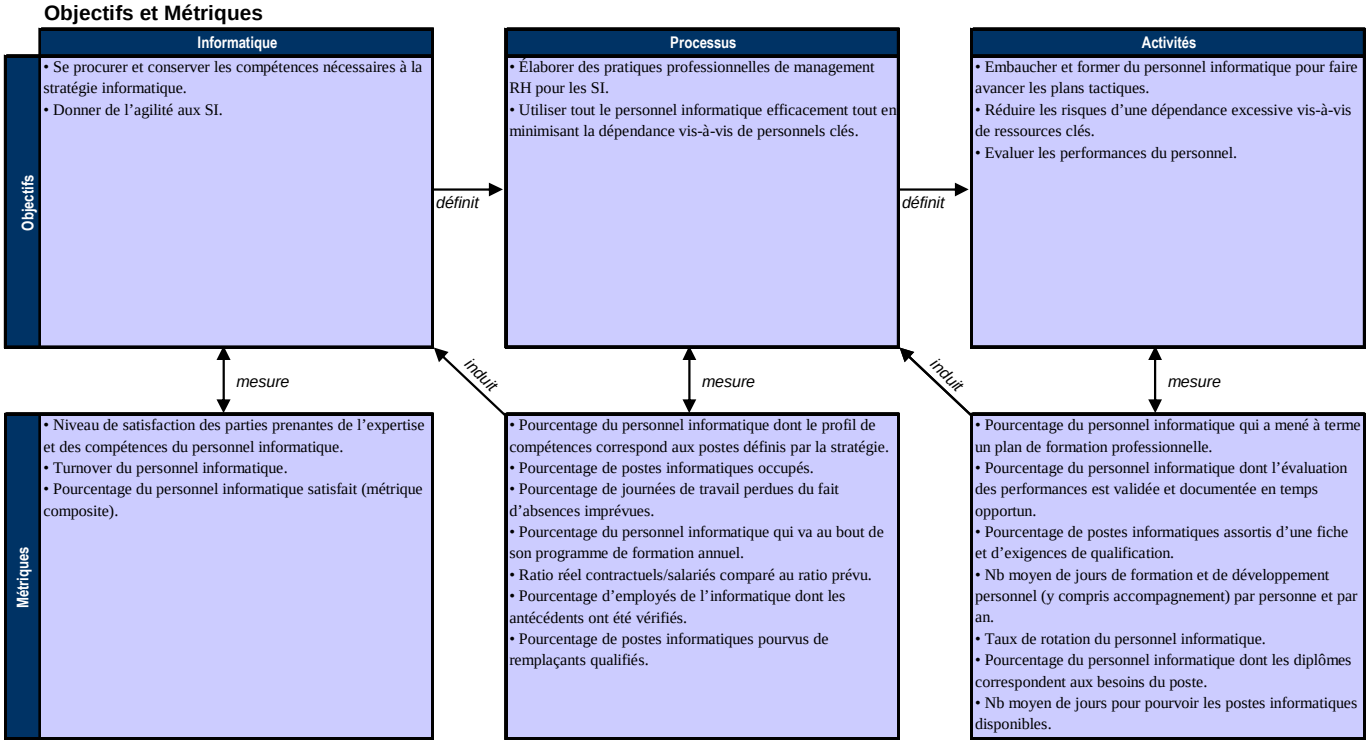
Sorties	Vers						
Politiques et procédures RH des SI	PO4						
Tableau des compétences SI	PO4	PO10					
Fiches de poste	PO4						
Compétences et connaissances des utilisateurs et formation individuelle	DS7						
Besoins spécifiques de formation	DS7						
Rôles et responsabilités	Tous						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Identifier les compétences informatiques, les fiches de postes, l'éventail des salaires et les tests comparatifs de performance personnelle.		C		A		C	C	C	R	C	
Appliquer les politiques RH et les procédures particulières aux SI (recrutement, embauche, approbation, rémunération, formation, évaluation, promotion et licenciement).				A		R	R	R	R	R	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO7 Gérer les ressources humaines de l'informatique

La gestion du processus *Gérer les ressources humaines de l'informatique* qui répond à l'exigence des métiers vis-à-vis de l'informatique *disposer de personnes compétentes et motivées pour créer et fournir des services informatiques* est :

0 Inexistante quand

Il n'y a pas de prise de conscience de l'importance qu'il y a pour l'entreprise à mettre en cohérence la gestion des ressources humaines de l'informatique avec le processus de planification informatique. Personne, individuellement ou en groupe, n'est formellement responsable de la gestion des ressources humaines de l'informatique.

1 Initialisée, au cas par cas quand

Le management admet le besoin de gérer les ressources humaines informatiques. Le processus de gestion des ressources humaines de l'informatique est informel et dépend des circonstances. Il est axé sur l'activité d'embauche et de gestion du personnel informatique. Il y a cependant une prise de conscience de l'impact qu'ont les modifications rapides de l'entreprise et des technologies, ainsi que la complexité de plus en plus grande des solutions sur le besoin de nouvelles expertises et de compétences.

2 Reproductible mais intuitive quand

Il y a une approche tactique de l'embauche et de la gestion du personnel informatique, inspirée par les besoins de projets spécifiques plutôt que par la recherche d'un bon équilibre entre les compétences internes et externes. Le nouveau personnel bénéficie d'une formation informelle, puis de formations adaptées aux circonstances.

3 Définie quand

Il existe un processus défini et documenté pour la gestion des ressources humaines de l'informatique. Il existe un plan de gestion des ressources humaines de l'informatique. Il y a une approche stratégique de l'embauche et de la gestion du personnel informatique. On a conçu un programme formel de formation pour faire face aux besoins des ressources humaines de l'informatique. On a mis en place un plan de formation alterné, destiné à développer aussi bien les compétences métiers que les compétences techniques.

4 Gérée et mesurable quand

On a confié spécifiquement à une personne ou à un groupe doté(e) de l'expérience et des compétences requises, la responsabilité de développer et de maintenir opérationnel le plan de gestion des ressources humaines de l'informatique. Le processus de développement et de gestion du plan de gestion des ressources humaines de l'informatique est réactif aux changements. L'entreprise dispose de mesures standards qui lui permettent de faire ressortir les écarts par rapport au plan de gestion des ressources humaines de l'informatique, avec une attention particulière pour la gestion de la croissance des effectifs et du turnover. On met en place des analyses des rémunérations et des compétences et on les compare aux bonnes pratiques des autres DSI et des autres entreprises de la branche. La gestion des ressources humaines est proactive, et prend en compte les plans de développement de carrière.

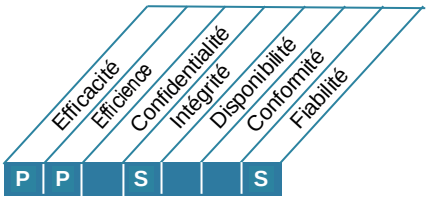
5 Optimisée quand

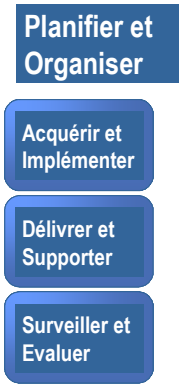
Le plan de gestion des ressources humaines de l'informatique est continuellement actualisé pour faire face aux besoins d'évolution de l'entreprise. La gestion des ressources humaines de l'informatique fait partie du plan informatique, assurant le développement et l'utilisation optimum des compétences informatiques disponibles. La gestion des ressources humaines de l'informatique fait partie des orientations stratégiques de l'entreprise et réagit à leur évolution. Les composantes de cette gestion telles que rémunération, évaluation des performances, participation à des forums professionnels, transfert de connaissances, formation et suivi individuel, sont conformes aux meilleures pratiques en vigueur dans la branche. On met en place des programmes de formation avant tout déploiement de nouveaux produits ou de nouvelles normes techniques dans l'entreprise.

DESCRIPTION DU PROCESSUS

PO8 Gérer la qualité

Un système de gestion de la qualité est développé et actualisé, ce qui implique des processus et des standards de développement et d'achat éprouvés. Ceci est rendu possible par la planification, la mise en place et l'actualisation d'un système de gestion de la qualité, et par des exigences, des procédures et des politiques de qualité clairement définies. Les exigences de qualité doivent être énoncées et communiquées au travers d'indicateurs quantifiables et réalistes. L'amélioration permanente s'obtient par une surveillance continue, l'analyse des écarts et leur correction, et la communication des résultats aux parties prenantes. La gestion de la qualité est essentielle pour s'assurer que l'informatique apporte de la valeur à l'entreprise, une amélioration continue et une transparence vis-à-vis des parties prenantes.





Le contrôle du processus informatique

Gérer la qualité

qui répond à l'exigence des métiers vis-à-vis de l'informatique

d'assurer une amélioration continue et mesurable de la qualité des services informatiques fournis

en se concentrant sur

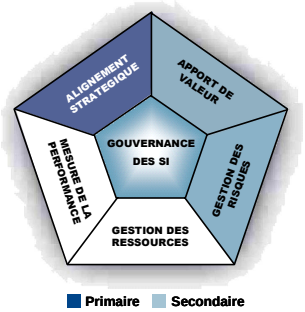
la définition d'un système de gestion de la qualité (SGQ), la surveillance permanente de la performance comparée aux objectifs et la mise en place d'un programme d'amélioration permanente des services informatiques

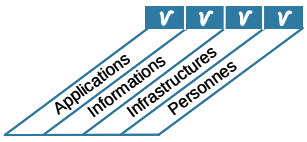
atteint son objectif en

- définissant des standards et des pratiques de qualité
- surveillant et révisant les performances internes et externes par rapport aux standards et pratiques de qualité définis
- améliorant le système de gestion de la qualité de façon permanente

et est mesuré par

- le pourcentage de parties prenantes satisfaites de la qualité des SI (en tenant compte de leur importance)
- le pourcentage de processus informatiques formellement et périodiquement révisés par l'assurance qualité qui atteignent leur cible et leurs objectifs qualité
- le pourcentage de processus qui font l'objet d'une revue d'assurance qualité





OBJECTIFS DE CONTRÔLE

PO8 Gérer la qualité

PO8.1 Système de gestion de la qualité (SGQ)
Mettre en place et actualiser un SGQ qui offre une approche standard, formelle et continue de la gestion qualité en ligne avec les exigences des métiers. Le SGQ doit identifier les exigences et les critères qualité, les processus informatiques clés, leur ordre de succession et leurs interactions, les politiques, critères et méthodes pour définir, détecter, corriger et prévenir les défauts de conformité. Le SGQ doit définir l'organisation de la gestion qualité, avec ses rôles, ses tâches et ses responsabilités. Tous les domaines clés développent leurs plans qualité avec leurs critères et leurs politiques, en ligne avec les critères et les politiques, et enregistrent leurs données qualité. Surveiller et mesurer l'efficacité et l'adoption du SGQ et l'améliorer lorsque c'est nécessaire.

PO8.2 Standards informatiques et pratiques qualité
Identifier et actualiser les standards, les procédures et les pratiques pour les processus clés pour guider l'entreprise vers l'objectif du SGQ. Utiliser les meilleures pratiques de la branche comme référence lorsqu'on adapte et qu'on améliore les pratiques qualité de l'entreprise.

PO8.3 Standards de développement et d'acquisition
Adopter et actualiser les standards pour tous les développements et acquisitions qui suivent le cycle de vie du livrable définitif et qui exigent un aval à chaque étape clé selon des critères d'agrément convenus. Prendre en compte les standards de codification des logiciels, conventions de nommage, formats de fichiers, standards de conception de schémas et de dictionnaires de données, standards d'interfaces utilisateurs, interopérabilité, efficience des performances des systèmes, capacité de mise à l'échelle, standards de développement et de tests, validation par rapport aux demandes, plans de tests et tests unitaires, de régression et d'intégration.

PO8.4 Orientation client
Orienter la gestion qualité vers les clients en déterminant leurs besoins et en alignant ces derniers sur les standards et les pratiques informatiques. Définir les rôles et les responsabilités concernant la résolution de conflits entre l'utilisateur/client et l'informatique.

PO8.5 Amélioration continue
Actualiser et communiquer régulièrement un plan général qualité qui promeut l'amélioration continue de la qualité.

PO8.6 Mesure, surveillance et revue qualité
Définir, planifier et mettre en place un système de mesure pour surveiller en continu la conformité au SGQ, ainsi que la valeur apportée par celui-ci. Le propriétaire du processus doit mesurer, surveiller et enregistrer les informations pour pouvoir décider des actions correctives et préventives appropriées.

GUIDE DE MANAGEMENT

PO8 Gérer la qualité

De	Entrées
PO1	Plan informatique stratégique
PO10	Plans détaillés des projets
SE1	Plans d'actions correctives

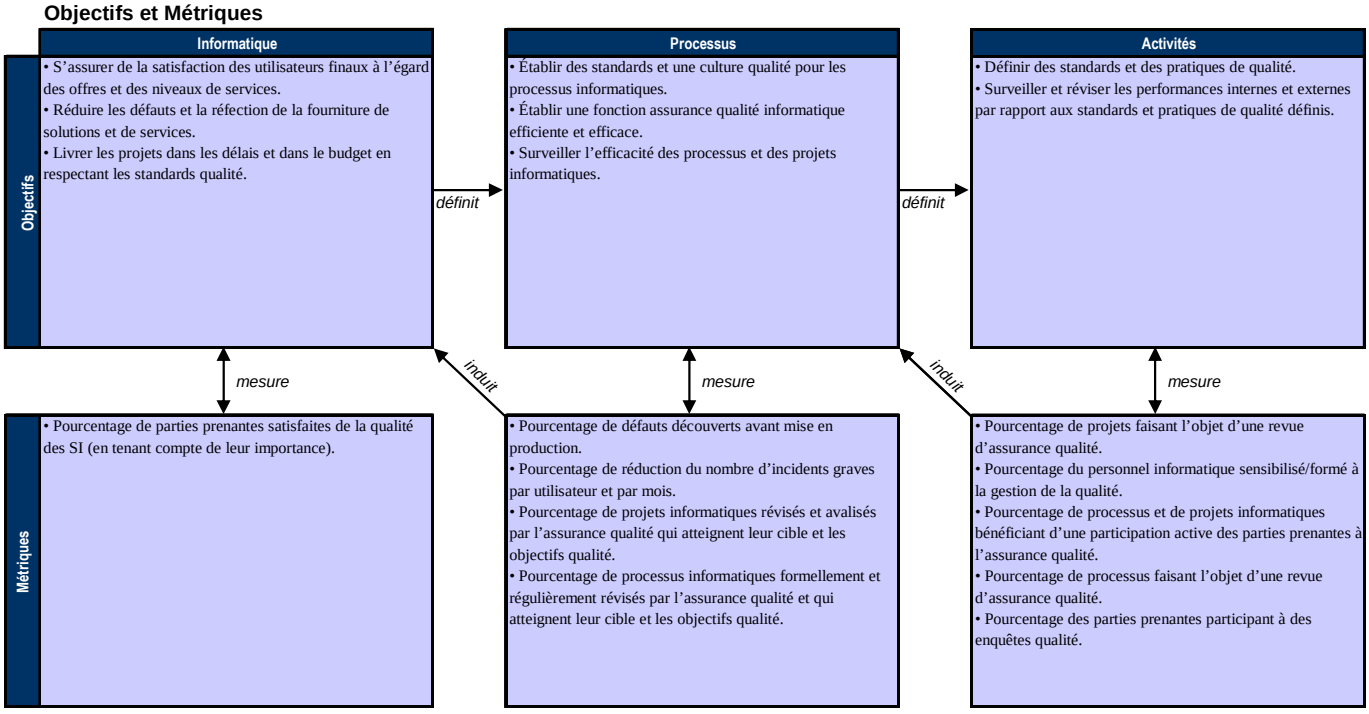
Sorties	Vers						
Standards d'acquisition	AI1	AI2	AI3	AI5	DS2		
Standards de développement	PO10	AI1	AI2	AI3	AI7		
Exigences de standards de qualité et de métriques	Tous						
Actions pour l'amélioration de la qualité	PO4	AI6					

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir un système de gestion qualité (SGQ).	C		C	A/R	I	I	I	I	I	I	C
Mettre en place et actualiser un SGQ.	I	I	I	A/R	I	C	C	C	C	C	C
Bâtir et communiquer des standards qualité dans toute l'entreprise.		I		A/R	I	C	C	C	C	C	C
Bâtir et gérer le plan qualité pour l'amélioration continue.				A/R	I	C	C	C	C	C	C
Mesurer, surveiller et réviser la conformité avec les objectifs qualité.				A/R	I	C	C	C	C	C	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO8 Gérer la qualité

La gestion du processus *Gérer la qualité* qui répond à l'exigence des métiers vis-à-vis de l'informatique *d'assurer une amélioration continue et mesurable de la qualité des services informatiques fournis* est :

0 Inexistante quand

L'entreprise ne dispose ni d'un processus de planification SGQ, ni d'une méthodologie du de gestion du cycle de vie des systèmes. Le management et le personnel informatique ne pensent pas qu'un programme qualité soit nécessaire. Les projets et les opérations ne font jamais l'objet d'une revue d'assurance qualité.

1 Initialisée, au cas par cas quand

Le management a conscience du besoin d'un SGQ. Lorsque le SGQ est mis en œuvre, c'est isolément. Le management porte des jugements informels sur la qualité.

2 Reproductible mais intuitive quand

On a lancé un programme de définition et de surveillance des activités SGQ au sein du SI. Lorsqu'elles se produisent, les démarches SGQ sont appliquées aux projets et aux initiatives orientés processus informatiques mais pas aux processus concernant l'ensemble de l'entreprise.

3 Définie quand

Un processus défini de SGQ est communiqué par le management et il concerne à la fois la gestion par l'informatique et par les utilisateurs finaux. Un programme d'enseignement et de formation voit le jour pour faire connaître la démarche qualité à tous les niveaux de l'entreprise. Les exigences qualité de base sont définies et adoptées pour les projets et au sein de l'informatique. On voit émerger des outils communs et des pratiques communes dans la gestion de la qualité. On prévoit des enquêtes de satisfaction qualité et on les fait à l'occasion.

4 Gérée et mesurable quand

Tous les processus font appel au SGQ, y compris ceux qui sont confiés à des tiers. On constitue une base de connaissances standardisée sur la mesure de la qualité. On utilise les méthodes d'analyse coûts/bénéfices pour justifier les initiatives SGQ. On commence à faire des tests comparatifs pour se situer vis-à-vis de la concurrence et du marché. Un programme d'enseignement et de formation est créé pour enseigner la démarche qualité à tous les niveaux de l'entreprise. On a standardisé les outils et les pratiques, et on utilise périodiquement l'analyse causale. On effectue régulièrement des enquêtes de satisfaction qualité. On a mis en place un programme standardisé et bien structuré de mesure de la qualité. Le management informatique est en train de constituer une base de connaissances sur la mesure de la qualité.

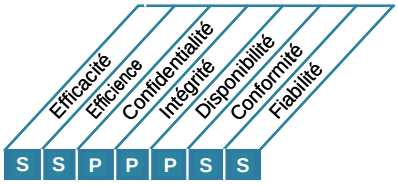
5 Optimisée quand

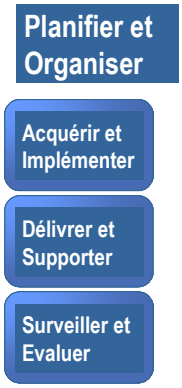
Le SGQ est intégré et appliqué par toutes les activités informatiques. Les processus d'assurance qualité sont souples et s'adaptent aux modifications de l'environnement informatique. La base de connaissances des mesures de qualité s'enrichit des meilleures pratiques constatées à l'extérieur. Les comparaisons avec les standards externes font partie de la routine. La surveillance de la satisfaction vis-à-vis de la qualité est un processus continu qui conduit à l'analyse causale et à des actions d'amélioration. Il existe une assurance formelle du niveau du processus de gestion de la qualité.

DESCRIPTION DU PROCESSUS

PO9 Évaluer et gérer les risques

Un référentiel de gestion des risques est créé et maintenu à niveau. Ce référentiel documente un niveau commun et agréé de risques informatiques, de stratégies pour les réduire et de risques résiduels. Tout impact potentiel d'un événement imprévu sur les objectifs de l'entreprise est identifié, analysé, et évalué. Des stratégies de réduction des risques sont adoptées pour ramener le risque résiduel à un niveau acceptable. Le résultat de l'évaluation est compréhensible par les parties prenantes et exprimé en termes financiers pour permettre à ces parties de préconiser le niveau de risque tolérable.





Le contrôle du processus informatique

Évaluer et gérer les risques

qui répond à l'exigence des métiers vis-à-vis de l'informatique

analyser et communiquer les risques informatiques ainsi que leur impact potentiel sur les objectifs et les processus métiers

en se concentrant sur

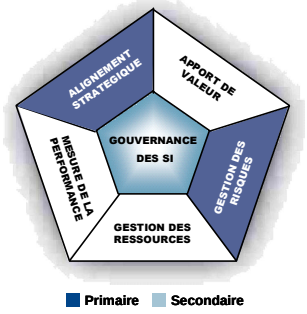
le développement d'un cadre de référence de gestion des risques, intégré à celui de la gestion des risques opérationnels, l'évaluation des risques, leur réduction et la communication des risques résiduels

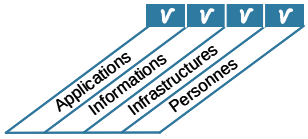
atteint son objectif en

- s'assurant que la gestion des risques est pleinement intégrée aux processus de management, en interne et en externe, et régulièrement appliquée
- procédant à l'évaluation des risques
- recommandant et en communiquant des plans d'action pour les réduire

et est mesuré par

- le pourcentage d'objectifs informatiques critiques pris en compte dans l'évaluation des risques
- le pourcentage de risques informatiques critiques pour lesquels des plans d'action ont été développés
- le pourcentage de plans d'action de gestion des risques dont la mise en œuvre a été approuvée





OBJECTIFS DE CONTRÔLE

PO9 Évaluer et gérer les risques

PO9.1 Référentiel de gestion des risques informatiques
Constituer un référentiel de gestion des risques informatiques aligné sur le référentiel de gestion des risques de l'entreprise.

PO9.2 Établissement du contexte du risque
Établir le contexte dans lequel s'applique le référentiel d'évaluation des risques pour s'assurer d'obtenir les résultats appropriés. Cela implique de déterminer le contexte interne et externe de chaque évaluation du risque, le but de l'évaluation et les critères de cette évaluation.

PO9.3 Identification des événements
Identifier les événements (un nombre important de menaces réalistes susceptibles d'exploiter un nombre significatif de vulnérabilités potentielles) qui peuvent avoir un impact négatif sur les objectifs ou les opérations de l'entreprise, dont l'activité, les aspects réglementaires et légaux, la technologie, les partenaires commerciaux, les ressources humaines et le caractère opérationnel. Déterminer la nature des impacts et maintenir à jour cette information. Établir une cartographie des risques actuels et la maintenir à jour.

PO9.4 Évaluation du risque
Évaluer régulièrement la probabilité et les conséquences de tous les risques identifiés, en utilisant des méthodes qualitatives et quantitatives. La probabilité et les conséquences associées aux risques inhérents et résiduels doivent être déterminées individuellement, par catégorie, et par portefeuille.

PO9.5 Réponse au risque
Développer et tenir à jour un processus de réponse au risque destiné à s'assurer que des contrôles économiquement rentables réduisent en permanence l'exposition au risque. La réponse au risque doit proposer des stratégies comme l'évitement, la réduction, le partage et l'acceptation. Elle doit préciser les responsabilités associées et tenir compte du niveau d'appétence aux risques.

PO9.6 Maintenance et surveillance d'un plan d'action vis-à-vis des risques
Établir les priorités et planifier les activités de contrôle à tous les niveaux pour mettre en place les réponses aux risques considérées comme nécessaires, sans oublier l'évaluation des coûts et des bénéfices, et la responsabilité de leur mise en œuvre. Rechercher l'approbation pour les actions recommandées et l'acceptation de tous les risques résiduels, et s'assurer que les propriétaires des processus affectés par le risque assument aussi la propriété des actions entreprises. Surveiller l'exécution des plans et rapporter tout écart au management.

GUIDE DE MANAGEMENT

PO9 Évaluer et gérer les risques

De	Entrées
PO1	Plans informatiques stratégiques et tactiques, portefeuille de services informatiques
PO10	Plan de gestion des risques des projets
DS2	Risques fournisseurs
DS4	Résultats des tests des plans de secours
DS5	Menaces et vulnérabilités de sécurité
SE1	Historique des événements de risque et des tendances
SE4	Appétence de l'entreprise pour le risque informatique

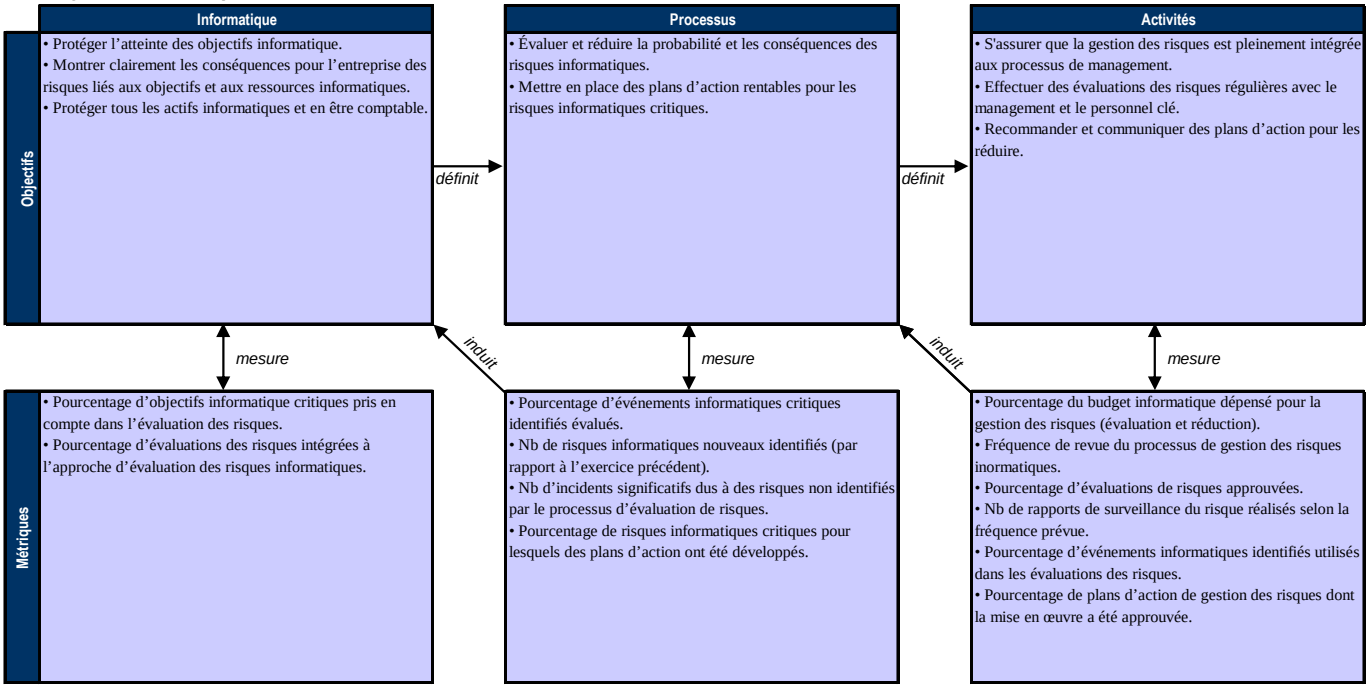
Sorties	Vers						
Évaluations des risques	PO1	DS4	DS5	DS12	SE4		
Rapports sur les risques	SE4						
Guides de gestion des risques informatiques	PO6						
Plans d'actions/solutions risques informatiques	PO4	AI6					

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Déterminer l'alignement pour la gestion des risques (ex. évaluer les risques).	A	R/A	C	C	R/A	I					I
Identifier les objectifs métiers stratégiques concernés.		C	C	R/A	C	C					I
Identifier les objectifs processus métiers concernés.				C	C	R/A					I
Identifier les objectifs informatiques internes et établir leur contexte risque.					R/A		C	C	C		I
Identifier les événements associés aux objectifs [certains événements sont orientés métiers (métier : A) ; certains sont orientés informatique (Informatique : A, métier : C)].	I			A/C	A	R	R	R	R		C
Évaluer les risques associés aux événements.				A/C	A	R	R	R	R		C
Évaluer les réponses aux risques.	I	I	A	A/C	A	R	R	R	R		C
Planifier les activités de contrôle en tenant compte des priorités.	C	C	A	A	R	R	C	C	C		C
Approuver les plans d'action de traitement des risques et en assurer le financement.		A	A		R	I	I	I	I		I
Tenir à jour et surveiller un plan d'action de traitement des risques.	A	C	I	R	R	C	C	C	C	C	R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO9 Évaluer et gérer les risques

La gestion du processus *Évaluer et gérer les risques* qui répond à l'exigence des métiers vis-à-vis de l'informatique *analyser et communiquer les risques informatiques ainsi que leur impact potentiel sur les objectifs et les processus métiers* est :

0 Inexistante quand

On ne fait pas d'évaluation des risques liés aux processus ou aux décisions métiers. L'entreprise ne prend pas en compte les conséquences pour son activité des faiblesses de sa sécurité et des incertitudes liées au développement de ses projets. La gestion des risques n'est pas identifiée comme pertinente dans l'acquisition de solutions et la livraison de services informatiques.

1 Initialisée, au cas par cas quand

Les risques informatiques sont traités au cas par cas. On fait des évaluations informelles des risques projet selon une approche spécifique à chaque projet. L'évaluation des risques est parfois incluse dans un plan de projet mais elle est rarement attribuée à des responsables spécifiques. On prend en compte les risques spécifiques à l'informatique, comme la sécurité, la disponibilité et l'intégrité, à l'occasion de chaque projet. On aborde peu souvent lors des réunions de direction les risques informatiques liés à l'exploitation quotidienne. Lorsque c'est le cas, la réduction de ces risques n'est pas cohérente. On comprend de mieux en mieux l'importance des risques liés à l'informatique, et la nécessité d'en tenir compte.

2 Reproductible mais intuitive quand

On commence à développer une approche encore embryonnaire de l'évaluation des risques et elle se met en place à l'initiative des chefs de projets. La gestion des risques est généralement mise en œuvre à un niveau élevé et ne s'applique typiquement qu'aux projets majeurs ou lorsqu'un problème surgit. Les processus de réduction des risques commencent à être mis en place lorsque certains risques ont été identifiés.

3 Définie quand

Une politique de gestion des risques définit, à l'échelle de l'entreprise, quand et comment doivent avoir lieu les évaluations. La gestion des risques suit un processus défini qui est documenté. La formation à la gestion des risques est accessible à tout le personnel. On laisse chacun libre de décider de suivre la formation et de mettre le processus en œuvre. La méthodologie d'évaluation des risques est convaincante et solide, et permet d'identifier presque à coup sûr les risques essentiels encourus par l'entreprise. On institue en général un processus de réduction des risques lorsque ceux-ci sont identifiés. Les fiches de poste prennent en compte les responsabilités de gestion des risques.

4 Gérée et mesurable quand

L'évaluation et la gestion des risques sont des procédures standard. On rapporte à la direction informatique les cas qui échappent au processus de gestion des risques. La gestion des risques informatiques est sous la responsabilité d'un cadre supérieur. On évalue et on réduit les risques aussi bien au niveau de chaque projet que, régulièrement, au niveau général de l'exploitation informatique. Le management est avisé des modifications de l'environnement métiers et informatique qui pourraient affecter de façon significative les scénarios de risques informatiques. Le management est capable de surveiller l'exposition au risque et de décider en toute connaissance de cause du niveau de risque acceptable. Tous les risques identifiés ont un propriétaire désigné, et la direction générale détermine avec la direction des systèmes d'information les niveaux de risques tolérables par l'entreprise. La DSI conçoit des mesures standard pour évaluer les risques et définir les ratios risques/bénéfices. Le management budgétise un projet de gestion des risques opérationnels pour réévaluer les risques de façon régulière. On a créé une base de donnée dédiée à la gestion des risques et une partie des processus de gestion des risques commence à être automatisée. La DSI envisage des stratégies de réduction des risques.

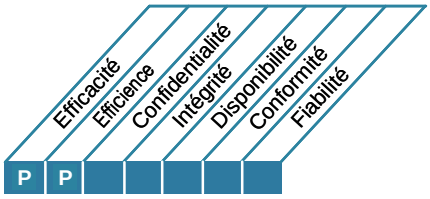
5 Optimisée quand

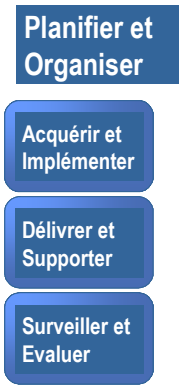
La gestion des risques a atteint le stade d'un processus structuré bien appliqué et bien géré dans toute l'entreprise. On applique les bonnes pratiques dans l'ensemble de l'entreprise. La capture, l'analyse et le reportage sur les informations de gestion des risques sont largement automatisés. On s'inspire des leaders dans le domaine, et l'informatique partage son expérience avec ses pairs. La gestion des risques est véritablement intégrée dans toutes les activités métiers et informatique ; elle est bien acceptée, et implique largement les utilisateurs des services informatiques. Le management détecte toute décision opérationnelle ou d'investissement majeure concernant l'informatique qui ne prend pas en compte le plan de gestion des risques et agit en conséquence. Le management évalue en permanence les stratégies de réduction des risques.

DESCRIPTION DU PROCESSUS

PO10 Gérer les projets

Un programme et un cadre de référence de gestion de projets pour la gestion de tous les projets informatiques est en place. Ce cadre permet de s'assurer que tous les projets sont correctement coordonnés et que les priorités sont établies. Il prévoit un plan maître, l'attribution de ressources, la définition des livrables, l'approbation par les utilisateurs, une approche de livraison par étapes, une assurance qualité, un plan de tests formalisé, des tests et une revue après mise en place pour s'assurer que la gestion des risques et que l'apport de valeur à l'entreprise sont effectives. Cette approche réduit les risques de coûts non prévus et d'annulation de projets, améliore la communication en direction des métiers et des utilisateurs finaux ainsi que leur implication, permet d'être sûr de la valeur et de la qualité des livrables du projet, et maximise leur contribution aux programmes d'investissements informatiques.





Le contrôle du processus informatique

Gérer les projets

qui répond à l'exigence des métiers vis-à-vis de l'informatique

livrer des projets conformes aux délais, aux coûts et à la qualité prévus

en se concentrant sur

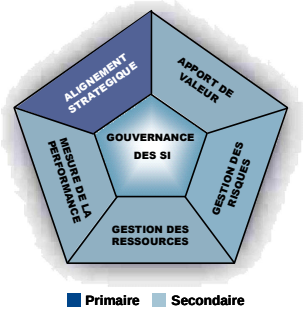
un programme défini et une approche de la gestion de projets qui s'appliquent aux projets informatiques, et permettent aux parties prenantes de s'impliquer et de surveiller les risques et l'avancement des projets

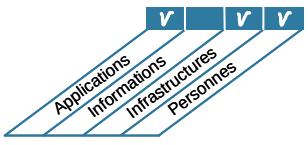
atteint son objectif en

- définissant et en appliquant des cadres et des approches pour les programmes et les projets
- diffusant des guides de gestion de projets
- utilisant la planification de projets pour chaque projet détaillé dans le portefeuille de projets

et est mesuré par

- le pourcentage de projets qui répondent aux attentes des parties prenantes (délais, coûts, conformité aux attentes, pondérés selon leur importance relative)
- le pourcentage de projets qui ont été révisés après leur mise en place
- le pourcentage de projets qui respectent les standards et les pratiques de la gestion de projet





OBJECTIFS DE CONTRÔLE

PO10 Gérer les projets

PO10.1 Référentiel de gestion de programme
Tenir à jour le programme des projets, en relation avec le portefeuille des programmes d'investissements informatiques, en identifiant, définissant, évaluant, sélectionnant, initiant et contrôlant ces projets, et en établissant leurs priorités respectives. S'assurer que les projets servent les objectifs du programme. Coordonner les activités et l'interdépendance de multiples projets, gérer la contribution de tous les projets aux résultats attendus au sein du programme, et résoudre les problèmes et les conflits liés aux ressources.

PO10.2 Référentiel de gestion de projet
Mettre en place et tenir à jour un référentiel de gestion de projets qui définit aussi bien l'étendue et les limites de la gestion de projets que la méthode à adopter et à appliquer pour chaque projet entrepris. Le référentiel et les méthodologies qui l'appuient doivent être intégrés aux processus de gestion de programmes.

PO10.3 Approche gestion de projet
Établir une approche de gestion de projet en rapport avec la taille, la complexité et les exigences réglementaires de chaque projet. La structure de gouvernance des projets peut comporter les rôles, responsabilités opérationnelles et finales du commanditaire du programme, des commanditaires des projets, du comité de pilotage, du bureau des projets et du chef de projet, ainsi que les mécanismes grâce auxquels ils peuvent faire face à ces responsabilités (comme le reporting et les revues d'étapes). Vérifier que chaque projet informatique est doté d'un commanditaire assez haut placé pour être propriétaire de la mise en œuvre du projet au sein du programme stratégique général.

PO10.4 Implication des parties prenantes
Obtenir l'implication et la participation de toutes les parties prenantes concernées par la définition et la mise en œuvre du projet à l'intérieur du programme global d'investissements informatiques.

PO10.5 Énoncé du périmètre du projet
Définir et documenter la nature et l'étendue du projet pour confirmer et développer parmi les parties prenantes une compréhension commune du périmètre du projet et la façon dont il est relié aux autres projets du programme global d'investissements informatiques. Cette définition doit être formellement approuvée par les commanditaires du programme et du projet avant que ce dernier ne démarre.

PO10.6 Démarrage d'une phase du projet
Le démarrage de chaque phase principale du projet est approuvée et communiqué à toutes les parties prenantes. Fonder l'approbation de la phase de démarrage sur les décisions de la gouvernance des programmes. L'approbation des phases suivantes doit se baser sur les revues et l'acceptation des livrables de la phase précédente, ainsi que sur l'approbation d'une analyse de rentabilité mise à jour lors de la prochaine revue majeure du programme. Dans l'éventualité où des phases du projet se chevaucheraient, les commanditaires du programme et de chaque projet devraient faire le point pour autoriser l'avancement du projet.

PO10.7 Plan projet intégré
Mettre en place un plan projet intégré, formalisé et approuvé (couvrant les ressources métiers et informatiques) pour guider la mise en œuvre et le contrôle du projet tout au long de son cycle de vie. Les activités et les interdépendances de projets multiples dans un programme doivent être comprises et documentées. Le plan projet doit être tenu à jour durant toute la vie du projet. Le plan projet et les modifications qui lui sont apportés doivent être approuvés en ligne avec le cadre de gouvernance des programmes et des projets.

PO10.8 Ressources du projet
Définir les responsabilités, les relations, l'autorité et les critères de performances des membres de l'équipe du projet et préciser la base sur laquelle on engagera et affectera des membres compétents et/ou des contractuels dans l'équipe du projet. L'achat de produits et de services nécessaires à chaque projet doit être planifié et géré pour favoriser l'atteinte des objectifs du projet en utilisant les pratiques d'achat de l'entreprise.

PO10.9 Gestion des risques du projet
Éliminer ou réduire les risques spécifiques à chaque projet au moyen d'un processus systématique de planification, d'identification, d'analyse, d'actions de réduction des risques, de surveillance et de contrôle des domaines ou des événements susceptibles de provoquer des changements non souhaités. Les risques auxquels le processus de gestion de projet et les livrables sont exposés doivent être identifiés et consolidés au niveau central.

PO10.10 Plan qualité du projet
Préparer un plan de gestion qualité qui décrit le système qualité du projet et comment il sera mis en place. Le plan doit être formellement revu et accepté par toutes les parties prenantes, puis incorporé au plan projet intégré.

PO10.11 Contrôle des changements du projet
Mettre en place un système de contrôle des changements pour chaque projet, de façon à ce que toutes les modifications de ses caractéristiques de base (ex. coût, planning, périmètre et qualité) soient dûment analysées, approuvées et incorporées au plan projet intégré en ligne avec le cadre de gouvernance des programmes et des projets.

PO10.12 Planification du projet et méthodes d'assurance
Identifier les tâches d'assurance destinées à appuyer la validation de systèmes nouveaux ou modifiés pendant la planification du projet, et les inclure dans le plan projet intégré. Les tâches doivent fournir l'assurance que les contrôles internes et les caractéristiques de sécurité satisfont les exigences prévues.

PO10.13 Métrique, reporting et surveillance de la performance du projet
Mesurer la performance du projet par rapport à l'ensemble des critères clés de performance des projets : périmètre, planning, qualité, coût et risque. Identifier tout écart par rapport au plan. Évaluer les conséquences d'un écart sur le projet et sur l'ensemble du programme et rapporter les résultats aux parties prenantes clés. Recommander, mettre en place et surveiller les actions correctrices lorsque c'est nécessaire, en accord avec le cadre de gouvernance des programmes et des projets.

PO10.14 Clôture du projet
Exiger qu'à la fin de chaque projet, les parties prenantes déterminent si le projet a fourni les résultats et bénéfices prévus. Identifier et communiquer toutes les activités exceptionnelles qui ont été nécessaires pour obtenir les résultats du projet et les bénéfices du programme prévus, et identifier et documenter les enseignements qui en ont été tirés et qui pourront être utiles à des projets ou des programmes futurs.

Page volontairement laissée blanche

GUIDE DE MANAGEMENT

PO10 Gérer les projets

De	Entrées
PO1	Portefeuille projets
PO5	Portefeuille actualisé des projets informatiques
PO7	Tableau des compétences informatiques
PO8	Standards de développement
AI7	Revue post-démarrage

Sorties	Vers						
Rapports sur la performance des projets	SE1						
Plan de gestion des risques des projets	PO9						
Guides de gestion des projets	AI1…AI7						
Plans de projets détaillés	PO8	AI1…AI7		DS6			
Portefeuille de projets informatiques à jour	PO1	PO5					

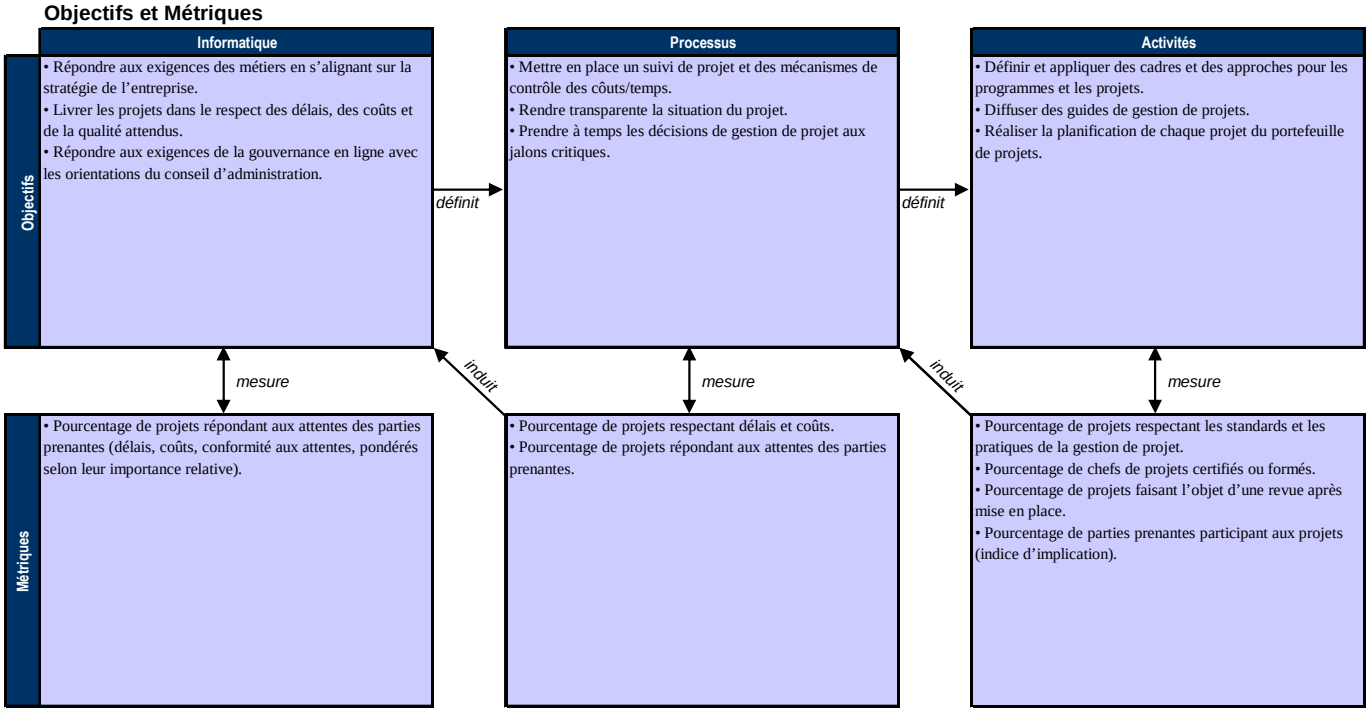
Tableau RACI

Fonctions / **Activités**

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir un cadre de gestion de programme et/ou de portefeuille pour les investissements informatiques.	C	C	A	R						C	C
Mettre en place et maintenir un cadre de gestion des projets informatiques.	I	I	I	A/R	I	C	C	C	C	R	C
Mettre en place et maintenir opérationnel un système de surveillance, de mesure et de gestion de gestion des projets informatiques.	I	I	I	R		C	C	C	C	A/R	C
Élaborer des chartes, plannings, plans qualité, budgets et des plans de gestion de la communication et des risques pour les projets.			C	C	C	C	C	C	C	A/R	C
S'assurer de la participation et de l'implication des parties prenantes aux projets.	I		A	R	C						C
Assurer un contrôle efficace des projets et des changements qui leur sont apportés.			C	C		C	C	C		A/R	C
Définir et mettre en place des méthodes d'assurance et de revue pour les projets.			I	C				I		A/R	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

PO10 Gérer les projets

La gestion du processus *Gérer les projets* qui répond à l'exigence des métiers vis-à-vis de l'informatique *livrer des projets conformes aux délais, aux coûts et à la qualité prévus* est :

0 Inexistante quand

On n'utilise pas les techniques de gestion de projets et l'entreprise ne prend pas en compte les conséquences pour son activité d'une mauvaise gestion des projets et des échecs survenus au cours du développement des projets.

1 Initialisée, au cas par cas quand

L'utilisation des techniques de gestion de projets et leur approche informatique est laissée à l'initiative individuelle des responsables informatiques. Il y a un manque d'implication de la part du management dans la propriété et la gestion des projets. Les décisions critiques concernant la gestion des projets sont prises participation des utilisateurs ni des clients. Les clients et utilisateurs ne sont que peu impliqués dans la définition des projets informatiques, voire pas du tout. Il n'y a pas d'organisation claire de la gestion des projets au sein de l'informatique. Les rôles et responsabilités en matière de gestion des projets ne sont pas définis. Les projets, leur planning et leurs jalons sont mal définis. On ne fait pas de relevés des temps ni des dépenses consacrés aux projets, et donc on ne les confronte pas aux prévisions.

2 Reproductible mais intuitive quand

La direction générale s'est convaincue du besoin de faire de la gestion des projets, et communique sur ce thème. L'entreprise a décidé de développer et d'utiliser certaines techniques et méthodes qu'elle commence à appliquer, projet après projet. Les objectifs métiers et techniques des projets informatiques sont définis de façon informelle. L'implication des parties prenantes dans la gestion des projets informatiques est faible. On développe les premiers guides pour de nombreux aspects de la gestion des projets. L'application des guides de gestion des projets est laissée à l'initiative de chaque chef de projets.

3 Définie quand

Le processus et la méthodologie de gestion des projets informatiques sont en place et on communique sur ces thèmes. On dote les projets informatiques d'objectifs métiers et techniques appropriés. Le management de l'informatique et des métiers commence à s'impliquer dans la gestion des projets informatiques. Un bureau de gestion des projets est mis en place à l'informatique, et on en a défini certains rôles et certaines responsabilités. On définit et actualise les jalons, le planning, le budget et les mesures de performance des projets, et on les surveille. La formation à la gestion des projets existe et résulte encore d'initiatives individuelles. On définit des procédures d'assurance qualité et des activités post-démarrage, cependant la direction des SI ne les applique pas systématiquement. Les projets commencent à être gérés en portefeuilles.

4 Gérée et mesurable quand

Le management exige des métriques projet standardisées et formelles, et une revue des enseignements à tirer à l'échéance d'un projet. La gestion des projets est mesurée et évaluée non seulement au sein de l'informatique mais dans toute l'entreprise. On formalise et communique les améliorations aux processus de gestion des projets avec les membres des équipes des projets formées à ces améliorations. La direction des SI met en place une structure d'organisation de projets, attribue des rôles/responsabilités et des critères de performance pour le personnel, le tout dûment documenté. Des critères d'évaluation de succès de chaque jalon sont mis en place. Valeur et risques sont mesurés et gérés avant, pendant et après l'achèvement des projets. Les projets visent de plus en plus des objectifs de l'entreprise plutôt que des objectifs spécifiquement informatiques. Les commanditaires de la direction générale et les parties prenantes soutiennent fortement et activement les projets. Une formation appropriée à la gestion des projets est prévue pour le personnel du bureau de gestion des projets et pour certains personnels de l'informatique.

5 Optimisée quand

On met en place et on applique une méthodologie de gestion des projets et des programmes qui prend en compte leur cycle de vie entier, et cette méthodologie fait désormais partie de la culture de toute l'entreprise. On met en place une initiative permanente pour identifier et institutionnaliser les meilleures pratiques de gestion des projets. L'informatique met en place une stratégie de recherche de collaborateurs pour les projets de développement et les projets techniques. Une cellule intégrée de gestion des projets est responsable des projets et des programmes, de leur origine à leur achèvement. La planification des programmes et des projets à l'échelle de l'entreprise permet de s'assurer que les ressources utilisateurs et informatiques sont utilisées au mieux pour soutenir les initiatives stratégiques.

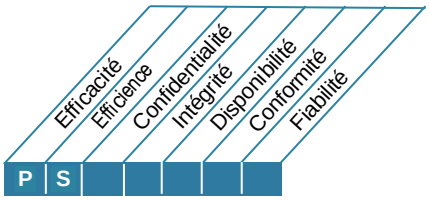
ACQUÉRIR ET IMPLÉMENTER

AI1 Trouver des solutions informatiques
AI2 Acquérir des applications et en assurer la maintenance
AI3 Acquérir une infrastructure technique et en assurer la maintenance
AI4 Faciliter le fonctionnement et l'utilisation
AI5 Acquérir des ressources informatiques
AI6 Gérer les changements
AI7 Installer et valider les solutions et les modifications

DESCRIPTION DU PROCESSUS

AI1 Trouver des solutions informatiques

Le besoin d'une nouvelle application ou fonction impose une analyse avant achat ou création pour s'assurer que les exigences des métiers seront satisfaites grâce à une approche efficace et efficiente. Ce processus recouvre la définition des besoins, la prise en compte de sources alternatives, l'analyse de la faisabilité technique et économique, l'analyse des risques et du rapport coûts/bénéfices, et la décision finale qui tranchera entre faire ou acheter. Toutes ces étapes permettent aux entreprises de minimiser les coûts d'achat et de mise en place de solutions et de s'assurer que celles-ci permettront à l'entreprise d'atteindre ses objectifs.



Le contrôle du processus informatique

Trouver des solutions informatiques

qui répond à l'exigence des métiers vis-à-vis de l'informatique

traduire les exigences fonctionnelles et de contrôle de l'entreprise en solutions informatiques efficaces et efficientes

en se concentrant sur

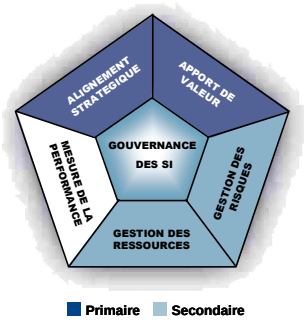
l'identification de solutions techniquement faisables et rentables

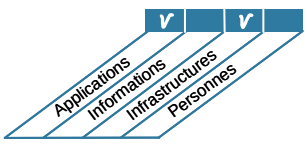
atteint son objectif en

- définissant les exigences des métiers et les impératifs techniques
- entreprenant des études de faisabilité telles que définies dans les standards de développement
- approuvant (ou rejetant) les résultats des études des besoins et de faisabilité

et est mesuré par

- le nombre de projets dont les bénéfices annoncés n'ont pas été réalisés à cause d'évaluations incorrectes de leur faisabilité
- le pourcentage d'études de faisabilité avalisées par le propriétaire de processus
- le pourcentage d'utilisateurs satisfaits des fonctionnalités livrées





OBJECTIFS DE CONTRÔLE

AI1 Trouver des solutions informatiques

AI1.1 Définition et actualisation des exigences métiers, techniques et fonctionnelles
Identifier, classer par priorités et agréer les exigences métiers, techniques et fonctionnelles, qui couvrent l'étendue complète de toutes les initiatives requises pour obtenir les résultats escomptés du programme d'investissement informatique.

AI1.2 Rapport d'analyse de risques
Identifier, documenter et analyser les risques associés aux processus métiers en tant qu'éléments du processus d'entreprise pour l'élaboration des exigences.

AI1.3 Étude de faisabilité et formulation d'alternatives
Mener une étude de faisabilité qui examine la possibilité de mettre en place les exigences. Le management des métiers, assisté par l'informatique, doit évaluer la faisabilité et les alternatives et faire des recommandations aux commanditaires métiers.

AI.4 Décision et approbation concernant les exigences et la faisabilité
S'assurer que le processus impose que les commanditaires métiers approuvent et avalisent les rapports sur les exigences des métiers fonctionnelles et techniques et sur l'étude de faisabilité à des étapes clés prédéterminées. La décision finale quant au choix de la solution et de la procédure d'acquisition doit appartenir aux commanditaires métiers.

GUIDE DE MANAGEMENT

AI1 Trouver des solutions informatiques

De	Entrées
PO1	Plans informatiques stratégiques et tactiques
PO3	Mises à niveau régulières de la technologie ; standards technologiques
PO8	Standards d'acquisition et de développement
PO10	Principes de gestion de projets et plans détaillés des projets
AI6	Description du processus de changement
DS1	Contrats de services
DS3	Plan performance et capacité (exigences)

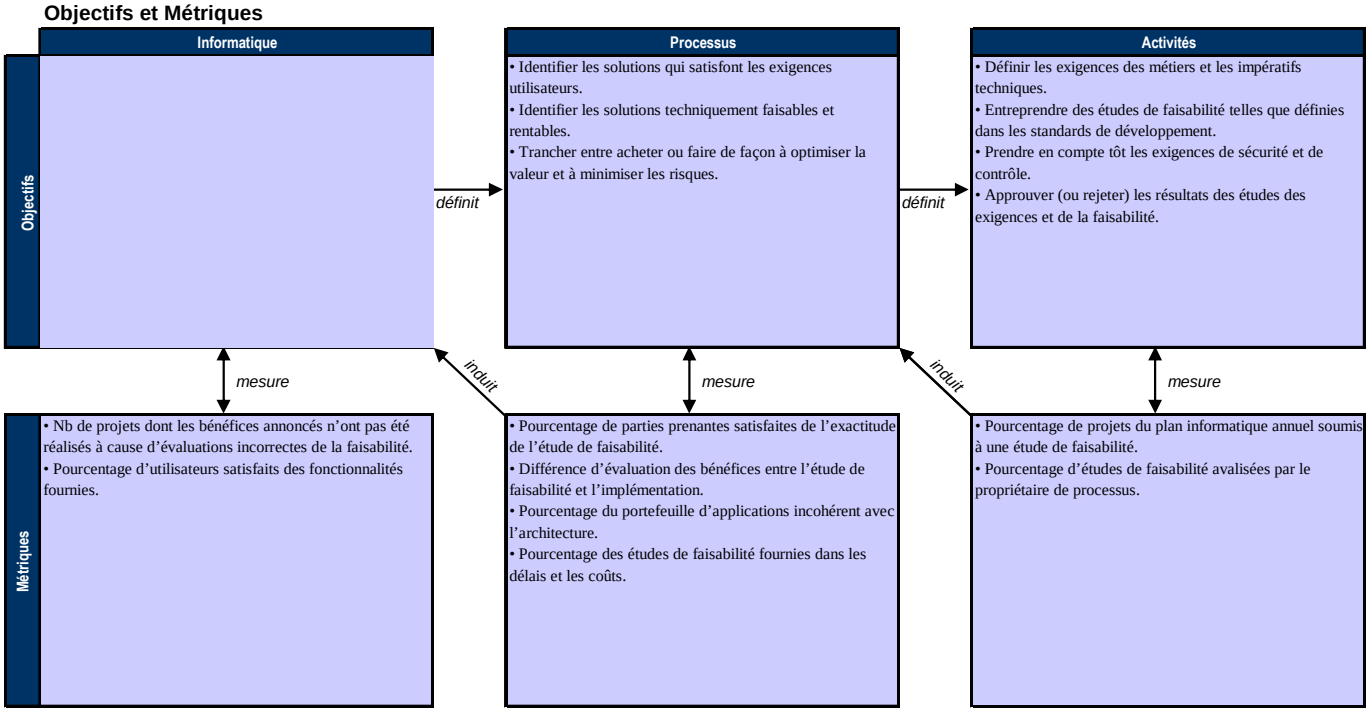
Sorties	Vers						
Étude de faisabilité des exigences des métiers	PO2	PO5	PO7	AI2	AI3	AI4	AI5

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir les exigences des métiers et les impératifs techniques.			C	C	R	C	R	R		A/R	I
Mettre en place les processus pour les exigences d'intégrité/d'actualité.				C		C		C		A/R	C
Identifier, documenter et analyser les risques des processus métiers.			A/R	R	R	R	C	R		R	C
Conduire une étude d'évaluation faisabilité/impact pour la mise en place des exigences des métiers proposées.			A/R	R	R	C	C	C		R	C
Évaluer les bénéfices informatiques des solutions proposées.		I	R	A/R	R	I	I	I		R	
Évaluer les bénéfices pour les métiers des solutions proposées.			A/R	R		C	C	C	I	R	
Élaborer un processus d'approbation des exigences.			C	A		C	C	C		R	C
Approuver et avaliser les solutions proposées.		C	A/R	R	R	C	C	C	I	R	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI1 Trouver des solutions informatiques

La gestion du processus *Trouver des solutions informatiques* qui répond à l'exigence des métiers vis-à-vis de l'informatique *traduire les exigences fonctionnelles et de contrôle de l'entreprise en solutions informatiques efficaces et efficientes* est :

0 Inexistante quand

L'entreprise ne se préoccupe pas d'identifier les besoins fonctionnels et opérationnels pour le développement, la mise en œuvre ou la modification de solutions telles que systèmes, services, infrastructures, logiciels ou données. L'entreprise ne se tient pas au courant des solutions techniques disponibles qui pourraient concerner son activité.

1 Initialisée, au cas par cas quand

On prend conscience de la nécessité de définir les besoins et de trouver des solutions techniques. Des groupes se réunissent pour discuter des besoins de manière informelle et les exigences sont parfois documentées. Certaines personnes trouvent des solutions grâce à une connaissance partielle des produits qui existent sur le marché ou par l'intermédiaire d'offres commerciales. Il existe un minimum de recherche et d'analyse raisonnée de la technologie disponible.

2 Reproductible mais intuitive quand

Il existe différentes approches intuitives à travers l'entreprise pour trouver des solutions informatiques. On trouve des solutions informelles, en fonction des connaissances et de l'expérience accumulées en interne à la DSI. Le succès de chaque projet dépend de l'expertise de quelques individus clés. La qualité de la documentation et de la prise de décision varie considérablement. On utilise des approches non structurées pour définir les exigences et trouver des solutions techniques.

3 Définie quand

Il existe des approches claires et structurées pour déterminer des solutions informatiques. Cette approche impose d'évaluer les solutions alternatives en fonction des exigences métiers ou utilisateurs, des opportunités technologiques, de la faisabilité économique, de l'évaluation des risques et d'autres facteurs. Ce processus *trouver des solutions informatiques* est mis en œuvre pour certains projets qui dépendent des décisions que prend individuellement une personne impliquée, du temps qu'y consacre le management, de l'importance et des priorités des exigences métiers qui en sont à l'origine. On utilise des approches structurées pour définir les exigences et trouver des solutions informatiques.

4 Gérée et mesurable quand

Il existe une méthodologie pour identifier et évaluer les solutions informatiques et on l'utilise pour la plupart des projets. La documentation des projets est de bonne qualité et chaque étape est dûment approuvée. Les exigences sont bien coordonnées et suivent des structures prédéfinies. On examine différentes hypothèses pour la solution choisie, en tenant compte d'analyses coûts/bénéfices. La méthode est claire, définie, en général comprise et mesurable. Il existe une interface clairement définie entre la direction des SI et les métiers pour identifier et évaluer les solutions informatiques.

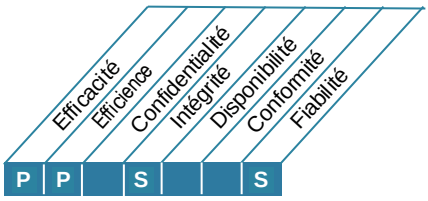
5 Optimisée quand

La méthodologie pour trouver et évaluer des solutions informatiques suit un processus d'amélioration continue. La méthodologie d'acquisition et d'implémentation est assez souple pour s'adapter à des projets de dimensions diverses. Cette méthodologie s'appuie sur des bases de connaissances internes et externes renfermant des références à des solutions techniques. La méthodologie elle-même produit de la documentation selon un format prédéfini qui permet une production et une maintenance efficaces. On découvre souvent de nouvelles occasions d'utiliser l'informatique pour obtenir un avantage concurrentiel, pour stimuler la ré-ingénierie des processus métiers, pour améliorer globalement l'efficience. Le management agit lorsqu'il se rend compte que les solutions informatiques ont été approuvées sans que des exigences techniques et fonctionnelles alternatives aient été prises en compte.

DESCRIPTION DU PROCESSUS

AI2 Acquérir des applications et en assurer la maintenance

Les applications sont rendues disponibles en fonction des exigences des métiers. Ce processus recouvre la conception des applications, les contrôles applicatifs et les exigences de sécurité appropriés qu'il faut y inclure, ainsi que leur développement et leur configuration conformément aux standards. Cela permet aux entreprises de disposer des applications informatiques qui conviennent pour supporter correctement les tâches métiers.



Le contrôle du processus informatique

Acquérir des applications et en assurer la maintenance

qui répond à l'exigence des métiers vis-à-vis de l'informatique

rendre disponibles des applications conformes aux exigences des métiers dans les délais prévus et à un coût raisonnable

en se concentrant sur

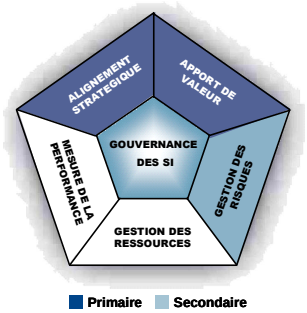
un processus de développement respectueux des délais et de la rentabilité

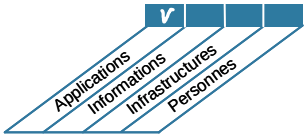
atteint son objectif en

- traduisant les exigences des métiers en spécifications pour la conception
- adoptant des standards de développement pour toutes les modifications
- séparant les activités de développement, de tests et de production

et est mesuré par

- le nombre de problèmes de production par application causant des retards perceptibles
- le pourcentage d'utilisateurs satisfaits des fonctionnalités fournies





OBJECTIFS DE CONTRÔLE

AI2 Acquérir des applications et en assurer la maintenance

AI2.1 Conception générale
Traduire les exigences des métiers en spécifications générales d'acquisition de logiciel, en prenant en compte les orientations technologiques de l'entreprise et l'architecture de l'information. Faire approuver les spécifications de la conception par le management pour s'assurer que la conception générale répond aux exigences. Réévaluer lorsque des anomalies techniques ou logicielles significatives se produisent pendant le développement ou la maintenance.

AI2.2 Conception détaillée
Présenter en détail les spécifications et les impératifs techniques des applications logicielles. Définir les critères d'acceptation de ces impératifs. Faire approuver ces impératifs pour être sûr qu'ils correspondent à la conception générale. Effectuer une réévaluation lorsque des anomalies significatives techniques ou logicielles se produisent pendant le développement ou la maintenance.

AI2.3 Contrôles applicatifs et auditabilité
Si nécessaire mettre en place des contrôles métiers des contrôles programmés de façon à ce que le traitement soit réalisé avec exactitude, complètement, au bon moment, et qu'il soit autorisé et auditable.

AI2.4 Sécurité et disponibilité des applications
Répondre aux exigences de sécurité et de disponibilité des applications en regard des risques identifiés et en ligne avec la classification des données, l'architecture de l'information et de la sécurité de l'information, de l'appétence au risque de l'entreprise.

AI2.5 Configuration et implémentation des logiciels applicatifs acquis
Configurer et implémenter les progiciels de façon à répondre aux objectifs des métiers.

AI2.6 Mises à jour majeures des systèmes existants
Suivre un processus de développement similaire à celui du développement de nouveaux systèmes dans l'éventualité de modifications majeures des systèmes existants qui ont pour conséquences des modifications significatives de conception et/ou des fonctionnalités actuelles.

AI2.7 Développement d'applications
S'assurer que les nouvelles fonctionnalités automatisées se conforment aux spécifications de conception, aux standards de développement et de documentation, aux exigences de qualité et aux normes de recette. S'assurer que tous les aspects légaux et contractuels sont identifiés et pris en compte dans les applications développées par des tiers.

AI2.8 Assurance qualité des logiciels
Développer un plan d'assurance qualité, le doter de ressources et le mettre en œuvre de façon à obtenir la qualité spécifiée dans la définition des exigences et dans les politiques et les procédures qualité de l'entreprise.

AI2.9 Gestion des exigences des applications
Au cours de la conception, du développement et de la mise en place effectuer un suivi individuel de chaque exigence (y compris de celles qui ont été rejetées) et approuver les modifications apportées à certaines exigences selon un processus établi de gestion des changements.

AI2.10 Maintenance des applications
Développer un plan stratégique pour la maintenance des applications.

GUIDE DE MANAGEMENT

AI2 Acquérir des applications et en assurer la maintenance

De	Entrées
PO2	Dictionnaire de données ; schéma de classification des données, plan optimisé des systèmes métiers
PO3	Mises à niveau régulières de l'état de l'art de la technologie
PO5	Comptes-rendus coûts/bénéfices
PO8	Standards d'acquisition et de développement
PO10	Guides de gestion des projets et plans de projets détaillés
AI1	Étude de faisabilité des exigences des métiers
AI6	Description du processus de changement

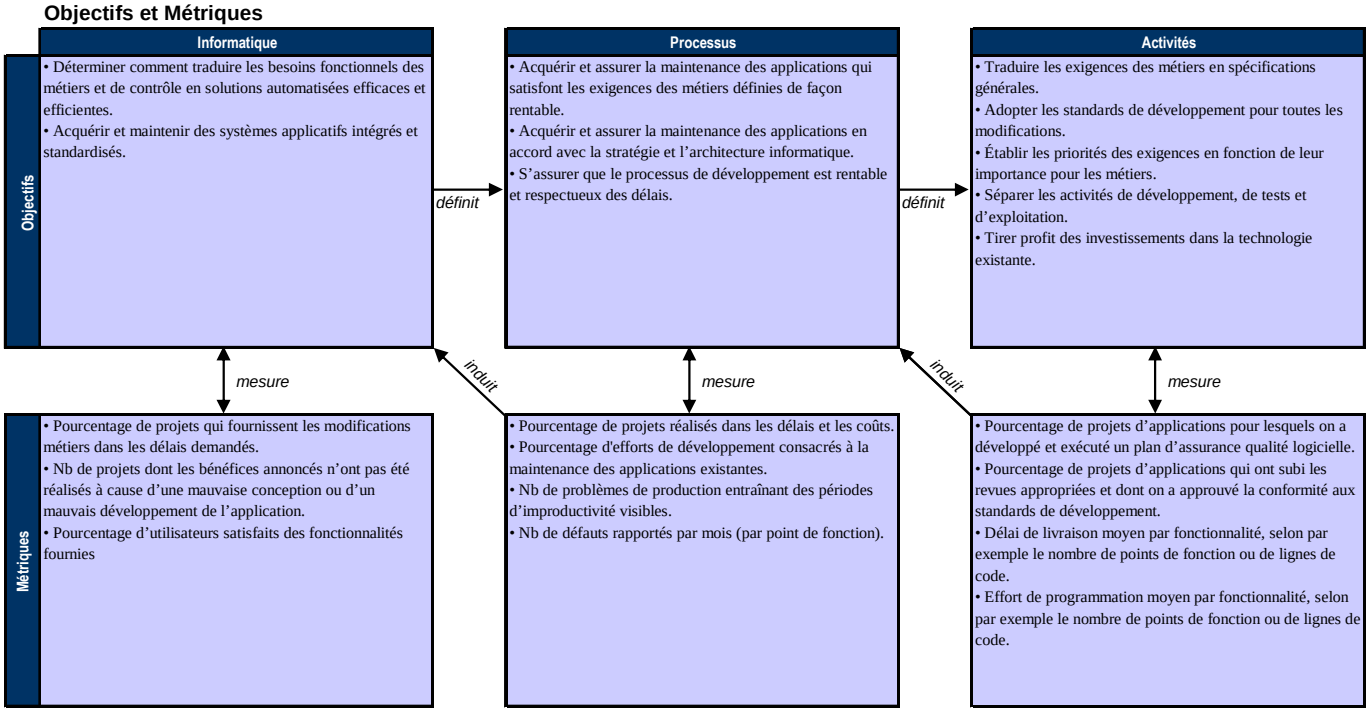
Sorties	Vers						
Spécification des contrôles de sécurité des applications	DS5						
Connaissance des applications et des progiciels	AI4						
Décisions d'acquisition	AI5						
Contrats de services initialement prévus	DS1						
Spécifications de disponibilité, continuité et reprise	DS3	DS4					

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Traduire les exigences des métiers en spécifications de conception générale.					C		C	A/R		R	C
Préparer la conception détaillée et les besoins techniques des applications.				I	C	C	C	A/R		R	C
Spécifier les contrôles applicatifs dans la conception.					R	C		A/R		R	R
Adapter et implémenter les fonctionnalités automatisées acquises.					C	C		A/R		R	C
Développer des méthodologies, les formaliser et des processus pour gérer le processus de développement des applications.				C		C	C	A	C	R	C
Créer un plan d'assurance qualité pour le projet.					I		C	R		A/R	C
Suivre et gérer les exigences des applications.								R		A/R	
Développer un plan pour la maintenance des applications.				C		C		A/R		C	

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI2 Acquérir des applications et en assurer la maintenance

La gestion du processus *Acquérir des applications et en assurer la maintenance* qui répond à l'exigence des métiers vis-à-vis de l'informatique *rendre disponibles des applications conformes aux exigences des métiers, dans les délais prévus et à un coût raisonnable* est :

0 Inexistante quand

Il n'existe pas de processus pour concevoir des applications et en faire le cahier des charges. Typiquement, on achète les applications en se basant sur les offres des fournisseurs, la réputation d'une marque, ou les habitudes des informaticiens, sans beaucoup tenir compte des véritables besoins.

1 Initialisée, au cas par cas quand

On est conscient de la nécessité d'avoir un processus d'acquisition et de maintenance des applications. Les façons d'acheter et d'assurer la maintenance de logiciels applicatifs varient d'un projet à l'autre. On a sans doute acheté de façon indépendante quelques solutions individuelles pour répondre à certaines exigences des métiers, ce qui pénalise l'efficacité de la maintenance et du support.

2 Reproductible mais intuitive quand

Il existe des processus différents, mais similaires, pour l'achat et la maintenance d'applications, et on se fie à l'expertise de la fonction informatique. Le taux de succès des applications dépend largement des compétences internes et du niveau d'expérience de l'informatique. La maintenance est en général problématique et sa qualité se dégrade lorsque des personnels qui ont accumulé des connaissances spécifiques quittent l'entreprise. On n'a que peu pris en compte la sécurité et la disponibilité dans la conception ou l'acquisition des logiciels applicatifs.

3 Définie quand

Il existe un processus clair et globalement compris pour l'achat et la maintenance de logiciels applicatifs. Ce processus est aligné sur les stratégies SI et métiers. On s'efforce de mettre en œuvre des processus documentés et cohérents pour différentes applications et différents projets. Les méthodologies sont en général rigides et difficiles à appliquer à tous les cas, si bien qu'il peut arriver qu'on en néglige certaines étapes. Les activités de maintenance sont planifiées et coordonnées.

4 Gérée et mesurable quand

Il existe une méthodologie formelle et bien comprise qui comporte un processus de conception et de spécifications, des critères d'achat, un processus de tests et des exigences de documentation. On s'est mis d'accord sur des mécanismes d'approbation formels et documentés pour s'assurer que toutes les étapes sont respectées, et que les cas particuliers sont gérés. Les pratiques et les procédures ont évolué pour bien s'adapter à l'entreprise, elles sont utilisées par tout le personnel et répondent à la plupart des exigences des applications.

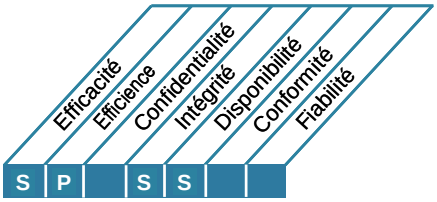
5 Optimisée quand

Les pratiques d'acquisition et de maintenance des applications sont conformes aux processus définis. L'approche est modulaire, favorisant des applications prédéfinies, standardisées, et adaptées aux besoins de l'entreprise. Cette approche concerne l'ensemble de l'entreprise. La méthodologie d'acquisition et de maintenance est bien avancée et permet des déploiements rapides, une forte réactivité ainsi que suffisamment de souplesse pour répondre à des exigences métiers évolutives. La méthodologie d'acquisition et de mise en place des applications connaît des améliorations permanentes et s'appuie sur des bases de connaissances internes et externes donnant accès à des documents de référence et aux bonnes pratiques. La méthodologie produit de la documentation selon un format prédéfini qui permet une production et une maintenance efficaces.

DESCRIPTION DU PROCESSUS

AI3 Acquérir une infrastructure technique et en assurer la maintenance

Une entreprise dispose de processus pour l'acquisition, la mise en place et la mise à niveau de son infrastructure technique. Cela exige une approche planifiée de l'acquisition, de la maintenance et de la protection de l'infrastructure en accord avec les stratégies technologiques adoptées et de disposer d'environnements de développement et de tests. On est ainsi sûr de disposer d'un support technique permanent pour les applications métiers.



Le contrôle du processus informatique

Acquérir une infrastructure technique et en assurer la maintenance

qui répond à l'exigence des métiers vis-à-vis de l'informatique

acquérir et maintenir opérationnelle une infrastructure technique intégrée et standardisée

en se concentrant sur

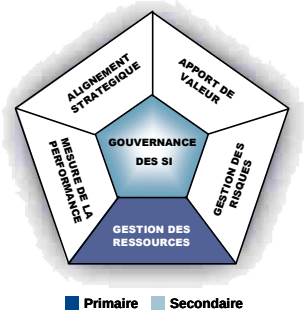
la mise à disposition de plates-formes appropriées pour les applications métiers en accord avec les standards informatiques et d'architecture technique définis

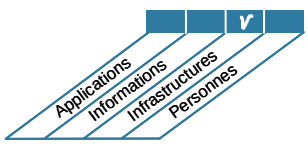
atteint son objectif en

- élaborant un plan d'acquisition des technologies qui s'aligne sur le plan d'infrastructure technique
- planifiant la maintenance de l'infrastructure
- mettant en place des mesures de contrôle interne, de sécurité et d'aptitude à être audité.

et est mesuré par

- le pourcentage de plates-formes non conformes aux standards informatiques et d'architecture technique définis
- le nombre de processus métiers critiques qui s'appuient sur une infrastructure obsolète ou en voie de l'être
- le nombre de composants d'infrastructure dont la maintenance est devenue impossible ou qui le sera bientôt





OBJECTIFS DE CONTRÔLE

AI3 Acquérir une infrastructure technique et en assurer la maintenance

AI3.1 Plan d'acquisition d'une infrastructure technique
Élaborer un plan d'acquisition, de mise en place et de maintenance de l'infrastructure technique qui réponde aux besoins fonctionnels et techniques définis des métiers, et qui soit en accord avec les orientations technologiques de l'entreprise.

AI3.2 Protection et disponibilité des ressources de l'infrastructure
Mettre en place des mesures de contrôle interne, de sécurité et d'aptitude à être audité au cours de la configuration, de l'intégration et de la maintenance du matériel et des logiciels système pour protéger les ressources et assurer la disponibilité et l'intégrité. Il faut que ceux qui développent et intègrent les composants d'infrastructure définissent clairement les responsabilités d'utilisation des composants sensibles. Leur utilisation doit être suivie et évaluée.

AI3.3 Maintenance de l'infrastructure
Développer une stratégie et un plan pour la maintenance de l'infrastructure et s'assurer que les modifications sont contrôlées conformément à la procédure de gestion des changements de l'entreprise. Inclure une révision périodique en fonction des besoins des métiers, de la gestion des correctifs et des stratégies de mise à niveau, et en fonction de l'évaluation de la vulnérabilité et des exigences de sécurité.

AI3.4 Environnement de test de faisabilité
Mettre en place des environnements de développement et de test pour s'assurer d'une faisabilité et de tests d'intégration des composants de l'infrastructure efficaces et efficients.

GUIDE DE MANAGEMENT

AI3 Acquérir une infrastructure technique et en assurer la maintenance

De	Entrées
PO3	Plan d'infrastructure technique, standards et opportunités ; mises à niveau techniques régulières
PO8	Standards d'acquisition et de développement
PO10	Principes généraux gestion de projets et plans projets détaillés
AI1	Étude de faisabilité des exigences des métiers
AI6	Changer l'intitulé des processus
DS3	Plan performance et capacité (exigences)

Sorties	Vers						
Décisions d'acquisition	AI5						
Système configuré à tester/installer	AI7						
Exigences de l'environnement physique	DS12						
Mises à jour des standards techniques	PO3						
Exigences de surveillance des systèmes	DS3						
Connaissance de l'infrastructure	AI4						
CE prévus initialement	DS1						

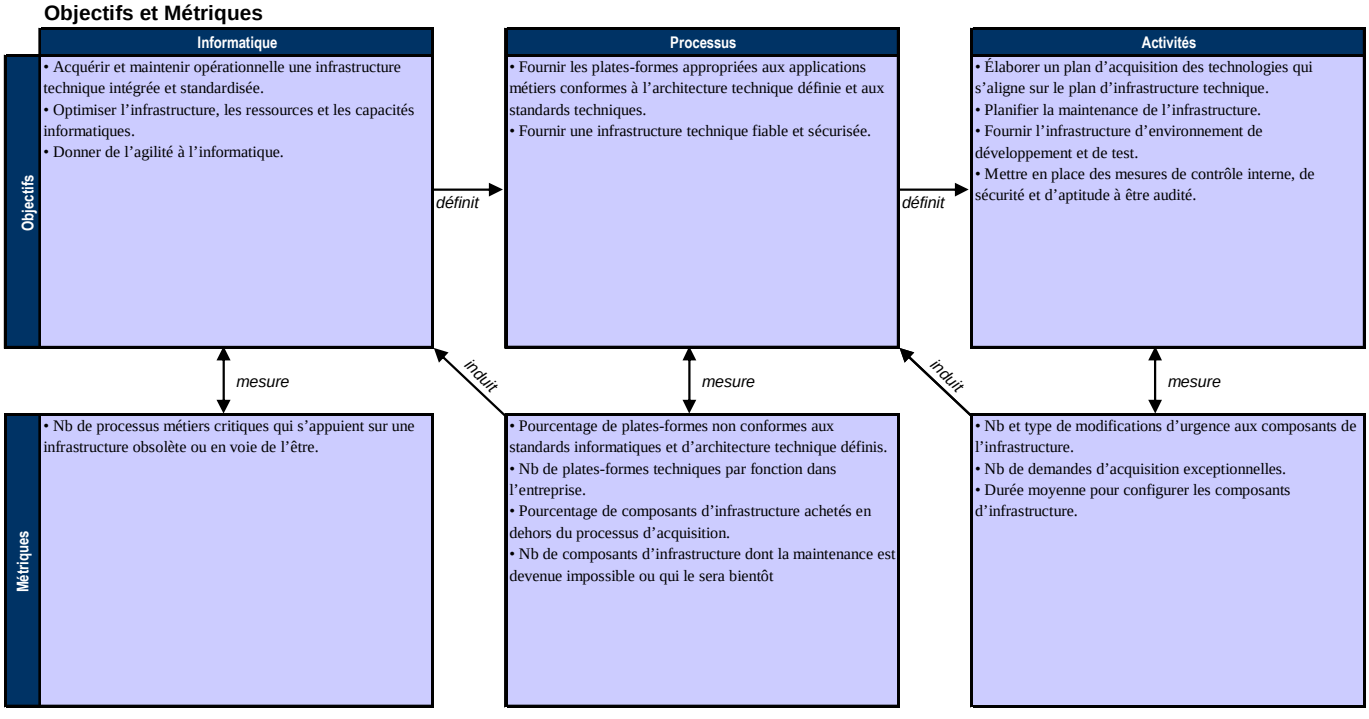
Tableau RACI

Fonctions

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir les procédures/processus d'acquisition.		C		A		C	C	C	R		I
Examiner les besoins d'infrastructure avec les fournisseurs (agréés).		C/I		A	I	R	C	C	R		I
Définir la stratégie et planifier la maintenance pour l'infrastructure.				A		R	R	R	C		
Configurer les composants de l'infrastructure.				A		R	C				I

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI3 Acquérir une infrastructure technique et en assurer la maintenance

La gestion du processus *Acquérir une infrastructure technique et en assurer la maintenance* qui répond à l'exigence des métiers vis-à-vis de l'informatique *acquérir et maintenir opérationnelle une infrastructure technique intégrée et standardisée* est :

0 Inexistante quand

On ne considère pas l'infrastructure technique comme une question suffisamment importante pour s'en occuper.

1 Initialisée, au cas par cas quand

On modifie l'infrastructure pour chaque nouvelle application, sans avoir de plan général. Bien que l'on ait conscience de l'importance de l'infrastructure technique, il n'y a pas d'approche globale cohérente. Les activités de maintenance réagissent aux besoins à court terme. L'environnement de test est l'environnement de production.

2 Reproductible mais intuitive quand

Il y a une certaine cohérence dans les approches tactiques lors de l'acquisition et de la maintenance d'une infrastructure technique. L'acquisition et la maintenance d'une infrastructure technique ne sont pas basées sur une stratégie définie et ne prennent pas en compte les besoins des applications métiers qu'il s'agit de supporter. On comprend que l'infrastructure technique est importante, et certaines pratiques formelles en tiennent compte. On planifie une certaine maintenance, mais incomplètement et sans coordination. Dans certains cas de figure, il existe un environnement de test spécifique.

3 Définie quand

Il existe un processus clair et globalement compris pour l'achat et la maintenance de l'infrastructure technique. Ce processus répond aux besoins des applications critiques de l'entreprise, et il est calé sur la stratégie des métiers et sur la stratégie des SI, mais il n'est pas constamment mis en œuvre. La maintenance est planifiée et coordonnée. Les environnements de test et de production sont séparés.

4 Gérée et mesurable quand

Le processus d'acquisition et de maintenance de l'infrastructure technique s'est développé au point de bien fonctionner dans la plupart des situations, d'être mis en œuvre avec constance, et d'être réutilisable. L'infrastructure technique supporte comme il convient les applications métiers. Le processus est à la fois bien structuré et proactif. Le coût en temps et en argent pour atteindre le niveau souhaitable d'évolutivité, compatibilité, souplesse, et intégration est partiellement optimisé.

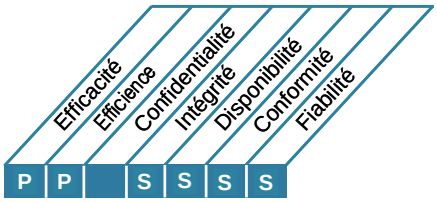
5 Optimisée quand

Le processus d'acquisition et de maintenance de l'infrastructure technique est proactif et parfaitement aligné sur les applications métiers clés et sur l'architecture technique. On applique les bonnes pratiques pour ce qui est des solutions technologiques et l'entreprise est au courant des derniers développements en matière de plates-formes et d'outils de gestion. On réduit les coûts par la rationalisation et la standardisation des composants d'infrastructure et par l'automatisation. Grâce à un haut niveau de veille technologique on sait trouver les meilleurs moyens d'anticiper pour améliorer les performances, y compris en externalisant. L'infrastructure matérielle et logicielle est vue comme le facteur essentiel pour généraliser l'utilisation de l'informatique.

DESCRIPTION DU PROCESSUS

AI4 Faciliter le fonctionnement et l'utilisation

Les connaissances sur les nouveaux systèmes sont rendues disponibles. Ce processus impose de produire de la documentation et des manuels pour les utilisateurs et pour l'informatique, et de proposer des formations pour assurer une bonne utilisation et un bon fonctionnement des applications et de l'infrastructure.



Le contrôle du processus informatique

Faciliter le fonctionnement et l'utilisation

qui répond à l'exigence des métiers vis-à-vis de l'informatique

satisfaire les utilisateurs finaux par l'offre de services et par les niveaux de services, et intégrer progressivement les applications et les solutions informatiques dans les processus métiers

en se concentrant sur

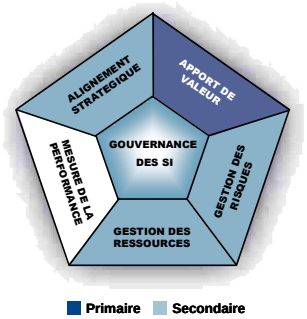
la fourniture de manuels utilisateurs, de manuels opérationnels et de supports de formation efficaces pour transférer la connaissance nécessaire au bon fonctionnement et à la bonne utilisation des systèmes.

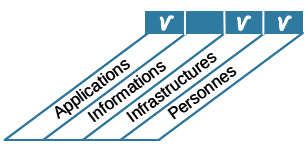
atteint son objectif en

- développant la documentation de transfert des connaissances et en la rendant disponible
- communiquant en direction des utilisateurs et des directions des métiers, du personnel en charge du support et de la production et en les formant
- produisant des supports de formation

et est mesuré par

- le nombre d'applications où des procédures informatisées sont intégrées progressivement dans les processus métiers
- le pourcentage de responsables d'activités satisfaits des documents de formation aux applications et des documents de support
- le nombre d'applications pour lesquelles les utilisateurs et les agents du support bénéficient d'une formation adéquate





OBJECTIFS DE CONTRÔLE

AI4 Faciliter le fonctionnement et l'utilisation

AI4.1 Planification pour rendre les solutions exploitables
Développer un plan pour identifier et documenter tous les aspects techniques, d'exploitation et d'utilisation de façon à ce que tous ceux qui doivent exploiter, utiliser et maintenir les solutions automatisées puissent exercer leurs responsabilités.

AI4.2 Transfert de connaissances aux métiers
Transférer les connaissances aux responsables des métiers pour permettre à cette population d'assumer la propriété des systèmes et des données et d'exercer la responsabilité de la livraison de services et de la qualité, du contrôle interne et de l'administration des applications.

AI4.3 Transfert de connaissances aux utilisateurs finaux
Transférer les connaissances et le savoir-faire aux utilisateurs finaux pour leur permettre d'utiliser les applications avec efficacité et efficience au bénéfice des processus métiers.

AI4.4 Transfert de connaissances aux équipes d'exploitation et de support
Transférer les connaissances et le savoir-faire aux équipes d'exploitation et de support technique pour leur permettre de travailler, de fournir l'assistance et d'assurer la maintenance du système et de l'infrastructure associée avec efficacité et efficience.

GUIDE DE MANAGEMENT

AI4 Faciliter le fonctionnement et l'utilisation

De	Entrées
PO10	Principes généraux gestion de projets et plans projets détaillés
AI1	Étude de faisabilité des exigences des métiers
AI2	Connaissance de l'application et de la suite logicielle
AI3	Connaissance de l'infrastructure
AI7	Erreurs connues et acceptées
DS7	Mises à jour de la documentation requise

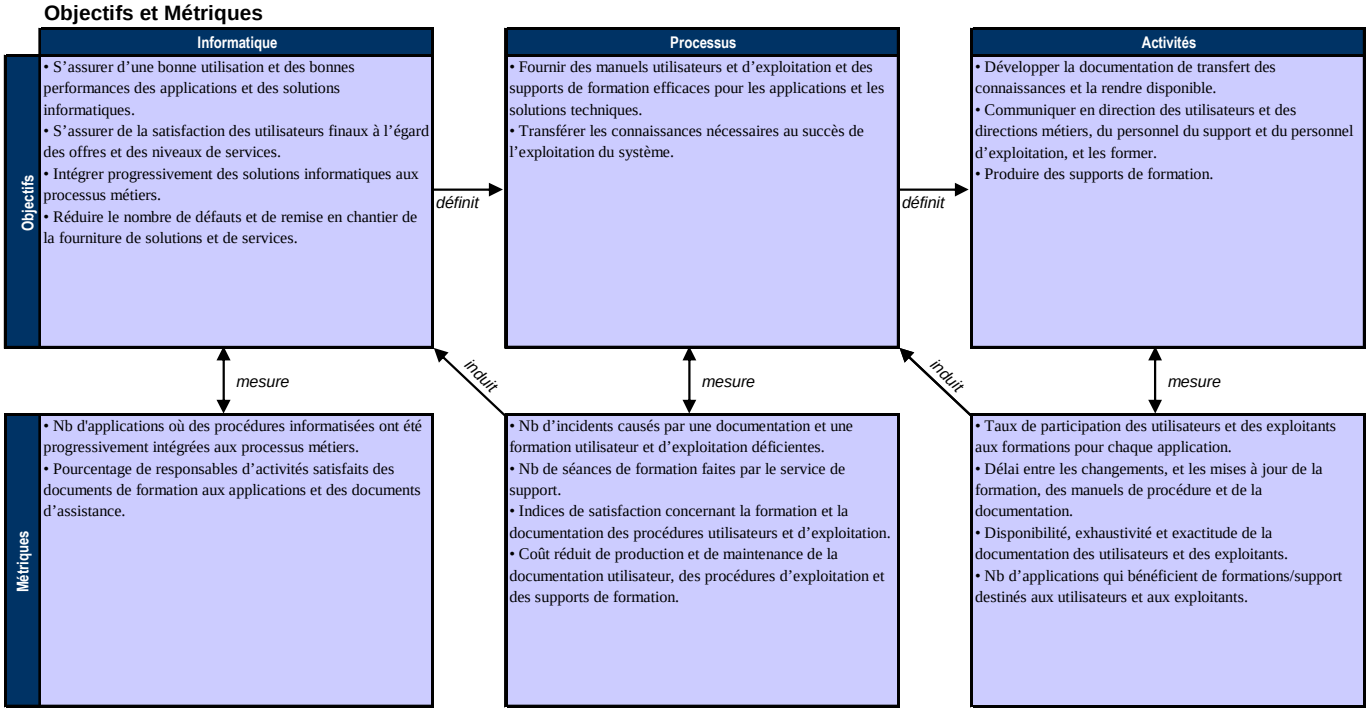
Sorties	Vers						
Manuels utilisateur, d'exploitation, d'assistance, technique et d'administration	AI7	DS4	DS8	DS9	DS11	DS13	
Exigences de transfert de connaissances pour la mise en place d'une solution	DS7						
Supports de formation	DS7						

Tableau RACI

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité	Equipe de déploiement	Service formation
Développer une stratégie pour rendre la solution exploitable.				A	A	R		R			I	R	C
Développer une méthodologie de transfert de connaissances.				C	A							C	R
Développer des manuels de procédure pour les utilisateurs finaux.					A/R			R			C	C	
Développer de la documentation de support technique pour le personnel de l'exploitation et du support.						A/R		C			C		
Développer et fournir la formation.					A	A		R					R
Évaluer les résultats de la formation et améliorer la documentation lorsque c'est nécessaire.					A	A						R	R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI4 Faciliter le fonctionnement et l'utilisation

La gestion du processus *Faciliter le fonctionnement et l'utilisation* qui répond à l'exigence des métiers vis-à-vis de l'informatique *satisfaire les utilisateurs finaux par l'offre de services et par les niveaux de services, et intégrer progressivement les applications et les solutions informatiques dans les processus métiers* est :

0 Inexistante quand

Il n'existe pas de processus de production de la documentation utilisateurs, des manuels d'exploitation, ni des supports de formation. Les seuls documents existants sont ceux qui sont fournis avec les produits achetés.

1 Initialisée, au cas par cas quand

On est conscient de la nécessité de documenter les processus. On produit certaines documentations et on les distribue irrégulièrement à des groupes limités. Une grande partie de la documentation et de nombreuses procédures sont périmées. Les supports de formation ont tendance à être à usage unique et leur qualité est inconstante. Il n'y a pratiquement aucune intégration des procédures dans les différents services systèmes et métiers. Les services métiers ne sont pas impliqués dans la conception des programmes de formation.

2 Reproductible mais intuitive quand

On utilise des approches similaires pour produire des procédures et de la documentation, mais sans s'appuyer sur un référentiel ou sur une méthodologie. Les approches du développement des procédures utilisateur ou d'exploitation ne sont pas uniformisées. Les supports de formation sont faits par des individus ou par des équipes de projet, et la qualité dépend des personnes impliquées. Les procédures et la qualité du support aux utilisateurs varient de médiocres à très bonnes, l'ensemble étant inconstant et le niveau d'intégration dans l'entreprise très faible. On fournit ou on encourage les programmes de formation pour les utilisateurs et les métiers, mais il n'existe pas de plan général de fourniture ou de déploiement de formations.

3 Définie quand

Il existe un cadre clairement défini, accepté et compris pour ce qui concerne la documentation utilisateurs, les manuels d'exploitation et les supports de formation. Les procédures sont stockées et mises à jour dans une bibliothèque officielle, et sont accessibles par tous ceux qui en ont besoin. La documentation et les procédures sont corrigées en fonction des besoins. Il existe des versions de sauvegarde des procédures que l'on peut mettre à jour et auxquelles on peut accéder en cas de sinistre. Il existe un processus qui spécifie que les mises à jour des procédures et des supports de formation font partie des livrables d'un projet de changement. Malgré l'existence d'approches définies, le contenu réel varie parce qu'on ne contrôle pas la conformité avec les standards. Les utilisateurs sont impliqués dans le processus de manière informelle. On automatise de plus en plus la génération et la distribution des procédures. La formation des utilisateurs et des métiers est planifiée et programmée.

4 Gérée et mesurable quand

Il existe un cadre défini pour la maintenance des procédures et les supports de formation qui a le soutien du management de l'informatique. L'approche adoptée pour la maintenance des procédures et pour les manuels de formation concerne tous les systèmes et toutes les services, si bien qu'on peut considérer les processus dans une perspective métier. Les manuels de procédures et les supports de formation sont intégrés de façon à inclure les éléments communs et les interfaces. Il existe des contrôles pour s'assurer qu'on applique les standards et qu'on développe des procédures, qu'on assure leur maintenance, pour tous les processus. On collecte les informations en provenance des utilisateurs et des métiers et on les évalue comme éléments d'un processus d'amélioration continue. La documentation et les supports de formation ont en général un bon niveau de fiabilité et de disponibilité. On a mis en place un nouveau processus d'utilisation de la documentation et de gestion des procédures informatisées. Le développement de procédures informatisées est de plus en plus intégré au développement d'applications, ce qui améliore la cohérence et facilite l'accès des utilisateurs. La formation des métiers et des utilisateurs s'adapte aux besoins des métiers. Le management de l'informatique élabore des outils pour mesurer le développement et la fourniture de documentation, de supports et de programmes de formation.

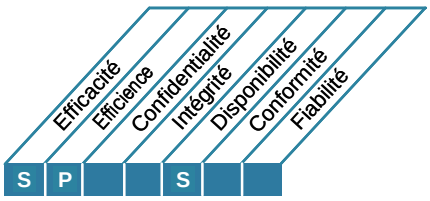
5 Optimisée quand

Le processus de documentation destinée aux utilisateurs et exploitants s'améliore constamment grâce à l'adoption de nouveaux outils et de nouvelles méthodes. La documentation des procédures et les supports de formation sont traités comme une base de connaissances en constante évolution, qui est tenue à jour au moyen des outils de gestion des connaissances, de *workflow* et de diffusion les plus modernes, ce qui en facilite l'accessibilité et la maintenance. La documentation et les supports de formation sont mis à jour pour tenir compte des changements dans l'entreprise, dans l'exploitation et dans les logiciels. Le développement de documentation et de supports de formation ainsi que la fourniture de programmes de formation sont pleinement intégrés aux métiers et aux définitions des processus métiers, satisfaisant ainsi aux exigences générales de l'entreprise et non plus seulement aux procédures informatisées.

DESCRIPTION DU PROCESSUS

AI5 Acquérir des ressources informatiques

On a besoin d'acquérir des ressources informatiques. Elles comprennent les personnes, le matériel, le logiciel et les services. Cela exige de définir et d'appliquer des procédures de recrutement et d'achat, la sélection des fournisseurs, l'établissement d'arrangements contractuels, et l'acte lui-même de se procurer ces ressources. C'est ainsi qu'on peut assurer à l'entreprise toutes les ressources informatiques requises au bon moment et au meilleur coût.



Le contrôle du processus informatique

Acquérir des ressources informatiques

qui répond à l'exigence des métiers vis-à-vis de l'informatique

améliorer la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise

en se concentrant sur

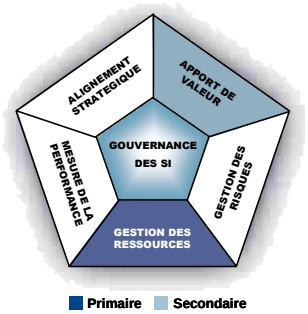
le recrutement et la conservation des compétences informatiques qui correspondent à la stratégie de fourniture de services, l'acquisition d'une infrastructure informatique intégrée et standardisée, et la réduction des risques liés aux achats informatiques

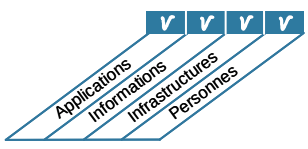
atteint son objectif en

- se faisant conseiller sur les aspects juridiques et contractuels
- définissant des procédures et des standards d'achat
- se procurant les matériels, logiciels et services nécessaires conformément aux procédures définies

et est mesuré par

- le nombre de contestations liées aux contrats d'achat
- la réduction des coûts d'achat
- le pourcentage des parties prenantes clés satisfaites des fournisseurs





OBJECTIFS DE CONTRÔLE

AI5 Acquérir des ressources informatiques

AI5.1 Contrôle des achats
Développer et suivre un ensemble de procédures et de standards conformes au processus général et à la stratégie d'acquisition de l'entreprise pour acheter l'infrastructure informatique, les installations, les matériels, logiciels et services dont les métiers ont besoin.

AI5.2 Gestion des contrats fournisseurs
Mettre en place, pour tous les fournisseurs, une procédure pour établir, modifier et mettre un terme aux contrats. Cette procédure doit recouvrir, au minimum, les responsabilités légales, financières et civiles, ainsi que celles qui sont liées à la documentation, à la performance, à la sécurité, à la propriété intellectuelle et à la résiliation (y compris les clauses pénales). Tous les contrats doivent être examinés par des conseillers juridiques ainsi que toutes les modifications.

AI5.3 Choix des fournisseurs
Choisir les fournisseurs selon une pratique loyale et formelle pour garantir la meilleure adaptation durable aux exigences formulées. Ces exigences doivent être optimisées en fonction de propositions de fournisseurs potentiels.

AI5.4 Acquisition de ressources informatiques
Veiller à la protection et au respect des intérêts de l'entreprise dans tous les accords contractuels d'acquisition en incluant les droits et obligations de toutes les parties dans les clauses contractuelles d'acquisition de logiciels, de ressources de développement, d'infrastructures et de services.

GUIDE DE MANAGEMENT

AI5 Acquérir des ressources informatiques

De	Entrées
PO1	Stratégie d'achats informatiques
PO8	Standards d'acquisition
PO10	Principes généraux gestion de projets et plans projets détaillés
AI1	Étude de faisabilité des exigences des métiers
AI2-3	Décisions d'acquisition
DS2	Catalogue fournisseurs

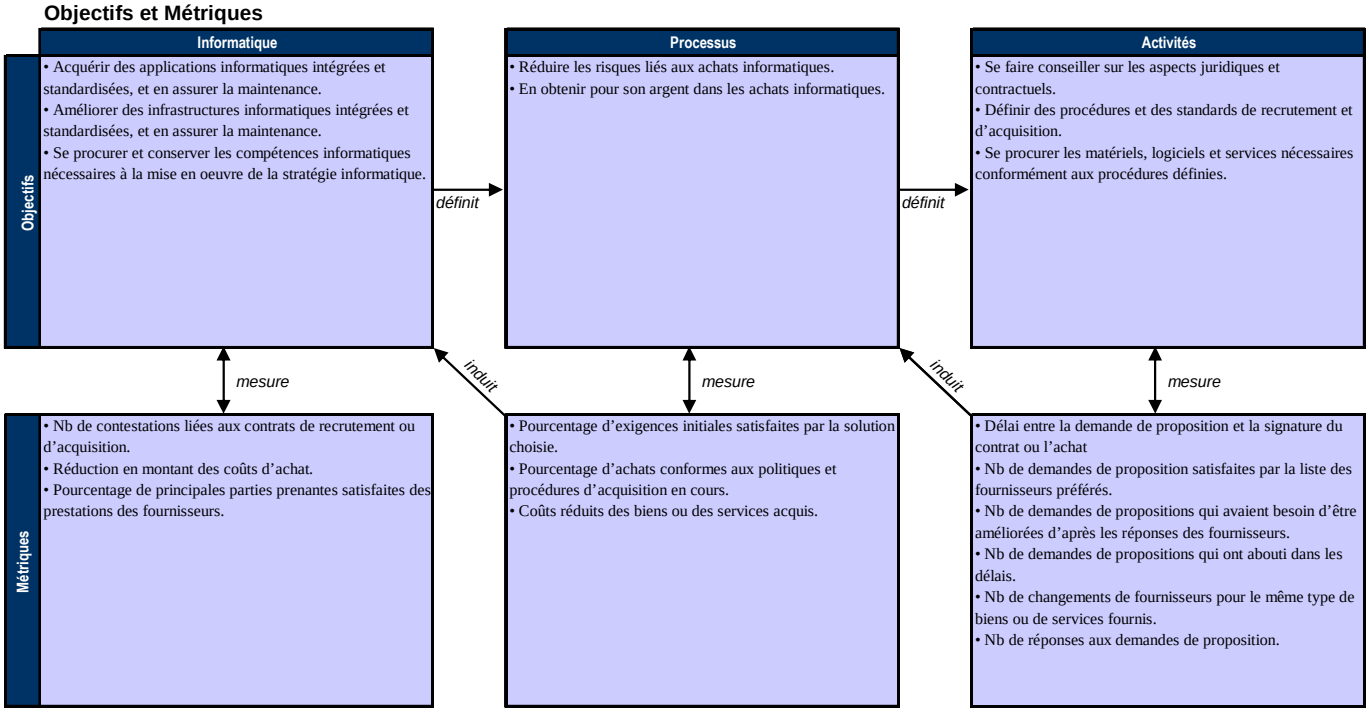
Sorties	Vers
Exigences gestion des relations avec les tiers	DS2
Articles achetés	AI7
Accords contractuels	DS2

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Développer des politiques et des procédures d'acquisition informatique conformes aux politiques d'acquisition de l'entreprise.	I	C		A		I	I	I	R		C
Établir/tenir à jour une liste de fournisseurs accrédités.									A/R		
Évaluer et sélectionner les fournisseurs selon un processus de demande de proposition (devis).	C	C		A		R		R	R	R	C
Rédiger des contrats qui protègent les intérêts de l'entreprise.	R	C		A		R		R	R		C
Respecter les procédures d'acquisition établies.				A		R		R	R		C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI5 Acquérir des ressources informatiques

La gestion du processus *Acquérir des ressources informatiques* qui répond à l'exigence des métiers vis-à-vis de l'informatique *améliorer la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise* est :

0 Inexistante quand

On n'a pas mis en place un processus défini d'acquisition de ressources. L'entreprise ne reconnaît pas la nécessité de politiques et de procédures claires pour s'assurer que toutes les ressources informatiques soient acquises au bon moment et dans de bonnes conditions économiques.

1 Initialisée, au cas par cas quand

L'entreprise reconnaît la nécessité d'avoir des procédures et des politiques qui lient les acquisitions informatiques au processus général d'acquisition. Les contrats d'acquisition de ressources informatiques sont rédigés et gérés par des directeurs de projets et d'autres personnes qui exercent leur jugement professionnel au lieu d'être le résultat de procédures et de politiques formelles. La relation entre les processus de gestion des achats et des contrats de l'entreprise d'une part et l'informatique d'autre part n'existe qu'au cas par cas. Les contrats d'achats sont gérés au moment de la conclusion des projets au lieu de l'être de façon continue.

2 Reproductible mais intuitive quand

On est conscient au niveau de l'entreprise du besoin d'avoir des politiques et des procédures de base pour les acquisitions informatiques. Les politiques et les procédures sont partiellement intégrées au processus global d'acquisition de l'entreprise. Les processus d'achats sont essentiellement utilisés pour les projets importants à grande visibilité. C'est l'expérience individuelle du gestionnaire de contrats qui permet de définir les responsabilités opérationnelles et finales des achats informatiques et de la gestion des contrats. On reconnaît l'importance de la gestion des fournisseurs et de la gestion des relations, mais elles ne sont mises en œuvre que sur des initiatives individuelles. Les processus de passation de contrats sont essentiellement utilisés pour les projets importants ou à grande visibilité.

3 Définie quand

Le management met en place des politiques et des procédures pour les achats informatiques. Les politiques et les procédures sont inspirées par le processus global d'acquisition de l'entreprise. Les achats informatiques sont largement intégrés aux systèmes d'achats généraux de l'entreprise. Il existe des standards pour l'acquisition de ressources informatiques. Les fournisseurs de ressources informatiques sont intégrés aux mécanismes de gestion de projets de l'entreprise en ce qui concerne la gestion des contrats. Le management de l'informatique communique à l'ensemble du service le besoin d'une bonne gestion des achats et des contrats.

4 Gérée et mesurable quand

Les achats informatiques sont totalement intégrés aux systèmes d'achats généraux de l'entreprise. Les standards d'achat des ressources informatiques sont utilisés pour toutes les acquisitions. On utilise des métriques pour la gestion des contrats et des acquisitions qui sont en rapport avec les analyses de rentabilité des achats informatiques. On dispose de rapports sur les achats informatiques qui prennent en compte les objectifs des métiers. Le management est en général au courant des exceptions aux politiques et aux procédures d'acquisition informatique. La gestion stratégique des relations se développe. Le management de l'informatique fait appliquer le processus de gestion de contrats et d'acquisitions pour tous les achats en analysant les mesures de performance.

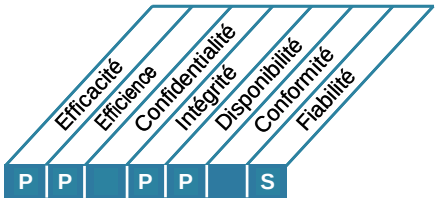
5 Optimisée quand

Le management établit des processus complets pour les achats informatiques et il fournit les ressources nécessaires. Le management impose la conformité avec les politiques et les procédures pour les acquisitions informatiques. On utilise des métriques pour la gestion des contrats et des acquisitions qui sont en rapport avec les analyses de rentabilité des achats informatiques. On a établi au fil du temps de bonnes relations avec la plupart des fournisseurs et partenaires, et on mesure et on surveille la qualité de ces relations. Les relations font l'objet d'une gestion stratégique. Les standards informatiques, les politiques et les procédures pour l'acquisition de ressources informatiques sont gérés de façon stratégique et réagissent aux mesures effectuées au cours du processus. Le management de l'informatique communique à l'ensemble du service l'importance stratégique d'une bonne gestion des achats et des contrats.

DESCRIPTION DU PROCESSUS

AI6 Gérer les changements

Tous les changements, y compris la maintenance et les correctifs d'urgence, concernant l'infrastructure et les applications de l'environnement de production sont gérés et contrôlés de façon formelle. Les changements (y compris ceux relatifs aux procédures, processus, paramètres systèmes et services) sont enregistrés dans un fichier, évalués et autorisés avant mise en place, et confrontés aux résultats attendus dès leur mise en œuvre. Cela réduit les risques de conséquences négatives pour la stabilité ou l'intégrité de l'environnement de production.



Le contrôle du processus informatique

Gérer les changements

qui répond à l'exigence des métiers vis-à-vis de l'informatique

réagir aux exigences des métiers en ligne avec la stratégie de l'entreprise, tout en réduisant les défauts des solutions et des services livrés ainsi que les reprises

en se concentrant sur

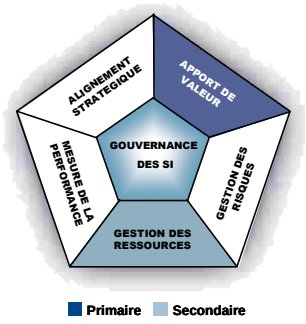
le contrôle de l'évaluation des conséquences, de l'autorisation et de la mise en place de toutes les modifications de l'infrastructure informatique, des applications et des solutions techniques ; la réduction des erreurs dues à des spécifications insuffisantes ; et l'interruption de modifications non autorisées

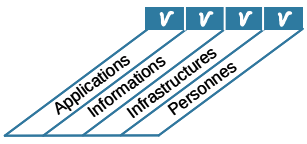
atteint son objectif en

- définissant et en communiquant les procédures de changement, y compris pour les modifications d'urgence
- évaluant les changements, définissant leurs priorités, et en les autorisant
- faisant un suivi des changements et en en rendant compte

et est mesuré par

- le nombre de perturbations ou de données erronées provoquées par des spécifications inexactes ou une évaluation insuffisante de l'impact
- un travail supplémentaire sur les applications ou sur l'infrastructure du fait de spécifications inadéquates des modifications
- le pourcentage de changements qui suivent le processus formel de contrôle des changements





OBJECTIFS DE CONTRÔLE

AI6 Gérer les changements

AI6.1 Standards et procédures de changement
Mettre en place des procédures formelles de gestion des changements pour traiter de façon standardisée toutes les demandes de modifications (y compris maintenance et correctifs) des applications, procédures, processus, paramètres systèmes et services, ainsi qu'aux plates-formes sur lesquelles ils s'appuient.

AI6.2 Évaluation de l'impact, choix des priorités et autorisation
Évaluer toutes les demandes de changements de façon structurée en terme d'impacts sur le système en exploitation et sur ses fonctionnalités. S'assurer que les changements sont classés par catégorie, par priorité et sont autorisés.

AI6.3 Modifications d'urgence
Mettre en place un processus pour définir, réaliser, tester, documenter, évaluer et autoriser les modifications d'urgence qui ne suivent pas le processus de changement établi.

AI6.4 Suivi et compte-rendu des changements
Mettre en place un système de suivi et de reporting pour documenter les changements refusés et communiquer sur la situation des changements approuvés, en cours et achevés. S'assurer que les changements approuvés sont mis en œuvre comme planifiés.

AI6.5 Clôture et documentation des changements
A chaque mise en œuvre de changement, mettre à jour les systèmes associés, la documentation utilisateur et les procédures.

GUIDE DE MANAGEMENT

AI6 Gérer les changements

De	Entrées
PO1	Portefeuille de projets informatiques
PO8	Actions pour l'amélioration de la qualité
PO9	Plans d'actions pour remédier aux risques informatiques
PO10	Principes généraux de gestion de projets et plans de projets détaillés
DS3	Changements demandés
DS5	Changements de sécurité demandés
DS8	Demande de service/demande de changement
DS9-10	Demande de changement (où et comment faire la modification)
DS10	Historique des problèmes

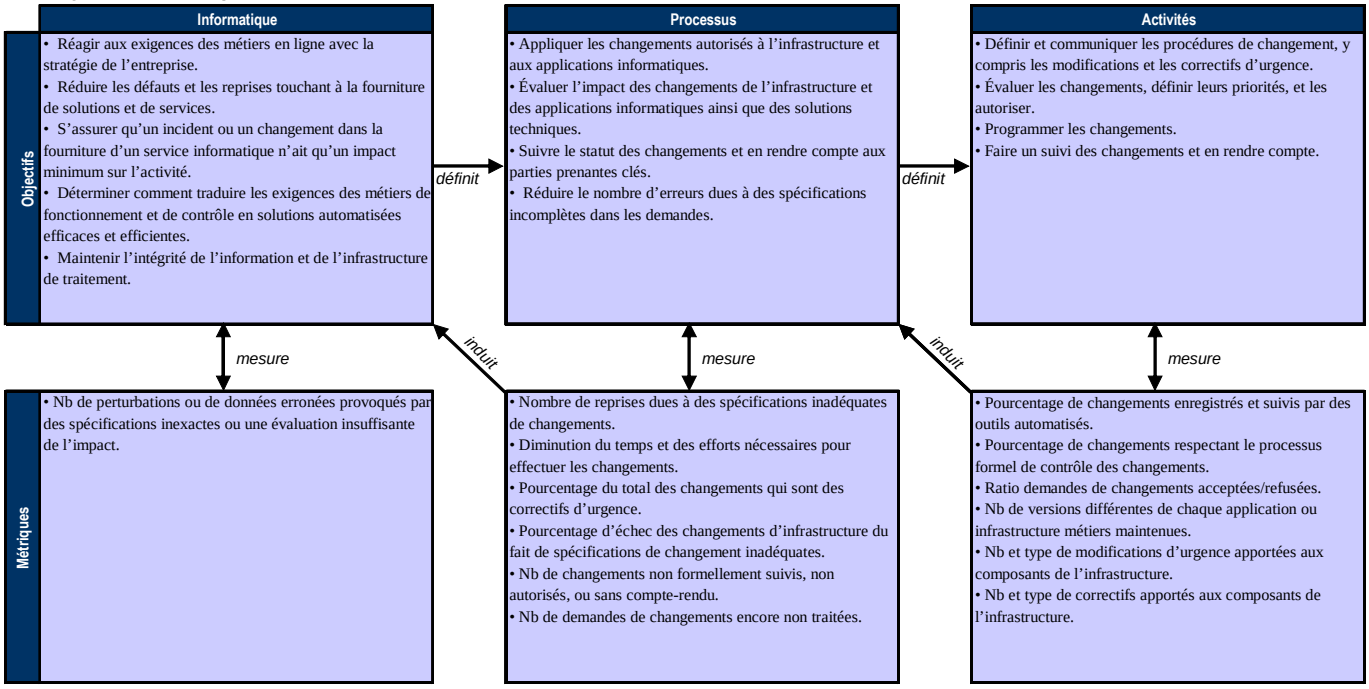
Sorties	Vers						
Modifier la description du processus	AI1…AI3						
Modifier le rapport sur le statut	SE1						
Modifier l'autorisation	AI7	DS8	DS10				

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Développer et mettre en place un processus pour enregistrer et évaluer les demandes de changements et les classer par priorités.				A	I	R	C	R	C	C	C
Évaluer l'impact des changements et définir leur priorité en fonction des besoins des métiers.				I	R	A/R	C	R	C	R	C
S'assurer que toute modification d'urgence ou critique suit le processus approuvé.				I	I	A/R	I	R			C
Autoriser les changements.				I	C	A/R		R			
Gérer et diffuser les informations utiles concernant les modifications.				A	I	R	C	R	I	R	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI6 Gérer les changements

La gestion du processus *Gérer les changements* qui répond à l'exigence des métiers vis-à-vis de l'informatique *réagir aux exigences des métiers en ligne avec la stratégie de l'entreprise, tout en réduisant les défauts des solutions et des services livrés ainsi que les reprises* est :

0 Inexistante quand

Il n'existe pas de processus défini de gestion des changements, et les changements peuvent être faits pratiquement en dehors de tout contrôle. On n'a pas conscience que les changements peuvent perturber le fonctionnement de l'informatique et celui de l'entreprise, et on n'est pas conscient non plus des bénéfices qu'apporterait une bonne gestion des changements.

1 Initialisée, au cas par cas quand

On reconnaît qu'il faudrait gérer et contrôler les changements. Les pratiques varient, et il est probable que des changements non autorisés ont lieu. La documentation des changements est pauvre ou absente, et celle de la configuration est incomplète et peu fiable. Des erreurs se produisent vraisemblablement ainsi que des interruptions dans l'environnement de production du fait d'une mauvaise gestion des changements.

2 Reproductible mais intuitive quand

Il existe un processus informel de gestion des changements, et la plupart des changements le suivent. Il est cependant mal structuré, rudimentaire, et sujet à erreurs. La documentation de la configuration n'est pas précise, et avant un changement on se contente d'une planification et d'une évaluation de l'impact limitées.

3 Définie quand

Il existe un processus défini et formel de gestion des changements qui comporte leur répartition par catégories et par priorités, les procédures d'urgence, les autorisations de changements et la gestion de leur diffusion, et on s'y conforme peu à peu. On improvise des solutions et les processus sont souvent court-circuités. Des erreurs peuvent toujours se produire, et de temps en temps des changements sont pratiqués sans autorisation. On commence à formaliser l'analyse de l'impact des changements informatiques sur les activités métiers pour soutenir le déploiement programmé de nouvelles applications et technologies.

4 Gérée et mesurable quand

Le processus de gestion des changements est bien développé et suivi avec constance dans tous les cas. Le management est convaincu qu'il n'y a qu'un minimum d'exceptions. Le processus est efficace et efficient, mais s'appuie sur de nombreuses procédures et contrôles manuels pour garantir le niveau de qualité. Tous les changements sont assujettis à une planification complète et à une évaluation d'impact de façon à minimiser la probabilité de problèmes après la mise en production. On a mis en place un processus d'approbation des changements. La documentation de la gestion des changements est bien faite et à jour, les changements étant formellement suivis de près. La documentation de la configuration est en général précise. La planification et la mise en place de la gestion des changements informatiques sont de plus en plus intégrées aux évolutions des processus métiers, de manière à s'assurer que les questions concernant la formation, les changements organisationnels, et la continuité de l'activité sont bien prises en compte. Il y a une coordination accrue entre la gestion des changements informatiques et la redéfinition des processus métiers. Il existe un processus continu de surveillance de la qualité et de la performance du processus de gestion des changements.

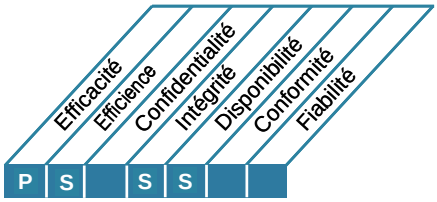
5 Optimisée quand

Le processus de gestion des changements est régulièrement révisé et mis à jour pour rester au niveau des bonnes pratiques. Le processus de revue est le reflet des résultats de la surveillance. L'information sur la configuration est informatisée et permet de contrôler les différentes versions. Le suivi des changements est élaboré et comporte des outils de détection des logiciels non autorisés et/ou sans licence. La gestion des changements informatiques est intégrée à la gestion des changements métiers pour s'assurer que l'informatique apporte un plus en productivité et en nouvelles opportunités métiers pour l'entreprise.

DESCRIPTION DU PROCESSUS

AI7 Installer et valider les solutions et les modifications

Il faut mettre en exploitation les nouveaux systèmes lorsque la phase de développement est achevée. Cela exige d'effectuer les bons tests sur les données dans un environnement dédié, de définir les instructions de déploiement et de migration, un planning de livraison et la mise en production proprement dite, et des revues après mise en place. Cela garantit que les systèmes opérationnels sont en phase avec les attentes et les résultats recherchés.



Le contrôle du processus informatique

Installer et valider les solutions et les modifications

qui répond à l'exigence suivante des métiers vis-à-vis de l'informatique

mettre en place de nouveaux systèmes ou des systèmes modifiés qui fonctionnent sans problèmes majeurs après leur installation

en se concentrant sur

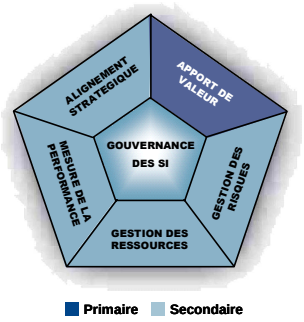
la vérification que les applications et l'infrastructure sont appropriées à l'objectif proposé et libres d'erreurs, et sur la planification de la mise en production des versions

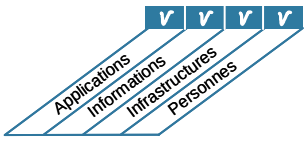
atteint son objectif en

- mettant en place une méthodologie de tests
- travaillant sur un planning des versions
- faisant évaluer et approuver les résultats de tests par le management
- effectuant des revues après la mise en œuvre

et est mesuré par

- le nombre d'applications indisponibles et de correctifs apportés du fait de tests inappropriés
- le pourcentage de systèmes qui apportent les bénéfices attendus, mesurés par le processus post-implémentation
- le pourcentage de projets accompagnés d'un plan de tests documenté et approuvé





OBJECTIFS DE CONTRÔLE

AI7 Installer et valider les solutions et les modifications

AI7.1 Formation
Former le personnel des services utilisateurs concernés et l'équipe de production informatique conformément au plan de formation défini et aux supports associés ; cette étape doit faire partie intégrante de tous les projets de développement, de mise en place ou de modification des systèmes d'information.

AI7.2 Plan de tests
Élaborer un plan de tests basé sur des standards de l'entreprise définissant les rôles, les responsabilités et les critères d'entrée et de sortie. S'assurer que le plan est approuvé par les parties concernées.

AI7.3 Plan d'implémentation
Élaborer un plan d'implémentation, de repli ou de retour en arrière. Obtenir l'approbation des parties concernées.

AI7.4 Environnement de tests
Définir et mettre en place un environnement séparé de tests sécurisé et représentatif de l'environnement de production prévu sur le plan de la sécurité, des contrôles internes, des pratiques d'exploitation, de la qualité des données, des exigences liées à la protection des données personnelles et de la charge de travail.

AI7.5 Conversion des systèmes et des données
Planifier la conversion des données et la migration d'infrastructure comme faisant partie des méthodes de développement de l'entreprise et incluant les pistes d'audit, les reprises et les retours en arrière.

AI7.6 Test des modifications
Tester les modifications unitaires conformément au plan de test défini avant la migration dans l'environnement d'exploitation. S'assurer que le plan prend en compte la sécurité et la performance.

AI7.7 Tests de recette définitive
S'assurer que les responsables des processus métiers et les parties prenantes de l'informatique évaluent les résultats du processus de test tel que défini dans le plan de test. Corriger les erreurs significatives mises en lumière par le processus de test après avoir achevé l'ensemble des tests recensés dans le plan de test ainsi que tous les tests de non régression nécessaires. Après l'évaluation, approuver la mise en production.

AI7.8 Mise en production
Après les tests, contrôler le passage en production du système modifié, en veillant à ce qu'il se réalise conformément au plan d'implémentation. Obtenir l'accord des parties prenantes clés comme les utilisateurs, le propriétaire du système et le management. Si c'est opportun, exploitez pendant un moment l'ancien système parallèlement au nouveau de façon à comparer leur fonctionnement et leurs résultats.

AI7.9 Revue post-implémentation
Dans le cadre des standards de gestion des changements de l'organisation, élaborer des procédures pour exiger une revue post-implémentation comme mentionnée dans le plan d'implémentation.

GUIDE DE MANAGEMENT

AI7 Installer et valider les solutions et les modifications

De	Entrées
PO3	Standards technologiques
PO4	Documentation sur les propriétaires de systèmes
PO8	Standards de développement
PO10	Guides de gestion de projets et plans de projets détaillés
AI3	Système configuré à tester/installer
AI4	Manuels utilisateur, d'exploitation, de support, technique et d'administration
AI5	Articles achetés
AI6	Autorisation de changement

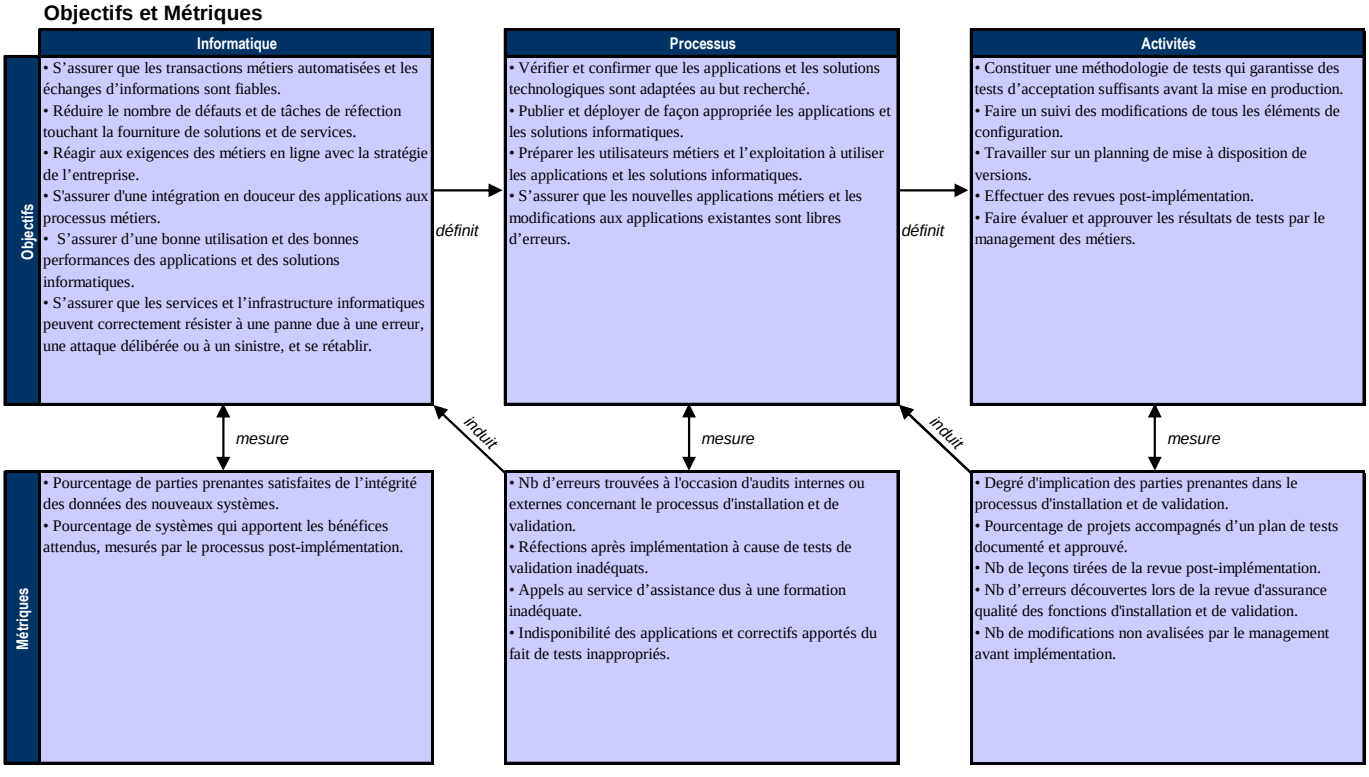
Sorties	Vers						
Éléments de configuration mis à disposition	DS8	DS9					
Erreurs connues et acceptées	AI4						
Mises en production	DS13						
Plan de publication et de diffusion de logiciel	DS13						
Revue post-démarrage	PO2	PO5	PO10				

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Construire et vérifier les plans d'implémentation.			C	A	I	C	C	R		C	C
Définir et vérifier une stratégie de tests (critères d'entrée/sortie) et une méthodologie de programme de tests.			C	A	C	C	C	R		C	C
Constituer un dossier de référence des exigences métiers et techniques, le tenir à jour, et y joindre des résultats de tests types pour les systèmes validés.				A				R			
Faire des tests d'intégration et de conversion système sur l'environnement de tests.			I	I	R	C	C	A/R		I	C
Déployer l'environnement de tests et conduire les tests de recette définitive.			I	I	R	A	C	A/R		I	C
Recommander le transfert en production selon des critères de validation approuvés.			I	R	A	R	C	R		I	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

AI7 Installer et valider les solutions et les modifications

La gestion du processus *Installer et valider les solutions et les modifications* qui répond à l'exigence des métiers *mettre en place de nouveaux systèmes ou des systèmes modifiés qui fonctionnent sans problèmes majeurs après leur installation* est :

0 Inexistante quand
Il n'y a aucun processus formel d'installation et de validation et ni la direction générale ni les informaticiens ne reconnaissent le besoin de vérifier que les solutions correspondent aux objectifs prévus.

1 Initialisée, au cas par cas quand
On est conscient du besoin de vérifier et de confirmer que les solutions permettent d'atteindre les objectifs fixés. Certains projets sont soumis à des tests, mais l'initiative des tests est laissée individuellement à chaque équipe de projet, et les approches sont différentes. La validation formelle et le visa opérationnel sont rares ou inexistants.

2 Reproductible mais intuitive quand
Les approches de tests et de validation ont une certaine cohérence, mais elles ne sont basées sur aucune méthode. Les équipes de développement décident en général individuellement de la façon de faire les tests, et il n'y a habituellement pas de système de tests d'intégration. Le processus d'approbation existe, mais il est informel.

3 Définie quand
On a mis en place une méthodologie formelle pour l'installation, la migration, la conversion et l'acceptation. Les processus d'installation et de validation sont intégrés au cycle de vie du système, et automatisés en partie. La formation, les tests, le passage en production et la validation peuvent différer du processus défini, en fonction de décisions individuelles. La qualité des systèmes qui entrent en production est variable, les nouveaux systèmes pouvant souvent générer un nombre significatif de problèmes suite à leur mise en place.

4 Gérée et mesurable quand
Les procédures sont formalisées et développées pour être bien organisées et pratiques ; les environnements de tests et les procédures de validation sont bien définis. Dans la pratique toutes les modifications majeures apportées aux systèmes suivent cette approche formalisée. On a standardisé l'évaluation des résultats permettant de savoir si les exigences des utilisateurs sont satisfaites, et on est capable de fournir des mesures qui peuvent effectivement être étudiées et analysées par le management. La qualité des systèmes entrant en production satisfait le management, et le nombre d'incidents post-implémentation reste raisonnable. L'automatisation des processus se fait au cas par cas en fonction des projets. Le management peut être satisfait du niveau d'efficacité malgré l'absence d'évaluation post-implémentation. Le système de tests reflète bien les conditions réelles. On fait subir des tests de stress aux nouveaux systèmes et des tests de non régression aux systèmes modifiés pour les projets les plus importants.

5 Optimisée quand
Les processus d'installation et de validation ont atteint le niveau des bonnes pratiques du fait d'améliorations et perfectionnements continuels. Ces processus sont pleinement intégrés au cycle de vie du système et automatisés lorsque c'est une bonne solution, ce qui donne la meilleure efficacité à la formation, aux tests, et au passage en production des nouveaux systèmes. Des environnements de tests bien développés, des relevés d'anomalies et des processus de correction de problèmes assurent une transition efficace et performante vers l'environnement de production. La validation n'implique en général pas de réfections, et les problèmes post-implémentation sont habituellement limités à des corrections mineures. Les revues post-implémentation sont elles aussi standardisées, et les enseignements qu'on en tire sont en général dirigés vers le processus pour assurer une amélioration permanente de la qualité. On fait systématiquement subir des tests de stress aux nouveaux systèmes et des tests de non régression aux systèmes modifiés.

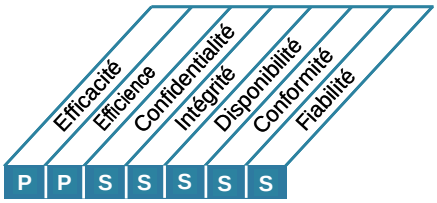
DÉLIVRER ET SUPPORTER

DS1 Définir et gérer les niveaux de services
DS2 Gérer les services tiers
DS3 Gérer la performance et la capacité
DS4 Assurer un service continu
DS5 Assurer la sécurité des systèmes
DS6 Identifier et imputer les coûts
DS7 Instruire et former les utilisateurs
DS8 Gérer le service d'assistance client et les incidents
DS9 Gérer la configuration
DS10 Gérer les problèmes
DS11 Gérer les données
DS12 Gérer l'environnement physique
DS13 Gérer l'exploitation

DESCRIPTION DU PROCESSUS

DS1 Définir et gérer les niveaux de services

Une communication efficace entre les responsables informatiques et les clients métiers à propos des services demandés est facilitée par des accords sur les services informatiques et sur les niveaux de services, et par leur définition et leur documentation. Ce processus inclut aussi la surveillance et le compte-rendu en temps utile aux parties prenantes du respect des niveaux de services convenus. Il permet l'alignement entre les services informatiques et les exigences des métiers qui s'y rapportent.



Le contrôle du processus informatique

Définir et gérer des niveaux de services

qui répond à l'exigence des métiers vis-à-vis de l'informatique

assurer l'alignement des services informatiques clés sur la stratégie des métiers

en se concentrant sur

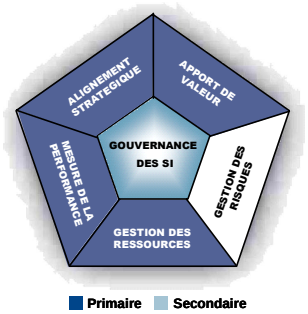
l'identification des exigences de service, l'accord sur les niveaux de services et la surveillance du respect des niveaux de services convenus

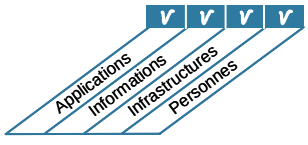
atteint son objectif en

- formalisant les accords internes et externes en tenant compte des exigences et des capacités de fourniture
- rendant compte des niveaux de services atteints (rapports et réunions)
- identifiant et en communiquant les nouvelles exigences de services et leur évolution à la planification stratégique

et est mesuré par

- le pourcentage de parties prenantes métiers satisfaites de voir les fournitures de services atteindre les niveaux convenus
- le nombre de services livrés qui ne sont pas répertoriés
- le nombre annuel de réunions avec les clients métiers destinées à la révision formelle des contrats de services





OBJECTIFS DE CONTRÔLE

DS1 Définir et gérer les niveaux de services

DS1.1 Référentiel pour la gestion des niveaux de services
Définir un cadre de référence qui propose un processus formalisé de gestion des niveaux de services entre les clients et les fournisseurs. Ce cadre veille à l'alignement continu avec les exigences des métiers et avec les priorités pour faciliter une compréhension commune entre clients et fournisseur(s). Il comporte des processus de récolte des exigences en matière de services, des définitions des services, des contrats de services, des contrats de niveau opérationnel et des sources de financement. Ces éléments sont répertoriés dans un catalogue de services. Le référentiel définit l'organisation de la gestion de niveau de service, s'intéresse aux rôles, tâches et responsabilités des fournisseurs de services internes et externes et des clients.

DS1.2 Définition des services
Fonder les définitions des services informatiques sur les caractéristiques des services et des exigences des métiers. S'assurer qu'ils sont structurés et répertoriés dans un catalogue/portefeuille de services centralisé.

DS1.3 Contrats ou conventions de services (CS)
Définir et accepter les contrats/conventions de services pour tous les services informatiques critiques, en se fondant sur les besoins du client et les capacités de l'informatique. Cela recouvre les engagements du client, les besoins d'assistance, les métriques qualitatives et quantitatives pour mesurer le service contresigné par les parties prenantes, les sources de financement et, le cas échéant, les accords commerciaux, et les rôles et responsabilités, y compris la supervision des conventions de services. Les principaux points à prendre en compte sont la disponibilité, la fiabilité, la performance, la capacité de croissance, le niveau d'assistance, la planification de la continuité, les contraintes de sécurité et de réclamation.

DS1.4 Contrats d'exploitation (CE)
Définir des contrats d'exploitation expliquant comment les services seront techniquement fournis pour appuyer le mieux possible les conventions de services. Les contrats d'exploitation doivent préciser ce que sont les processus techniques en termes compréhensibles par le fournisseur et peuvent concerner plusieurs conventions de services.

DS1.5 Surveillance et comptes-rendus des niveaux de services atteints
Surveiller en continu les critères de performance des niveaux de services. La présentation des comptes-rendus doit permettre aux parties prenantes de bien comprendre les niveaux de services atteints. Les statistiques de surveillance doivent être analysées et on y réagit pour mettre en évidence les tendances positives et négatives de chaque service, mais aussi globalement de l'ensemble des services.

DS1.6 Revue des conventions de services et des contrats
Faire une revue régulière des conventions de services et des contrats qui les accompagnent avec les fournisseurs de services internes et externes pour s'assurer qu'elles sont efficaces, à jour, et qu'on a pris en compte les modifications des exigences.

GUIDE DE MANAGEMENT

DS1 Définir et gérer les niveaux de services

De	Entrées
PO1	Plans informatiques stratégiques et tactiques, portefeuille de projets informatiques
PO2	Classifications attribuées aux données
PO5	Portefeuille actualisé des services informatiques
AI2	CS initialement prévus
AI3	CE initialement prévus
DS4	Exigences de services en cas de sinistres, y compris rôles et responsabilités
SE1	Entrée de la performance dans le planning informatique

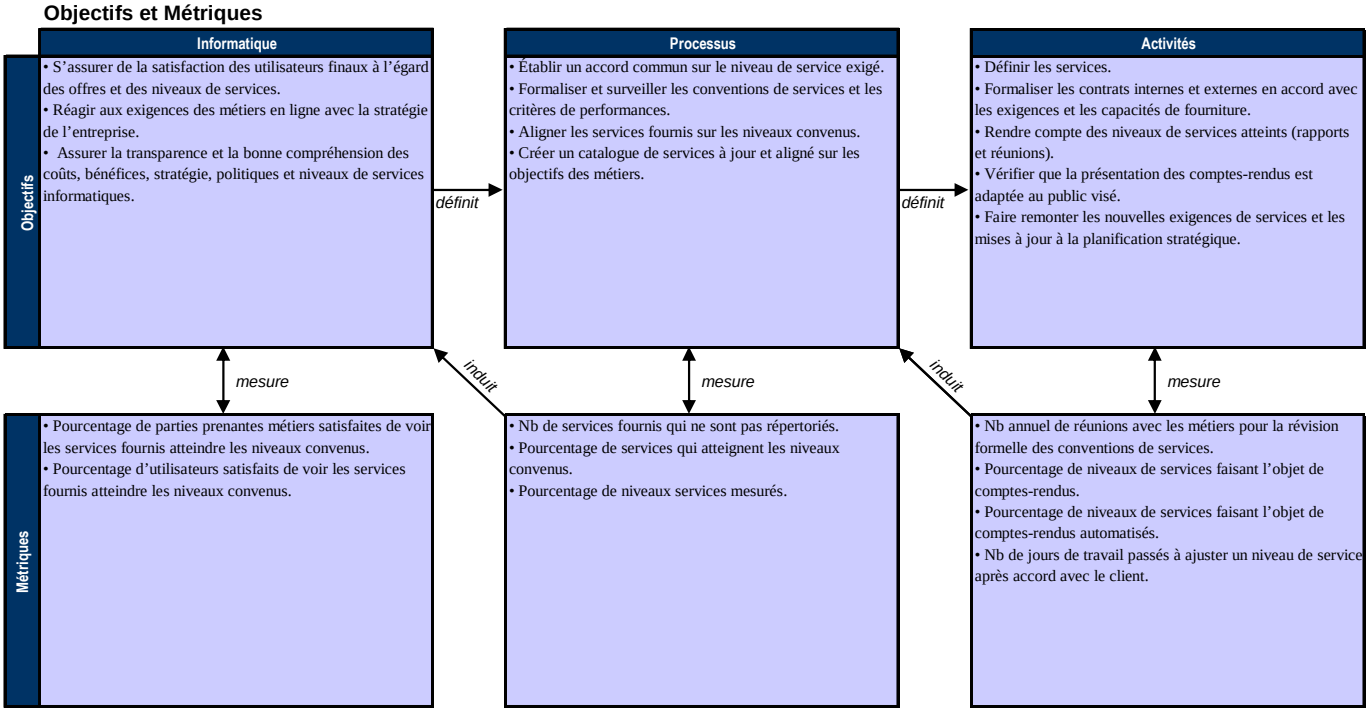
Sorties	Vers						
Rapport de revue des contrats	DS2						
Rapports sur la performance des processus	SE1						
Exigences de service nouvelles/modifiées	PO1						
CS	AI1	DS2	DS3	DS4	DS6	DS8	DS13
CE	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Portefeuille actualisé des services informatiques	PO1						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité	Chef de service
Créer un référentiel pour définir les services informatiques.			C	A	C	C	I	C	C	I	C	R
Elaborer un catalogue des services informatiques.			I	A	C	C	I	C	C	I	I	R
Définir les conventions de services pour les services informatiques critiques.		I	I	C	C	R	I	R	R	C	C	A/R
Définir les contrats d'exploitation pour atteindre les niveaux de services convenus.				I	C	R	I	R	R	C	C	A/R
Surveiller la performance des services du début à la fin et rendre compte.				I	I	R		I	I		I	A/R
Faire une revue des conventions de services et des contrats qui les supportent.		I		I	C	R		R	R		C	A/R
Faire une revue/mise à jour du catalogue des services informatiques.			I	A	C	C	I	C	C	I	I	R
Créer un plan d'amélioration des services.			I	A	I	R	I	R	C	C	I	R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS1 Définir et gérer les niveaux de services

La gestion du processus *Définir et gérer les niveaux de services* qui répond à l'exigence des métiers vis-à-vis de l'informatique *assurer l'alignement des services informatiques clés sur la stratégie des métiers* est :

0 Inexistante quand

Le management n'a pas ressenti le besoin de mettre en place un processus pour définir les niveaux de services. Les responsabilités opérationnelles et finales de leur surveillance ne sont pas attribuées.

1 Initialisée, au cas par cas quand

On a pris conscience du besoin de gérer les niveaux de services, mais le processus est informel et dépend des circonstances. Les responsabilités opérationnelle et finale de définition et de gestion des services ne sont pas attribuées. Lorsque les mesures des performances existent, elles sont qualitatives seulement, et leurs buts ne sont pas clairement définis. Les comptes-rendus sont informels, peu fréquents et peu méthodiques.

2 Reproductible mais intuitive quand

Il existe des conventions de services, mais elles ne sont ni formalisées ni révisées. Les comptes-rendus de niveaux de services sont incomplets et parfois non pertinents ou susceptibles d'induire le client en erreur. Les comptes-rendus sur les niveaux de services dépendent des compétences et des initiatives individuelles de responsables. On a engagé un coordinateur de niveaux de services et on lui a attribué des responsabilités définies, mais une autorité insuffisante. S'il existe un processus de conformité aux conventions de services, il dépend de bonnes volontés individuelles.

3 Définie quand

Les responsabilités sont bien définies, mais elles ne sont pas exercées avec méthode. Le processus de développement des conventions de services est en place, et il y a des contrôles programmés pour réévaluer les niveaux de services et la satisfaction des clients. Les services et les niveaux de services sont définis, documentés, ils font l'objet de conventions et utilisent un processus standard. Les insuffisances des niveaux de services sont identifiées, mais les procédures pour y remédier sont informelles. Le lien entre les niveaux de services attendus et le financement est clairement établi. On s'est mis d'accord sur les niveaux de services, mais ils ne correspondent pas toujours aux exigences des métiers.

4 Gérée et mesurable quand

Les niveaux de services sont de plus en plus définis au cours de la phase de définition des exigences système, et intégrés dans la conception des environnements des applications et d'exploitation. On mesure et on évalue la satisfaction des clients de façon régulière. Les mesures de performance correspondent davantage aux besoins du client qu'aux objectifs informatiques. Les mesures d'évaluation des niveaux de services se standardisent et correspondent aux normes de la profession. Les critères pour définir les niveaux de services sont basés sur ce qui est critique pour les métiers et recouvrent la disponibilité, la fiabilité, la performance, la capacité de croissance, l'assistance aux utilisateurs, la planification de la continuité, et les considérations de sécurité. On pratique l'analyse causale lorsque les niveaux de services ne correspondent pas aux attentes. Le système de comptes-rendus du suivi de niveaux de services s'automatise de plus en plus. On a défini et bien compris les risques financiers et opérationnels liés à des services qui n'atteignent pas les niveaux convenus. On a formalisé un système de métriques et on l'actualise.

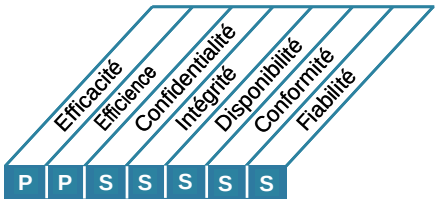
5 Optimisée quand

Les niveaux de services sont réévalués en continu pour assurer l'alignement des objectifs informatiques et métiers, ils tirent profit de l'informatique, y compris du ratio coûts/bénéfices. Tous les processus de niveaux de services font l'objet d'améliorations continues. On surveille et on gère les niveaux de satisfaction clients. Les niveaux de services convenus reflètent les objectifs stratégiques des unités métiers, et on les évalue selon les normes de la profession. Les responsables informatiques ont les ressources et la marge d'initiatives voulues pour atteindre les objectifs de niveaux de services, et le management bénéficie de primes lorsque ces objectifs sont atteints. La direction générale surveille les métriques de performance selon un processus d'amélioration continu.

DESCRIPTION DU PROCESSUS

DS2 Gérer les services tiers

Le besoin de garantir que les services fournis par des tiers (fournisseurs et partenaires) satisfont les exigences des métiers impose un processus de gestion des services tiers. Ce processus exige de définir clairement les rôles, responsabilités et les attentes dans les contrats avec des tiers, et aussi d'effectuer des revues et une surveillance de l'efficacité et de la conformité de tels contrats. Une gestion efficace des services fournis par des tiers minimise les risques métiers liés à des fournisseurs non performants.



Le contrôle du processus informatique

Gérer les services tiers

qui répond à l'exigence des métiers vis-à-vis de l'informatique

fournir des services tiers satisfaisants qui permettent une transparence sur les bénéfices, coûts et risques

en se concentrant sur

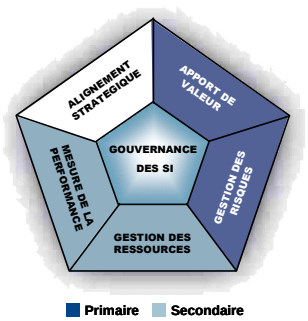
l'instauration de relations et de responsabilités bilatérales avec des tiers fournisseurs de services et sur la surveillance de la fourniture des services pour vérifier et garantir le respect des clauses contractuelles.

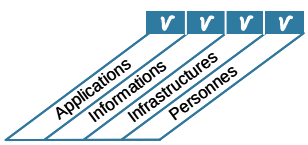
atteint son objectif en

- identifiant et en répartissant les fournisseurs de services par catégorie
- identifiant et en réduisant le plus possible les risques fournisseurs
- surveillant et en mesurant leurs performances

et est mesuré par

- le nombre de plaintes utilisateurs dues aux services tiers
- le pourcentage de fournisseurs principaux soumis à des exigences et des niveaux de services clairement définis
- le pourcentage de fournisseurs principaux objets d'une surveillance





OBJECTIFS DE CONTRÔLE

DS2 Gérer les services tiers

DS2.1 Identification des relations avec tous les fournisseurs
Identifier tous les services fournisseurs et les répartir en catégorie selon leur type, importance et niveau critique. Tenir à jour une documentation formelle des relations organisationnelles et techniques en précisant les rôles et responsabilités, les objectifs, les livrables attendus et les accréditations des représentants de ces fournisseurs.

DS2.2 Gestion des relations fournisseurs
Formaliser le processus de gestion des relations fournisseurs pour chacun d'entre eux. Les propriétaires de relations doivent intervenir sur les questions qui concernent la relation clients/fournisseurs et garantir la qualité de relations basées sur la confiance et la transparence (par ex. au moyen de conventions de services).

DS2.3 Gestion du risque fournisseurs
Identifier et réduire les risques liés à l'aptitude des fournisseurs à fournir, de manière continue, des services efficaces, sûrs et efficients. S'assurer que les contrats se conforment aux standards universels de la profession, en conformité avec les exigences légales et réglementaires. La gestion des risques doit par ailleurs prendre en compte les clauses de confidentialité, les contrats de mise sous séquestre, la viabilité du fournisseur (continuité), la conformité aux exigences de sécurité, les solutions alternatives en fourniture, les pénalités/récompenses, etc.

DS2.4 Surveillance des performances fournisseurs
Établir un processus de surveillance de la fourniture de services pour s'assurer que le fournisseur respecte les exigences des métiers en cours et qu'il continue à se conformer aux clauses de son contrat et à celles du contrat de service, et que ses performances sont concurrentielles par rapport aux autres fournisseurs et aux conditions du marché.

GUIDE DE MANAGEMENT

DS2 Gérer les services tiers

De	Entrées
PO1	Stratégie de fourniture informatique
PO8	Standards d'acquisition
AI5	Clauses contractuelles, exigences de la gestion des relations avec les tiers
DS1	Compte-rendu de revue de contrats, conventions de services
DS4	Exigences de services en cas de sinistres, y compris rôles et responsabilités

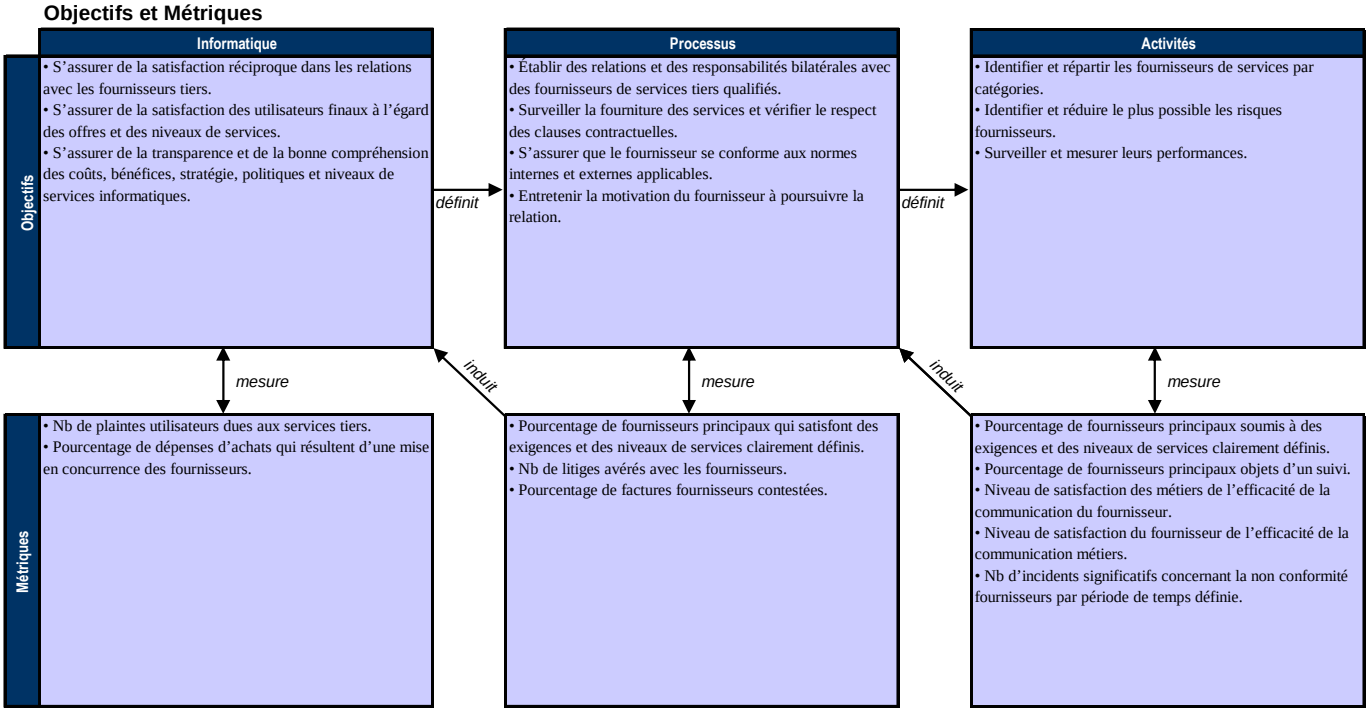
Sorties	Vers
Rapports sur la performance des processus	SE1
Catalogue fournisseurs	AI5
Risques fournisseurs	PO9

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Identifier et cataloguer les relations avec les services tiers.				I	C	R	C	R	A/R	C	C
Définir et documenter les processus de gestion des fournisseurs.		C		A	I	R	I	R	R	C	C
Établir des politiques et des procédures d'évaluation et de sélection des fournisseurs.		C		A	C	C		C	R	C	C
Identifier, évaluer et réduire le plus possible les risques fournisseurs.		I		A		R		R	R	C	C
Surveiller la fourniture de services des fournisseurs.				R	A	R		R	R	C	C
Évaluer les objectifs à long terme de la relation avec des services tiers pour toutes les parties prenantes.	C	C	C	A/R	C	C	C	C	R	C	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS2 Gérer les services tiers

La gestion du processus *Gérer les services tiers* qui répond à l'exigence des métiers vis-à-vis de l'informatique *fournir des services tiers satisfaisants qui permettent une transparence des bénéfices, des coûts et des risques* est :

0 Inexistante quand

On n'a pas défini qui est responsable de quoi et devant qui (responsabilités opérationnelles et finales). Il n'y a ni procédures ni politiques formelles concernant la passation de contrats avec des tiers. Le management ne vérifie ni n'agrée les services tiers. Les tiers ne réalisent pas de mesures de leurs activités ni ne fournissent de rapports. En l'absence d'obligations contractuelles de rendre compte, la direction générale n'est pas en mesure de connaître la qualité des services fournis.

1 Initialisée, au cas par cas quand

Le management est conscient du besoin d'avoir des politiques et des procédures documentées pour la fourniture de services par des tiers, y compris d'avoir des contrats signés. Il n'y a pas de conditions contractuelles standard pour les fournisseurs de services. La mesure du service fourni est informelle et se fait au cas par cas. Les pratiques dépendent de l'expérience individuelle et de celle du fournisseur (par ex. : fourniture à la demande).

2 Reproductible mais intuitive quand

Le processus de surveillance des fournisseurs de services tiers, des risques associés et de la fourniture de services reste informel. On signe des contrats pro forma dans les termes et conditions du fournisseur (ex. description des services à fournir). On dispose de rapports sur les services fournis, mais ils ne correspondent pas aux objectifs des métiers.

3 Définie quand

On a mis en place des procédures bien documentées pour piloter la fourniture de services par des tiers, avec des processus clairs pour définir des exigences et négocier avec les fournisseurs. Lorsqu'on a signé un contrat de services, la relation avec le tiers devient purement contractuelle. La nature des services à fournir est détaillée dans les contrats et elle inclut les exigences juridiques, opérationnelles, et de contrôle. On a attribué à quelqu'un la responsabilité de la surveillance de la fourniture de services par des tiers. Les clauses contractuelles sont empruntées à des modèles standardisés. On évalue les risques métiers liés aux services tiers et on les consigne dans des rapports.

4 Gérée et mesurable quand

On a établi des critères formels et standardisés pour définir les clauses contractuelles comme l'étendue du travail, les services/livrables à fournir, les hypothèses, les échéanciers, les coûts, les conditions de facturation et les responsabilités. On a nommé un responsable de la gestion des contrats et des fournisseurs. On vérifie en continu les qualifications, les risques et les capacités des fournisseurs. On définit les exigences de services en liaison avec les objectifs des métiers. Il existe un processus de vérification de la performance des services fournis par rapport aux termes du contrat, qui fournit des données pour évaluer les services tiers actuels et futurs. On utilise des modèles de prix de transfert dans le processus d'achat. Toutes les parties impliquées sont conscientes des attentes en ce qui concerne les services, les coûts et les principaux jalons. On a mis en place d'un commun accord des objectifs et des métriques pour la supervision des fournisseurs de services.

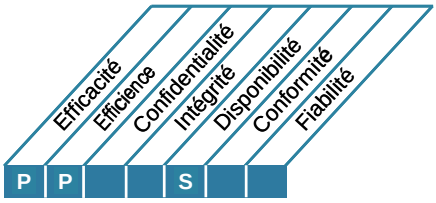
5 Optimisée quand

On fait une revue des contrats signés avec des tiers selon une fréquence prédéfinie. On a nommé un responsable de la gestion des fournisseurs et de la qualité des services fournis. On surveille que les contrats respectent les dispositions de conformité opérationnelle, juridique et de contrôle et on impose les corrections nécessaires. Le tiers est soumis à des revues indépendantes périodiques, et on obtient des retours d'information sur la performance, utilisés pour améliorer la fourniture de services. Les mesures choisies varient en fonction des changements des conditions d'exercice de l'activité. Les métriques permettent de détecter rapidement les problèmes qui peuvent se poser avec des services tiers. L'établissement de rapports définis et complets sur les niveaux de services est lié à la rétribution du tiers. Le management ajuste le processus d'acquisition et de surveillance de services tiers d'après les résultats des indicateurs de mesure.

DESCRIPTION DU PROCESSUS

DS3 Gérer la performance et la capacité

La bonne gestion des performances et des capacités des ressources informatiques exige qu'un processus les passe régulièrement en revue. Ce processus comporte la prévision des besoins futurs en fonction des exigences de charge de travail, de stockage et des imprévus. Ce processus assure que les ressources informatiques qui appuient les exigences des métiers sont constamment disponibles.



Le contrôle du processus informatique

Gérer la performance et la capacité

qui répond à l'exigence des métiers vis-à-vis de l'informatique

optimiser la performance de l'infrastructure, des ressources et des capacités informatiques pour satisfaire les exigences des métiers

en se concentrant sur

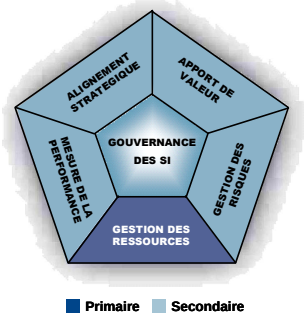
le respect du temps de réponse prévu dans les conventions de services, la réduction des périodes d'indisponibilité et l'amélioration continue des performances et des capacités informatiques grâce à la surveillance et aux mesures

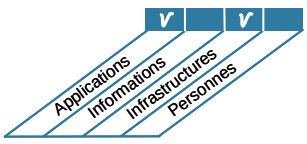
atteint son objectif en

- planifiant la capacité et la disponibilité des systèmes et en y subvenant
- surveillant les performances systèmes et en en rendant compte
- modélisant et en prévoyant les performances systèmes

et est mesuré par

- le nombre d'heures perdues par mois par les utilisateurs du fait d'une planification insuffisante des capacités
- le pourcentage de pics qui dépassent les seuils d'utilisation
- le pourcentage des temps de réponse prévus dans les conventions qui sont dépassés





OBJECTIFS DE CONTRÔLE

DS3 Gérer la performance et la capacité

DS3.1 Planification de la performance et de la capacité
Établir un processus de planification pour la revue des performances et des capacités des ressources informatiques pour garantir que des capacités et des performances sont disponibles à des coûts justifiés pour traiter les charges de travail convenues et déterminées par les conventions de niveaux de services. Les plans de capacité et de performance doivent mobiliser les techniques de modélisation appropriées pour proposer un modèle de performance, de capacité et de débit, actuels et prévus des ressources informatiques.

DS3.2 Performance et capacité actuelles
Évaluer les performances et les capacités des ressources informatiques pour déterminer si elles sont suffisantes pour satisfaire aux conventions de services signées.

DS3.3 Performance et capacité futures
Faire à intervalles réguliers des prévisions de performance et de capacité des ressources informatiques pour réduire le risque d'interruption de service à cause de la dégradation de leurs performances et de l'insuffisance de leurs capacités. Relever les excès de capacité pour un éventuel redéploiement. Relever les tendances de la charge de travail et déterminer les prévisions à inclure dans les plans de performance et de capacité.

DS3.4 Disponibilité des ressources informatiques
Fournir les capacités et les performances requises en prenant en compte des caractéristiques comme les charges de travail normales, les imprévus, les exigences de stockage et les cycles de vie des ressources informatiques. Il faut prévoir des dispositions telles qu'un classement des tâches par priorité, des machines à tolérance de pannes et des allocations de ressources. Le management doit s'assurer que les plans d'urgence peuvent correctement faire face à des problèmes de disponibilité, de capacité et de performance des ressources informatiques individuelles.

DS3.5 Surveillance et comptes-rendus
Surveiller en continu les performances et les capacités des ressources informatiques. Les données recueillies doivent servir à deux objectifs :
- Maintenir et ajuster les performances actuelles de l'informatique et traiter des questions comme la résilience, les imprévus, les charges de travail actuelles et futures, les plans d'archivage et l'acquisition de ressources.
- Rendre compte de la disponibilité des services livrés aux métiers comme le prévoient les conventions de services.

Assortir tous les rapports d'incidents de recommandations pour les résoudre.

GUIDE DE MANAGEMENT

DS3 Gérer la performance et la capacité

De	Entrées
AI2	Spécifications de disponibilité, continuité et récupération
AI3	Exigences de surveillance des systèmes
DS1	CS

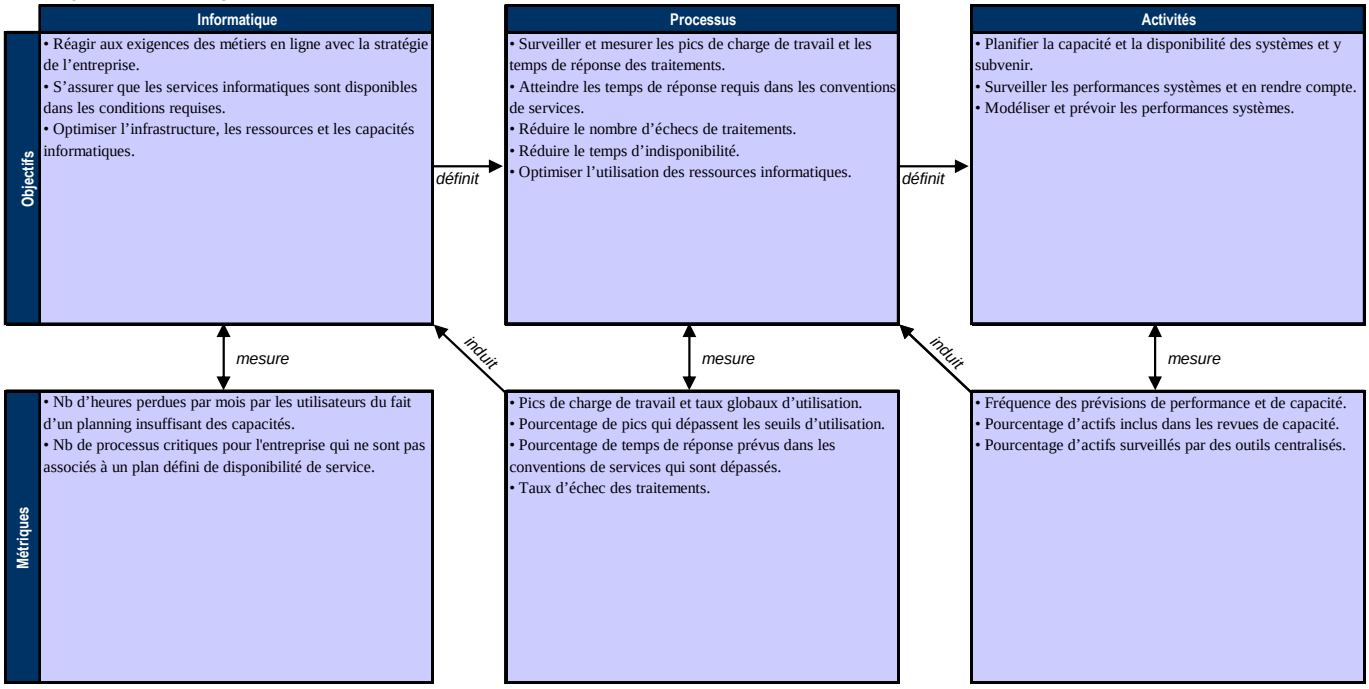
Sorties	Vers						
Information sur la performance et la capacité	PO2	PO3					
Plan de performance et capacité (exigences)	PO5	AI1	AI3	SE1			
Changements requis	AI6						
Rapports sur la performance des processus	SE1						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Mettre en place un processus pour planifier les revues de performance et de capacité des ressources informatiques.				A		R	C	C	C	C	
Réviser les performances et les capacités actuelles des ressources informatiques.				C	I	A/R		C	C	C	
Faire des prévisions de performance et de capacité des ressources informatiques.				C	C	A/R	C	C	C	C	
Faire des analyses d'écarts pour identifier les insuffisances des ressources informatiques.				C	I	A/R		R	C	C	I
Faire un plan d'urgence pour les indisponibilités potentielles des ressources informatiques.				C	I	A/R		C	C	I	C
Surveiller en continu et rendre compte de la disponibilité, de la performance et de la capacité des ressources informatiques.				I	I	A/R		I	I	I	I

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS3 Gérer la performance et la capacité

La gestion du processus *Gérer la performance et la capacité* qui répond à l'exigence des métiers vis-à-vis de l'informatique *optimiser la performance de l'infrastructure, des ressources et des capacités informatiques pour satisfaire les exigences des métiers* est :

0 Inexistante quand

Le management ne réalise pas que les processus clés de l'entreprise peuvent exiger de l'informatique de hauts niveaux de performance, ou que les besoins globaux de l'entreprise en services informatiques peuvent excéder la capacité de l'infrastructure existante. Il n'y a pas de processus de planification de la capacité.

1 Initialisée, au cas par cas quand

Les utilisateurs conçoivent des solutions de contournement pour répondre aux contraintes de puissance et de capacité. Les besoins de planification de la capacité et de la performance sont mal appréciés par les propriétaires des processus métiers. Les initiatives pour gérer la performance et la capacité sont typiquement provoquées par une situation particulière. Le processus de planification de la capacité et de la performance est informel. On a une connaissance limitée des capacités et des performances des ressources informatiques actuelles et des besoins futurs.

2 Reproductible mais intuitive quand

Le management des métiers et de l'informatique est conscient des conséquences de l'absence de gestion de la performance et de la capacité. On dispose en général des niveaux de performance nécessaires, grâce à l'évaluation faite sur des systèmes individuels et aux connaissances des équipes d'assistance et de projets. Certains outils individuels peuvent être utilisés pour diagnostiquer les problèmes de performance et de capacité, mais la cohérence des résultats dépend de l'expertise d'individus clés. Il n'y a pas d'évaluation globale du niveau de performance possible des SI, ou d'anticipation de situations de dépassement ou de crise. Des problèmes de disponibilité se produiront vraisemblablement de façon inattendue et aléatoire, ce qui fera perdre beaucoup de temps en diagnostic et en correction. Toute mesure de performance se base d'abord sur les besoins de l'informatique et non sur ceux du client.

3 Définie quand

Les exigences de performance et de capacité sont définies pour la durée du cycle de vie du système. On a défini des exigences de niveaux de services et les métriques qui peuvent être utilisées pour mesurer la performance opérationnelle. On a modélisé les exigences futures de performance et de capacité selon un processus défini. On produit des rapports sur les statistiques de performance. Il y a toujours une probabilité d'anomalies liées à la performance et à la capacité dont la correction prendra du temps. Malgré les niveaux de services publiés, les utilisateurs et les clients peuvent être parfois sceptiques sur la capacité de service.

4 Gérée et mesurable quand

On dispose de processus et d'outils pour mesurer l'utilisation, la performance et la capacité des systèmes, et on compare les résultats aux objectifs définis. On dispose aussi d'informations à jour qui donnent des statistiques normalisées sur la performance et qui alertent sur des incidents provoqués par des performances ou des capacités insuffisantes. On utilise des procédures définies et standardisées pour traiter les insuffisances de performance ou les problèmes de capacité. On utilise des outils automatisés pour surveiller des ressources spécifiques comme l'espace disque, les réseaux, les serveurs, et les passerelles réseau. Les statistiques de performance et de capacité font l'objet de comptes-rendus en termes de processus métiers de façon à ce que les utilisateurs et les clients comprennent les niveaux de services informatiques. Les utilisateurs se disent en général satisfaits de la capacité de service offerte et sont susceptibles d'exiger de nouveaux ou de meilleurs niveaux de disponibilité. On s'est mis d'accord sur des métriques pour évaluer la performance et la capacité des SI mais il est possible qu'on ne les utilise que sporadiquement et sans méthode.

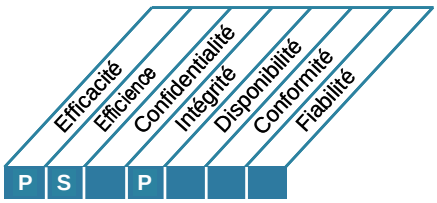
5 Optimisée quand

Les plans de performance et de capacité sont tout à fait synchronisés avec les prévisions d'exigences des métiers. L'infrastructure technologique et les exigences des métiers sont sujettes à des revues régulières pour s'assurer qu'on atteint la capacité optimale au meilleur prix. On a standardisé et on utilise sur les différentes plates-formes les outils de surveillance des ressources informatiques critiques, et on les a intégrés au système de gestion des incidents de l'entreprise. Des outils de surveillance détectent et peuvent automatiquement corriger des problèmes de performance et de capacité. L'analyse des tendances fait apparaître les baisses imminentes de performance causées par une augmentation des volumes d'activité, ce qui permet de s'organiser et d'éviter les imprévus. Les métriques d'évaluation de la performance et de la capacité des SI sont bien ajustées en termes de mesures de résultat et d'indicateurs de performance pour tous les processus métiers critiques et elles fournissent des mesures en continu. Le management ajuste la planification de la performance et de la capacité en fonction de l'analyse de ces mesures.

DESCRIPTION DU PROCESSUS

DS4 Assurer un service continu

Le besoin d'assurer la continuité des services informatiques exige de développer, de maintenir et de tester des plans de continuité des SI, d'utiliser des capacités de stockage de sauvegardes hors site et d'assurer une formation périodique au plan de continuité. Un processus de service continu efficace réduit les risques et les conséquences d'une interruption majeure des services informatiques aux fonctions et processus métiers clés.



Le contrôle du processus informatique

Assurer un service continu

qui répond à l'exigence des métiers vis-à-vis de l'informatique

s'assurer qu'une interruption d'un service informatique n'ait qu'un impact minimal sur les métiers

en se concentrant sur

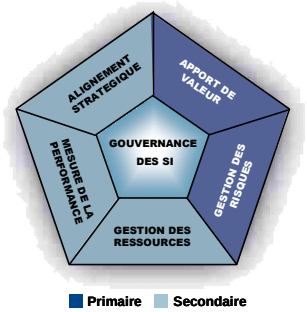
donner une capacité de résistance aux solutions automatisées et développer, tenir à jour et tester les plans de continuité des SI

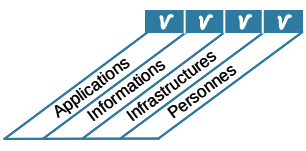
atteint son objectif en

- développant et en actualisant/améliorant les plans de secours des SI
- s'exerçant sur les plans de secours des SI et en les testant
- stockant hors site des copies des plans de secours et des données

et est mesuré par

- le nombre d'heures perdues par mois par les utilisateurs du fait d'interruptions imprévues
- le nombre de processus métiers critiques dépendants des SI qui ne sont pas pris en compte par le plan de continuité des SI





OBJECTIFS DE CONTRÔLE

DS4 Assurer un service continu

DS4.1 Référentiel de continuité informatique
Développer un cadre de référence de la continuité informatique pour assister la gestion de la continuité des activités métiers dans l'ensemble de l'entreprise selon un processus cohérent. L'objectif de ce cadre de référence doit aider à déterminer la résilience requise de l'infrastructure et inciter au développement d'un plan de secours informatique. Il doit prendre en compte la structure de gestion de la continuité de l'entreprise, couvrir les rôles, tâches et responsabilités des fournisseurs de services internes et externes, leur management et leurs clients, et les processus d'élaboration des règles et des structures pour documenter, tester et mettre en œuvre les plans de reprise et de secours informatique. Ce plan doit aussi traiter des questions comme l'identification des ressources critiques, des interdépendances clés, la surveillance et les comptes-rendus sur la disponibilité des ressources critiques, les traitements alternatifs, et les principes de sauvegarde et de restauration.

DS4.2 Plans de continuité informatique
En se basant sur le référentiel, développer des plans de continuité des SI destinés à réduire les conséquences d'une perturbation majeure des fonctions et processus métiers clés. Les plans doivent tenir compte d'une évaluation du risque en termes d'impacts potentiels pour les métiers et doivent traiter des exigences de résilience, des traitements alternatifs et des capacités de restauration pour tous les services informatiques critiques. Ils doivent aussi prendre en compte les guides de mise en oeuvre, les rôles et responsabilités, les procédures, les processus de communication et les modalités de tests.

DS4.3 Ressources informatiques critiques
Concentrer l'attention sur les éléments considérés comme les plus vitaux dans le plan de continuité des SI pour en renforcer la capacité de résilience et établir les priorités lorsqu'on est dans une situation de reprise. Éviter de perdre du temps à récupérer les éléments les moins importants et tenir compte des priorités des besoins métiers pour la réaction et la reprise ; s'assurer aussi que les coûts restent à un niveau acceptable et se conformer aux exigences réglementaires et contractuelles. Prendre en compte les exigences de durée en matière de résilience, réactivité et reprise pour différents laps de temps, par ex. 1 à 2 heures, 4 à 24 heures, plus de 24 heures et les périodes critiques d'exploitation des métiers.

DS4.4 Maintenance du plan de continuité des SI
Encourager la direction informatique à définir et à mettre en œuvre des procédures de contrôle des modifications pour s'assurer que le plan de continuité des SI est maintenu à jour et reflète en continu les véritables exigences métiers. Communiquer clairement et en temps opportun les modifications de procédures et de responsabilités.

DS4.5 Tests du plan de continuité des SI
Tester régulièrement le plan de continuité des SI pour s'assurer qu'on peut restaurer efficacement les systèmes informatiques, qu'on traite les anomalies et que le plan reste pertinent. Cela exige de faire une préparation minutieuse, de documenter les tests, de rendre compte des résultats, et de mettre en place un plan d'action en fonction de ces résultats. Envisager d'étendre les tests de restauration d'applications individuelles à des scénarios de tests intégrés, à des tests exhaustifs et à l'intégration de tests fournisseurs.

DS4.6 Formation au plan de continuité des SI
Assurer pour toutes les parties concernées des sessions de formation périodiques sur les procédures et sur leurs rôles et responsabilités en cas d'incident ou de sinistre. Vérifier et améliorer la formation en fonction des résultats des tests de situations d'urgence.

DS4.7 Diffusion du plan de continuité des SI
Vérifier ou faire en sorte qu'il existe une stratégie de diffusion définie et gérée, pour s'assurer que tous les plans sont distribués de façon sûre et qu'ils sont disponibles pour les parties dûment autorisées et intéressées, à l'endroit et au moment où elles en ont besoin. Bien vérifier que les plans soient accessibles selon tous les scénarios de sinistres.

DS4.8 Reprise et redémarrage des services informatiques
Prévoir les actions à entreprendre pendant la période de reprise et de redémarrage des services informatiques. Cela peut concerner l'activation de sites de secours, le lancement de traitements alternatifs, la communication en direction des parties prenantes et des clients, les procédures de redémarrage etc. S'assurer que les métiers comprennent les délais de restauration et les investissements informatiques nécessaires pour faire face aux besoins de reprise et de redémarrage des métiers.

DS4.9 Stockage de sauvegardes hors site
Stocker hors site tous les supports de sauvegarde critiques, la documentation et les autres ressources informatiques nécessaires à la reprise des SI et aux plans de continuité métiers. Le contenu de ce stockage de sauvegarde doit être déterminé par une collaboration entre les propriétaires des processus métiers et le personnel informatique. Les responsables de l'installation de stockage hors site doivent s'aligner sur la politique de classification des données et sur les pratiques de stockage des supports de l'entreprise. La direction informatique doit s'assurer que les équipements hors site sont évalués périodiquement, au moins annuellement, en ce qui concerne leur contenu, leur protection vis-à-vis de l'environnement, et leur sécurité. S'assurer que la compatibilité des matériels et de logiciels permet de restaurer les données archivées, et tester et rafraîchir périodiquement les archives.

DS4.10 Revue après redémarrage
Vérifier si la direction informatique a mis en place des procédures pour évaluer l'adéquation du plan de reprise de l'informatique dans de bonnes conditions après un sinistre et mettre à jour le plan en conséquence.

GUIDE DE MANAGEMENT

DS4 Assurer un service continu

De	Entrées
PO2	Classifications attribuées aux données
PO9	Évaluation des risques
AI2	Spécifications de disponibilité, continuité et reprise
AI4	Manuels utilisateur, d'assistance, technique et d'administration
DS1	CS et CE

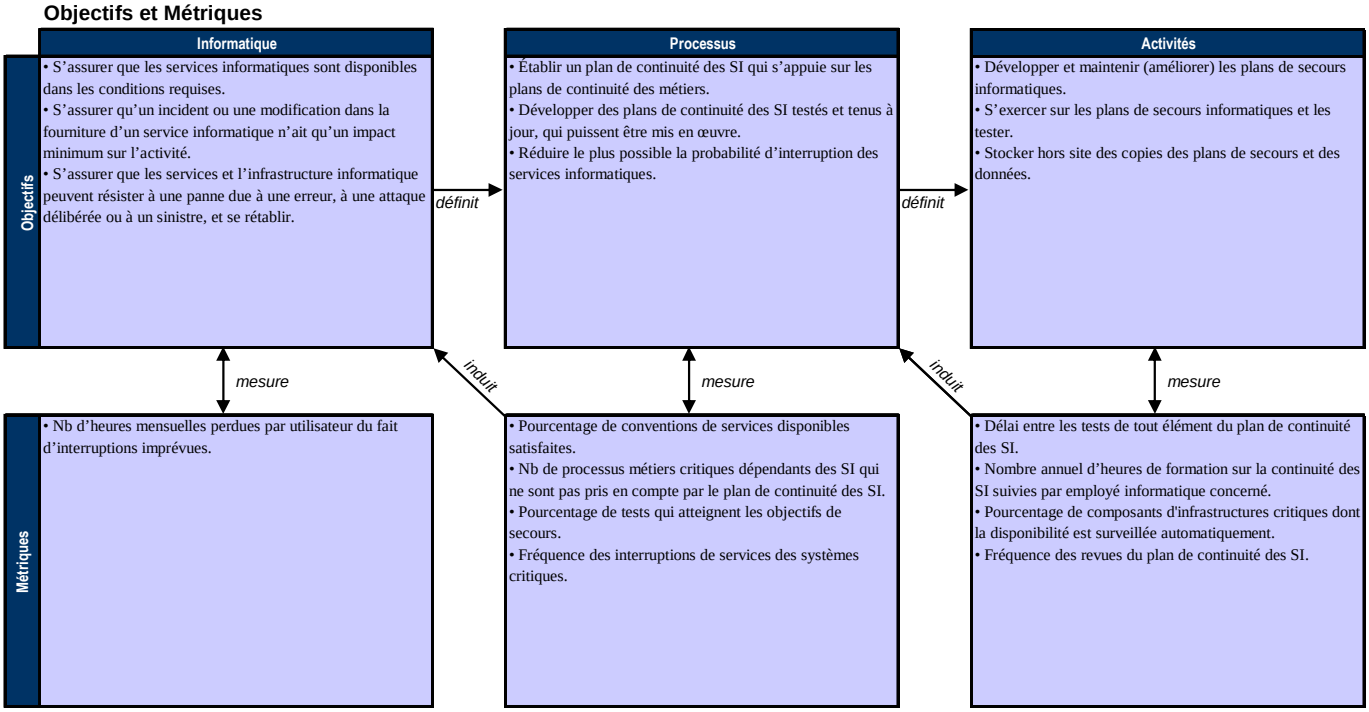
Sorties	Vers						
Résultats des tests de secours	PO9						
Eléments de configuration informatique critiques	DS9						
Plan de stockage et de protection hors site	DS11	DS13					
Seuils incidents/sinistres	DS8						
Exigences de service en cas de sinistres, y compris rôles et responsabilités	DS1	DS2					
Rapports sur la performance des processus	SE1						

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Développer un référentiel de continuité des SI.		C	C	A	C	R	R	R	C	C	R
Réaliser des analyses d'impact et des évaluations des risques au niveau des métiers.		C	C	C	C	A/R	C	C	C	C	C
Développer et maintenir les plans de continuité des SI.	I	C	C	C	I	A/R		C	C	C	C
Identifier et répartir par catégories les ressources informatiques en fonction des objectifs de reprise.				C		A/R		C	I	C	I
Définir et mettre en œuvre des procédures de contrôle des changements pour s'assurer que le plan de continuité des SI est à jour.				I		A/R		R	R	R	I
Tester régulièrement le plan de continuité des SI.				I	I	A/R		C	C	I	I
Élaborer un plan d'actions à entreprendre à la suite des résultats des tests.				C	I	A/R	C	R	R	R	I
Planifier et mettre en œuvre la formation à la continuité des SI.				I	R	A/R		C	R	I	I
Planifier la reprise et le redémarrage des services informatiques.		I	I	C	C	A/R	C	R	R	R	C
Planifier et mettre en place le stockage et la protection des sauvegardes.				I		A/R		C	C	I	I
Élaborer des procédures pour conduire des revues après reprise.				C	I	A/R		C	C		C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS4 Assurer un service continu

La gestion du processus *Assurer un service continu* qui répond à l'exigence des métiers vis-à-vis de l'informatique *s'assurer qu'une interruption d'un service informatique n'ait qu'un impact minimal sur les métiers* est :

0 Inexistante quand

On n'a pas conscience des risques, ni des menaces qui pèsent sur l'informatique, de ses points vulnérables, ni de l'impact d'une perte de services informatiques sur les métiers. On ne considère pas que la continuité des services doive mobiliser l'attention du management.

1 Initialisé, au cas par cas quand

Les responsabilités pour assurer un service continu sont informelles, et l'autorité pour exercer ces responsabilités est limitée. Le management commence à prendre conscience du besoin d'une continuité des services, et des risques liés au manque de continuité. L'attention que prête le management à la continuité se porte davantage sur les ressources de l'infrastructure que sur les services informatiques. Les utilisateurs mettent en place des solutions de contournement lorsque le service s'interrompt. Les réponses de l'informatique aux interruptions majeures de continuité dépendent des circonstances et ne sont pas préparées. On programme des interruptions de services en fonction des besoins de l'informatique mais elles ne tiennent pas compte des exigences des métiers.

2 Reproductible mais intuitive quand

On a nommé des responsables de la continuité des services. Les approches du problème sont fragmentaires. Les rapports sur la disponibilité des systèmes sont sporadiques, éventuellement incomplets, et ne prennent pas en compte l'impact sur les métiers. Il n'existe pas de plans de continuité des SI documentés, bien qu'il y ait un engagement à assurer un service continu et qu'on en connaisse les principes essentiels. Un inventaire des systèmes et des composants critiques existe, mais il n'est pas toujours fiable. On voit émerger des pratiques de service continu, mais leur succès repose sur certaines personnes.

3 Définie quand

Il n'y a pas d'ambiguïté sur la responsabilité finale de la gestion de la continuité. On a clairement défini et attribué les responsabilités opérationnelles de la planification et des tests de continuité des services. Les plans de continuité des SI sont documentés et axés sur les points vitaux des systèmes et sur l'impact pour les métiers. Les tests de continuité de services donnent lieu à des rapports réguliers. Certaines personnes prennent l'initiative de suivre les normes et de recevoir une formation pour affronter des incidents majeurs ou des sinistres. Le management communique constamment sur la nécessité d'un plan de continuité des services. On utilise des composants de haute disponibilité et des systèmes redondants. On tient à jour un inventaire des systèmes et composants les plus vitaux.

4 Gérée et mesurable quand

On impose les responsabilités et les standards du service continu. Les responsables de la maintenance du plan de continuité sont désignés. Les activités de maintenance se basent sur les résultats des tests de service continu, sur les bonnes pratiques internes et sur les évolutions de l'environnement informatique et métiers. On recueille dans une base structurée des informations sur la continuité des services, on les analyse, on élabore des rapports et on agit en conséquence. Il existe une formation formalisée et obligatoire sur les processus de service continu. On déploie systématiquement les bonnes pratiques de disponibilité des systèmes. Les pratiques de redondance et de planification de la continuité des services s'influencent réciproquement. Les incidents de rupture de continuité sont répartis par catégorie et les procédures d'escalade graduelles pour y remédier sont bien connues de toutes les personnes concernées. On a développé et fait adopter des objectifs et des métriques pour la continuité des services, mais ils ne sont pas toujours systématiquement mesurés.

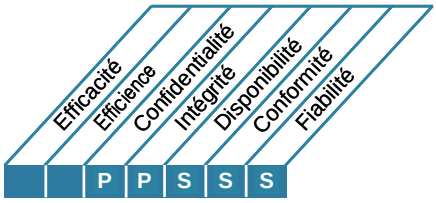
5 Optimisée quand

Les processus intégrés de continuité de services tiennent compte des tests comparatifs et des meilleures pratiques externes. Le plan de continuité des SI est intégré aux plans de continuité des métiers et il est systématiquement tenu à jour. On s'assure auprès des vendeurs et des fournisseurs principaux qu'ils respecteront les exigences de continuité des services. On pratique des tests globaux du plan de continuité des SI, et leurs résultats servent à mettre le plan à jour. On utilise la collecte et l'analyse de données pour l'amélioration continue du processus. Les pratiques de disponibilité et de service continu sont complètement alignées. Le management vérifie qu'un sinistre ou un incident majeur ne se produiront pas du fait d'un seul maillon faible. On comprend et on applique complètement les procédures d'escalade. On évalue systématiquement les objectifs et les métriques qui concernent les résultats du service continu. Le management ajuste les plans de continuité des services en fonction du résultat des mesures.

DESCRIPTION DU PROCESSUS

DS5 Assurer la sécurité des systèmes

Le besoin de maintenir l'intégrité de l'information et de protéger les actifs informatiques exige un processus de gestion de la sécurité. Ce processus comporte la mise en place et la maintenance de rôles et responsabilités, politiques, plans et procédures informatiques. La gestion de la sécurité implique aussi une surveillance de la sécurité, des tests périodiques et des actions correctives lors d'incidents ou de découverte de failles dans la sécurité. Une gestion efficace de la sécurité protège tous les actifs informatiques pour réduire le plus possible les conséquences de vulnérabilités et d'incidents de sécurité.



Le contrôle du processus informatique

Assurer la sécurité des systèmes

qui répond à l'exigence des métiers vis-à-vis de l'informatique

maintenir l'intégrité de l'information et de l'infrastructure technologique et réduire au maximum les conséquences de failles et d'incidents de sécurité

en se concentrant sur

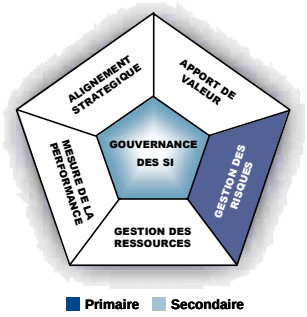
la définition de politiques, de procédures et de plans de sécurité informatique, et la surveillance et la détection des vulnérabilités et des incidents de sécurité, leur résolution et leur compte-rendu

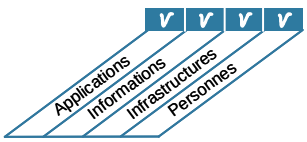
atteint son objectif en

- comprenant les exigences, les vulnérabilités et les menaces de sécurité
- gérant les identités et les autorisations des utilisateurs de façon standardisée
- testant régulièrement la sécurité

et est mesuré par

- le nombre d'incidents qui portent atteinte à la réputation de l'entreprise
- le nombre de systèmes qui ne répondent pas aux exigences de sécurité
- le nombre de manquements au principe de séparation des tâches





OBJECTIFS DE CONTRÔLE

DS5 Assurer la sécurité des systèmes

DS5.1 Gestion de la sécurité informatique
Gérer la sécurité informatique au plus haut niveau approprié de l'entreprise, de façon à ce que la gestion des actions de sécurité soit alignée sur les exigences des métiers.

DS5.2 Plan de sécurité informatique
Traduire les exigences des métiers, des risques et de la conformité dans un plan global de sécurité informatique tenant compte de l'infrastructure informatique et de la culture de la sécurité. S'assurer que le plan se décline en politiques et procédures de sécurité assorties des investissements appropriés en services, personnels, logiciels et matériels. Communiquer les politiques et les procédures de sécurité aux parties prenantes et aux utilisateurs.

DS5.3 Gestion des identités
S'assurer que tous les utilisateurs (internes, externes et temporaires) et leur action sur les systèmes informatiques (applications métiers, environnement informatique, exploitation, développement et maintenance des systèmes) sont identifiables sans ambiguïté. Gérer les identités à l'aide de systèmes d'authentification. S'assurer que les droits d'accès des utilisateurs aux systèmes et aux données sont en accord avec des besoins métiers définis et documentés et que des profils de fonctions sont attachés aux identités. S'assurer que les droits d'accès des utilisateurs sont demandés par leur management, approuvés par le propriétaire du système et mis en place par la personne responsable de la sécurité. Tenir à jour les identités et les droits d'accès des utilisateurs dans un entrepôt de données centralisé. Déployer et maintenir opérationnelles au meilleur coût des techniques et des procédures pour créer l'identité des utilisateurs, mettre en œuvre leur authentification et pour faire respecter les droits d'accès.

DS5.4 Gestion des comptes utilisateurs
Disposer de procédures de gestion des comptes utilisateurs permettant de traiter les demandes, attributions, ouvertures, suspensions, modifications et clôtures des comptes utilisateurs et des droits associés. Y inclure une procédure d'approbation spécifiant le nom du propriétaire des données ou du système qui attribue les droits d'accès. Ces procédures doivent s'appliquer à tous les utilisateurs, y compris les administrateurs (utilisateurs privilégiés), les utilisateurs internes et externes, dans les circonstances normales ou dans les cas d'urgence. Les droits et obligations relatifs à l'accès aux systèmes et aux données de l'entreprise doivent faire l'objet d'accord contractuel avec tous les types d'utilisateurs. Effectuer une revue régulière de la gestion de tous les comptes et des privilèges associés.

DS5.5 Tests de sécurité, vigilance et surveillance
Tester et surveiller de façon proactive la mise en place de la sécurité informatique. Pour s'assurer que la sécurité informatique se maintient au niveau convenu il faut revoir et renouveler en temps voulu sa validation. Une fonction de surveillance des identifications doit permettre une prévention /détection rapide suivie d'un rapport en temps voulu des activités inhabituelles/anormales qu'il peut être nécessaire de traiter.

DS5.6 Définition des incidents de sécurité
Définir clairement et communiquer les caractéristiques des incidents de sécurité potentiels de façon à ce que ceux-ci soient classifiés et traités comme il convient par le processus de gestion des incidents et des problèmes.

DS5.7 Protection de la technologie de sécurité
Rendre résistants à des tentatives d'intrusion les composants de sécurité et ne pas divulguer la documentation sur la sécurité inutilement.

DS5.8 Gestion des clefs de chiffrement
S'assurer que sont en place des politiques et des procédures pour gérer la génération, la modification, la révocation, la destruction, la distribution, la certification, le stockage, l'entrée, l'utilisation et l'archivage de clés de chiffrement afin de garantir leur protection contre toute modification ou divulgation non autorisée.

DS5.9 Prévention, détection et neutralisation des logiciels malveillants
Mettre en place des mesures de prévention, détection et neutralisation (en particulier des correctifs de sécurité et des anti-virus à jour) dans l'ensemble de l'entreprise pour protéger les systèmes d'information et la technologie des logiciels malveillants (par ex. virus, vers, logiciels espion, pourriels (spams)).

DS5.10 Sécurité des réseaux
Mettre en œuvre des techniques de sécurité et des procédures de gestion associées (ex. pare-feux, dispositifs de sécurité, compartimentage réseau, détection d'intrusion) pour autoriser et contrôler les flux d'informations entre réseaux.

DS5.11 Échange de données sensibles
Ne faire circuler les échanges de données sensibles que sur des circuits sûrs ou sur des supports dotés de contrôles qui garantissent l'authenticité du contenu et fournissent la preuve de la réception et celle de non-répudiation de la part de l'expéditeur.

GUIDE DE MANAGEMENT

DS5 Assurer la sécurité des systèmes

De	Entrées
PO2	Architecture de l'information ; classifications attribuées aux données
PO3	Standards informatiques
PO9	Évaluation des risques
AI2	Spécification des contrôles de sécurité des applications
DS1	CE

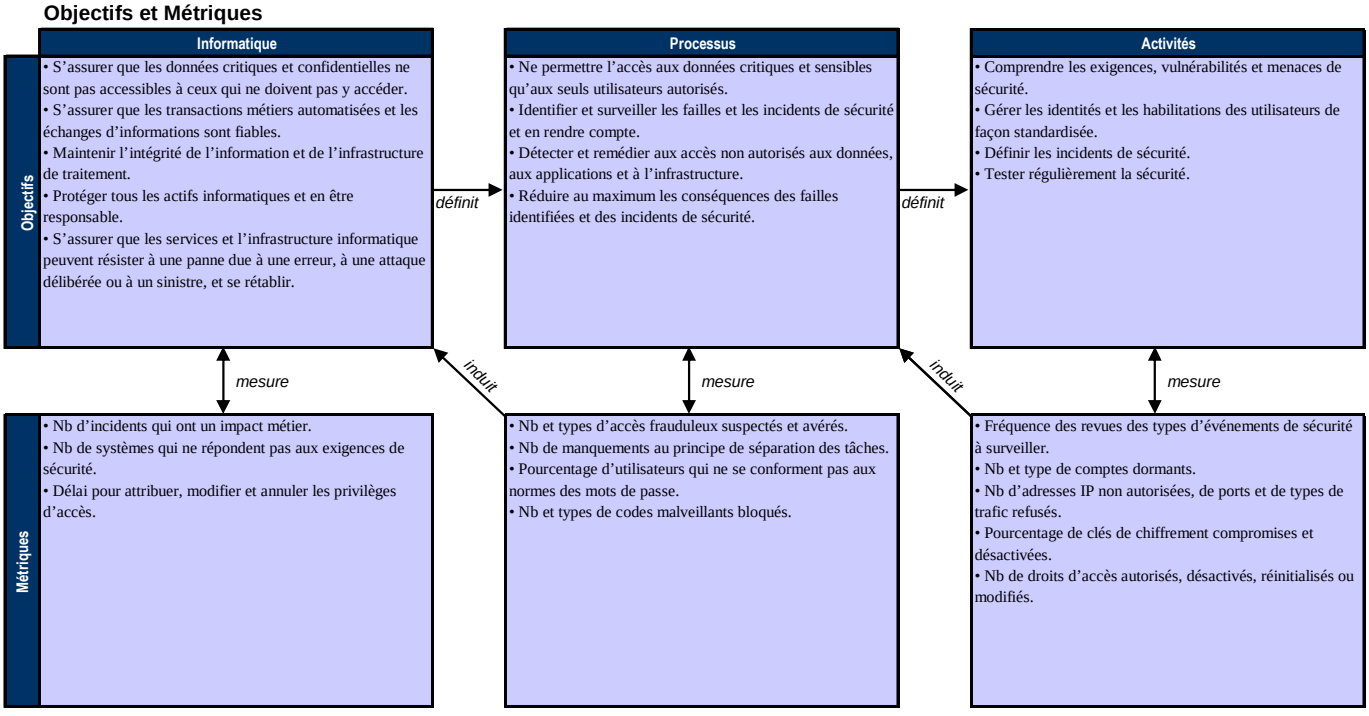
Sorties	Vers
Définition des incidents de sécurité	DS8
Exigences de formations spécifiques à la sensibilisation à la sécurité	DS7
Rapports sur la performance des processus	SE1
Modifications de sécurité requises	AI6
Menaces et vulnérabilités de sécurité	PO9
Plan et politiques de sécurité informatique	DS11

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir et tenir à jour un plan de sécurité informatique.	I	C	C	A	C	C	C	C	I	I	R
Définir, mettre en place et appliquer un processus de gestion des identités/comptes utilisateurs.			I	A	C	R	R	I			C
Surveiller les incidents de sécurité avérés et potentiels.				A	I	R	C	C			R
Réviser et valider périodiquement les droits d'accès et privilèges utilisateurs.				I	A	C					R
Installer et tenir à jour des procédures de maintenance et de sauvegarde des clés de chiffrement.				A		R			I		C
Mettre en place et tenir à jour des contrôles techniques et procéduraux pour protéger les flux de données entre réseaux.				A	C	C	R	R			C
Pratiquer des évaluations régulières de la vulnérabilité.		I		A	I	C	C	C			R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS5 Assurer la sécurité des systèmes

La gestion du processus *Assurer la sécurité des systèmes* qui répond à l'exigence des métiers vis-à-vis de l'informatique *maintenir l'intégrité de l'information et de l'infrastructure technologique et réduire au maximum les conséquences de failles et d'incidents de sécurité* est :

0 Inexistante quand

L'entreprise ne reconnaît pas le besoin de sécurité informatique. Les responsabilités opérationnelles et finales de la sécurité ne sont pas attribuées. On n'a pas mis en place de mesures pour gérer la sécurité informatique. Il n'y a pas de rapports sur cette question, ni de processus pour réagir aux atteintes à la sécurité informatique. Il y a une absence totale de processus reconnaissable d'administration de la sécurité des systèmes.

1 Initialisée, au cas par cas quand

L'entreprise reconnaît le besoin de sécurité informatique. La sensibilisation au besoin de sécurité est principalement une affaire individuelle. On réagit aux circonstances. La sécurité informatique ne fait pas l'objet de mesures. Chacun désigne quelqu'un d'autre lorsque des atteintes à la sécurité sont détectées, parce que les responsabilités ne sont pas clairement définies. On ne peut pas prévoir quelles réponses seront données aux incidents de sécurité.

2 Reproductible mais intuitive quand

Les responsabilités opérationnelles et finales de la sécurité des SI sont confiées à un coordinateur bien que son autorité soit limitée. La sensibilisation au besoin de sécurité est fragmentaire et limitée. Bien que les systèmes produisent des informations relatives à la sécurité, on ne les analyse pas. Les services fournis par des tiers ne répondent pas toujours aux besoins de sécurité spécifiques de l'entreprise. On développe des politiques de sécurité, mais les compétences et les outils sont inadéquats. Les rapports sur la sécurité sont incomplets, trompeurs ou sans pertinence. Il existe une formation à la sécurité, mais elle reste avant tout une initiative individuelle. La sécurité informatique est considérée surtout comme de la responsabilité et du domaine de l'informatique, et les métiers ne voient pas qu'elle fait partie du sien.

3 Définie quand

Le management fait la promotion de la sécurité et le personnel commence à y être sensibilisé. Les procédures de sécurité informatique sont définies et alignées sur la politique de sécurité des SI. Les responsabilités dans ce domaine sont attribuées et comprises, mais pas systématiquement exercées. Il existe un plan de sécurité des SI et des solutions élaborées à partir de l'analyse des risques. Les rapports sur la sécurité ne sont pas clairement axés sur les métiers. On fait des tests de sécurité (ex. tests d'intrusion) au cas par cas. La formation à la sécurité est accessible au personnel informatique et des métiers, mais elle n'est gérée et planifiée que de façon informelle.

4 Gérée et mesurable quand

Les responsabilités de la sécurité des SI sont clairement attribuées, gérées et exercées. On analyse régulièrement les risques informatiques et leurs conséquences. On complète les politiques et les procédures de sécurité par des principes de base spécifiques à la sécurité. On rend obligatoire les méthodes pour promouvoir la sensibilisation à la sécurité. On a standardisé l'identification des utilisateurs, leur authentification, et leurs droits d'accès. On poursuit la certification des personnels responsables de l'audit et de la gestion de la sécurité. Les tests de sécurité utilisent un processus standardisé et formalisé qui conduit à des améliorations des niveaux de sécurité. Les processus de sécurité des SI sont coordonnés avec la fonction de sécurité générale de l'entreprise. Les rapports sur la sécurité informatique sont liés aux objectifs métiers. La formation à la sécurité est suivie à la fois par le personnel informatique et par le personnel des métiers. La formation à la sécurité est planifiée et gérée de façon à répondre aux besoins des métiers et aux profils de risques définis pour la sécurité. On a défini des objectifs et des métriques de gestion de la sécurité mais on ne les évalue pas encore.

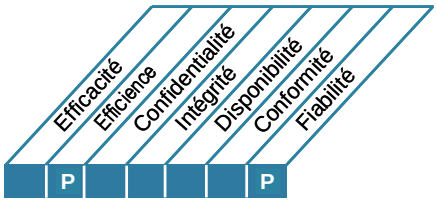
5 Optimisée quand

La sécurité des SI est sous la responsabilité conjointe des responsables métiers et informatique, et elle fait partie des objectifs de sécurité de l'entreprise. Les exigences de sécurité informatique sont clairement définies, optimisées, et incluses dans un plan de sécurité approuvé. Les utilisateurs et les clients sont de plus en plus responsables de la définition des exigences de sécurité, et les fonctions de sécurité sont intégrées aux applications dès la conception. On traite rapidement les incidents de sécurité à l'aide de procédures spécifiques formalisées qui s'appuient sur des outils informatiques. Des évaluations périodiques de la sécurité permettent d'évaluer le bon fonctionnement du plan de sécurité. On collecte et on analyse systématiquement les informations sur les menaces et sur les failles de sécurité. On communique et on met rapidement en place des contrôles adaptés pour réduire les risques. L'amélioration permanente des processus s'appuie sur des tests de sécurité, une analyse causale des incidents de sécurité, et une identification proactive des risques. Les processus et technologies de sécurité sont intégrés dans l'ensemble de l'entreprise. On évalue, on recueille les métriques de la gestion de la sécurité et on en communique le résultat. Le management en utilise les résultats pour adapter le plan de sécurité selon un processus d'amélioration continue.

DESCRIPTION DU PROCESSUS

DS6 Identifier et imputer les coûts

La nécessité d'un système loyal et équitable pour affecter les coûts informatiques aux métiers exige qu'ils soient chiffrés avec précision et qu'un accord soit conclu avec les utilisateurs métiers sur une juste répartition. Ce processus comprend l'élaboration et la mise en œuvre d'un système pour calculer et affecter les coûts informatiques et en rendre compte aux utilisateurs de services. Un système de répartition juste permet aux métiers de prendre des décisions mieux documentées à propos de l'utilisation des services informatiques.



Le contrôle du processus informatique

Identifier et imputer les coûts

qui répond à l'exigence des métiers vis-à-vis de l'informatique

assurer la transparence et la compréhension des coûts informatiques, et améliorer la rentabilité grâce à une utilisation bien documentée des services informatiques

en se concentrant sur

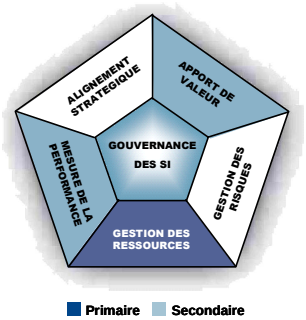
un recensement complet et précis des coûts informatiques, un système de répartition juste qui a l'accord des utilisateurs métiers, et un système de comptes-rendus en temps opportun de l'utilisation des SI et de l'affectation des coûts.

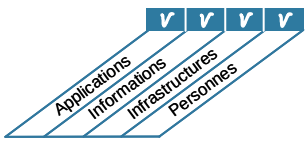
atteint son objectif en

- faisant correspondre les charges avec la qualité et la quantité des services fournis
- élaborant et en faisant adopter un modèle de coûts exhaustif
- répercutant les charges conformément à la politique agréée

et est mesuré par

- le pourcentage de factures de services informatiques acceptées/payées par la direction des métiers
- le pourcentage des écarts entre les coûts budgétés, prévisionnels, et réels
- le pourcentage des coûts informatiques globaux qui sont affectés conformément aux modèles de coûts agréés.





OBJECTIFS DE CONTRÔLE

DS6 Identifier et imputer les coûts

DS6.1 Définition des services
Identifier tous les coûts informatiques et les faire correspondre aux services informatiques pour aider à bâtir un modèle de coûts transparent. Il faut lier les services informatiques aux processus métiers pour que les métiers puissent identifier les niveaux de facturation de services associés.

DS6.2 Comptabilité de l'informatique
Calculer et affecter les coûts réels en respectant le modèle de coûts de l'entreprise. Les écarts entre les prévisions et les coûts réels doivent faire l'objet d'analyses et de comptes-rendus conformes aux systèmes de mesure financiers de l'entreprise.

DS6.3 Modèle de coûts et facturation
En se basant sur la définition des services, définir et mettre en place un modèle de coûts qui permette le calcul du taux de refacturation interne par service. Le modèle de coûts informatiques doit permettre aux utilisateurs d'identifier, de mesurer et de prévoir la facturation des services pour encourager une bonne utilisation des ressources.

DS6.4 Maintenance du modèle de coûts
Faire régulièrement des revues et des tests comparatifs du modèle de coûts et de refacturation pour en maintenir la pertinence et l'adéquation aux évolutions des activités métiers et informatique.

GUIDE DE MANAGEMENT

DS6 Identifier et imputer les coûts

De	Entrées
PO4	Propriétaires de systèmes documentés
PO5	Rapports coûts/bénéfices, budgets informatiques
PO10	Plans détaillés des projets
DS1	CS et CE

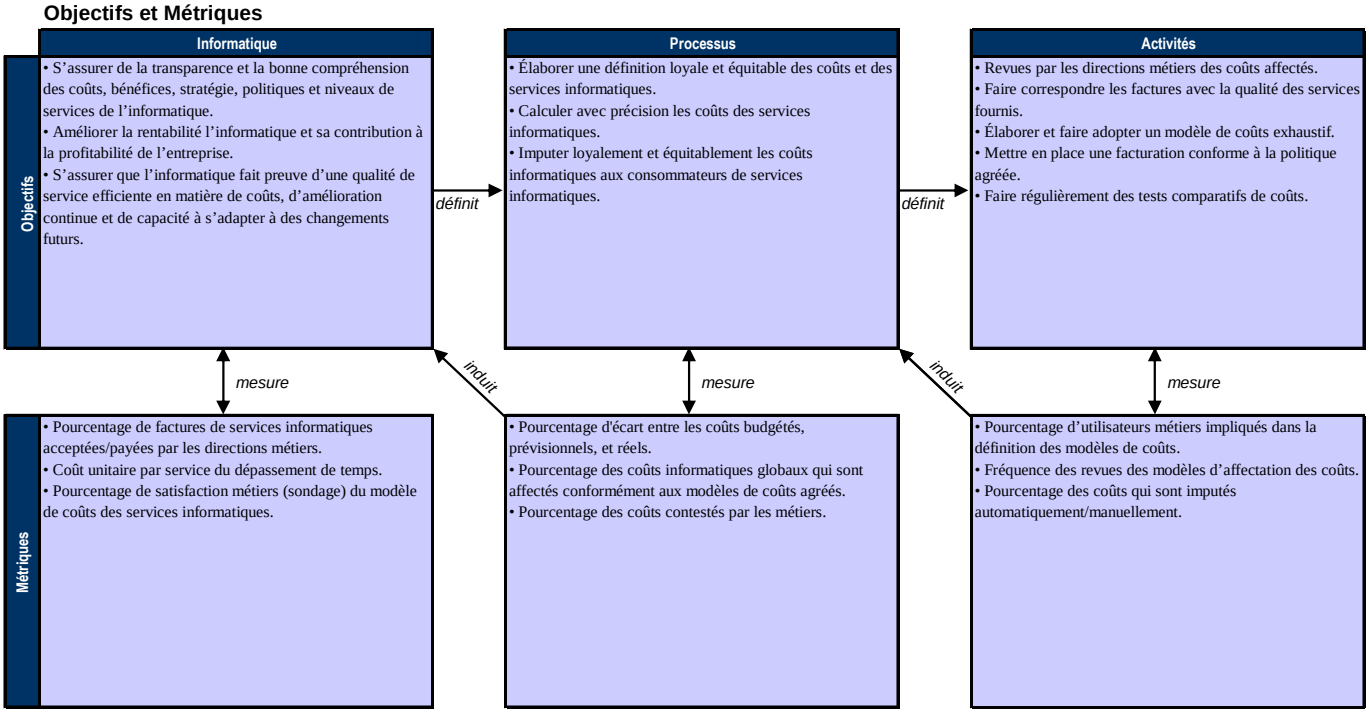
Sorties	Vers
Données financières informatiques	PO5
Rapports sur la performance des processus	SE1

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Faire correspondre les infrastructures informatiques aux services fournis et/ou aux processus métiers qu'elles supportent.		C	C	A	C	C	C	C	R	C	
Identifier tous les coûts informatiques (personnel, technologie, etc.) et les faire correspondre aux services informatiques sur la base de leur coût unitaire.		C		A		C	C	C	R	C	
Mettre en place et maintenir opérationnel un processus de comptabilité et de contrôle des coûts informatiques.		C	C	A	C	C	C	C	R	C	
Mettre en place et maintenir opérationnelles des politiques et des procédures de facturation.		C	C	A	C	C	C	C	R	C	

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS6 Identifier et imputer les coûts

La gestion du processus *Identifier et imputer les coûts* qui répond à l'exigence des métiers vis-à-vis de l'informatique *assurer la transparence et la compréhension des coûts informatiques, et améliorer la rentabilité grâce à une utilisation bien documentée des services informatiques* est :

0 Inexistante quand

Il y a une absence totale de processus reconnaissable susceptible de faire ressortir et d'imputer les coûts en ce qui concerne les services informatiques fournis. L'entreprise ne réalise même pas qu'il y a là une question à traiter et personne ne communique sur ce sujet.

1 Initialisée, au cas par cas quand

On comprend que les services informatiques ont un coût global, mais ces coûts ne sont pas répartis par utilisateur, client, service, groupe d'utilisateurs, fonction, projet ou livrable. Il n'existe pratiquement pas de suivi des coûts, seuls des comptes rendus sur les coûts globaux, non détaillés, sont fournis au management dans les rapports. Les coûts informatiques sont imputés comme des frais généraux opérationnels. Les métiers ne reçoivent aucune information sur les coûts ou les bénéfices de la fourniture de services.

2 Reproductible mais intuitive quand

On a généralement pris conscience du besoin de faire ressortir les coûts et de les imputer. L'imputation est basée sur des hypothèses informelles et rudimentaires telles que les coûts des matériels, et il n'y a pratiquement aucun lien avec la valeur générée. Les processus d'imputation des coûts sont reproductibles. Il n'existe ni formation ni communication formelles sur les procédures standard d'identification et d'imputation des coûts. On n'a pas affecté la responsabilité de collecter ou d'affecter les coûts.

3 Définie quand

Il existe un modèle de coûts des services informatiques défini et documenté. On définit un processus qui rend compte des coûts informatiques des services fournis aux utilisateurs. On a une bonne conscience des coûts imputables aux services informatiques. Les métiers disposent d'informations rudimentaires sur les coûts.

4 Gérée et mesurable quand

Les responsabilités opérationnelles et finales de gestion des coûts des services informatiques sont bien définies et pleinement comprises à tous les niveaux et s'appuient sur des formations formelles. On sait identifier les coûts directs et indirects, qui font l'objet de rapports, élaborés de façon automatique et en temps voulu, destinés au management, aux propriétaires de processus et aux utilisateurs. D'une façon générale on fait un suivi et une évaluation des coûts, et on réagit si on constate des dérives. Les comptes-rendus sur les services informatiques sont liés aux objectifs métiers et aux conventions de services, et ils sont surveillés par les propriétaires des processus métiers. Une fonction financière vérifie régulièrement si le processus d'affectation des coûts est raisonnable. Il existe un système de comptabilisation automatisé des coûts, mais il est plus axé sur la fonction informatique que sur les processus métiers. On a adopté des objectifs et des métriques d'évaluation des coûts, mais ils ne sont pas systématiquement mesurés.

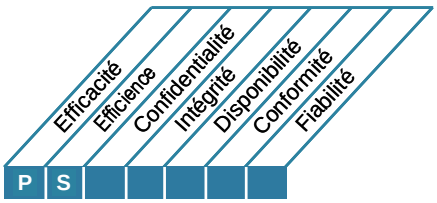
5 Optimisée quand

On identifie, consigne, résume, et fait le suivi des coûts des services fournis au management, aux propriétaires de processus et aux utilisateurs. Les coûts sont vus comme des articles facturables et peuvent alimenter un système de refacturation qui facture les utilisateurs de façon appropriée, en fonction de l'utilisation. Les conventions de services s'appuient sur des coûts détaillés. On utilise la surveillance et l'évaluation des coûts des services pour optimiser les coûts des ressources informatiques. On utilise les chiffres obtenus pour vérifier les bénéfices dans le processus de gestion du budget de l'entreprise. Les rapports sur les coûts informatiques permettent d'être alerté assez tôt en cas d'évolutions des exigences des métiers grâce à des systèmes de reporting intelligents. On utilise un modèle de coût variable qui est fonction des volumes traités pour chaque service fourni. On élève la gestion des coûts au niveau des pratiques de la profession grâce aux résultats du processus d'amélioration permanente et à la comparaison avec d'autres entreprises. L'optimisation des coûts est un processus permanent. La revue des objectifs et des métriques par le management fait partie du processus d'amélioration continue par l'ajustement des systèmes de mesure des coûts.

DESCRIPTION DU PROCESSUS

DS7 Instruire et former les utilisateurs

La formation efficace de tous les utilisateurs des systèmes informatiques, y compris les informaticiens, exige de connaître les besoins en formation de chaque groupe d'utilisateurs. Outre l'identification des besoins, ce processus doit aussi définir et mettre en œuvre une stratégie de formation efficace et en mesurer les résultats. Un programme de formation efficace augmente l'efficacité de l'utilisation de l'informatique en réduisant le nombre d'erreurs commises par les utilisateurs, en augmentant la productivité et en améliorant la conformité aux contrôles clés tels que les mesures de sécurité utilisateurs.



Le contrôle du processus informatique

Instruire et former les utilisateurs

qui répond à l'exigence des métiers vis-à-vis de l'informatique

permettre une utilisation efficace et efficiente des applications et des solutions informatiques et assurer le respect des politiques et des procédures par les utilisateurs

en se concentrant sur

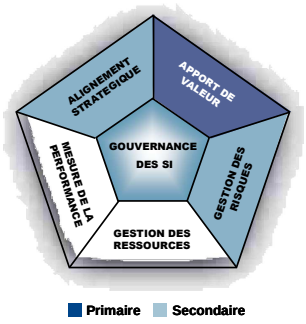
une bonne connaissance des besoins en formation des utilisateurs des SI, la mise en œuvre d'une stratégie efficace de formation et la mesure des résultats

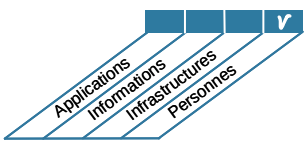
atteint son objectif en

- établissant des programmes de formation
- organisant la formation
- dispensant la formation
- surveillant et en rendant compte de l'efficacité de la formation

et est mesuré par

- le nombre d'appels au service d'assistance par insuffisance de formation des utilisateurs
- le pourcentage de parties prenantes satisfaites de la formation reçue
- le délai entre l'identification d'un besoin de formation et la mise en place de cette formation





OBJECTIFS DE CONTRÔLE

DS7 Instruire et former les utilisateurs

DS7.1 Identification des besoins en savoir et en formation
Établir et mettre régulièrement à jour un programme pour chaque groupe cible de salariés en prenant en compte :

- Les besoins des métiers et la stratégie actuels et futurs
- La valeur de l'information en tant qu'actif
- Les valeurs de l'entreprise (valeurs éthiques, culture de la sécurité et du contrôle, etc.)
- La mise en place d'une nouvelle infrastructure informatique et de nouveaux logiciels (par ex. progiciels et applications)
- Les qualifications existantes et futures, les profils de compétences et les besoins de certification et/ou d'accréditation ou de réaccréditation
- Les méthodes d'enseignement (par ex. classe, en ligne..), la dimension des groupes cibles, l'accessibilité et les horaires.

DS7.2 Fourniture de formation et d'enseignement
En se basant sur les besoins identifiés en formation et en enseignement, identifier les groupes cibles et leurs membres, les mécanismes efficaces, les enseignants, formateurs et conseillers pédagogiques. Engager des formateurs et organiser des sessions de formation en temps voulu. Enregistrer les inscriptions (y compris les conditions préalables), l'assiduité et l'évaluation des performances de la session.

DS7.3 Évaluation de la formation reçue
Évaluer en fin de session le contenu de l'enseignement et de la formation pour en déterminer la pertinence, la qualité, l'efficacité, ce qui a été retenu, le coût et la valeur. Les résultats de cette évaluation doivent nourrir la définition des programmes des sessions de formation à venir.

GUIDE DE MANAGEMENT

DS7 Instruire et former les utilisateurs

De	Entrées
PO7	Compétences et connaissances des utilisateurs, formation individuelle, besoins spécifiques de formation
AI4	Matériels de formation ; besoins de transfert de connaissances pour la mise en place de solutions
DS1	CE
DS5	Exigences de formations spécifiques à la sensibilisation à la sécurité
DS8	Rapports sur la satisfaction des utilisateurs

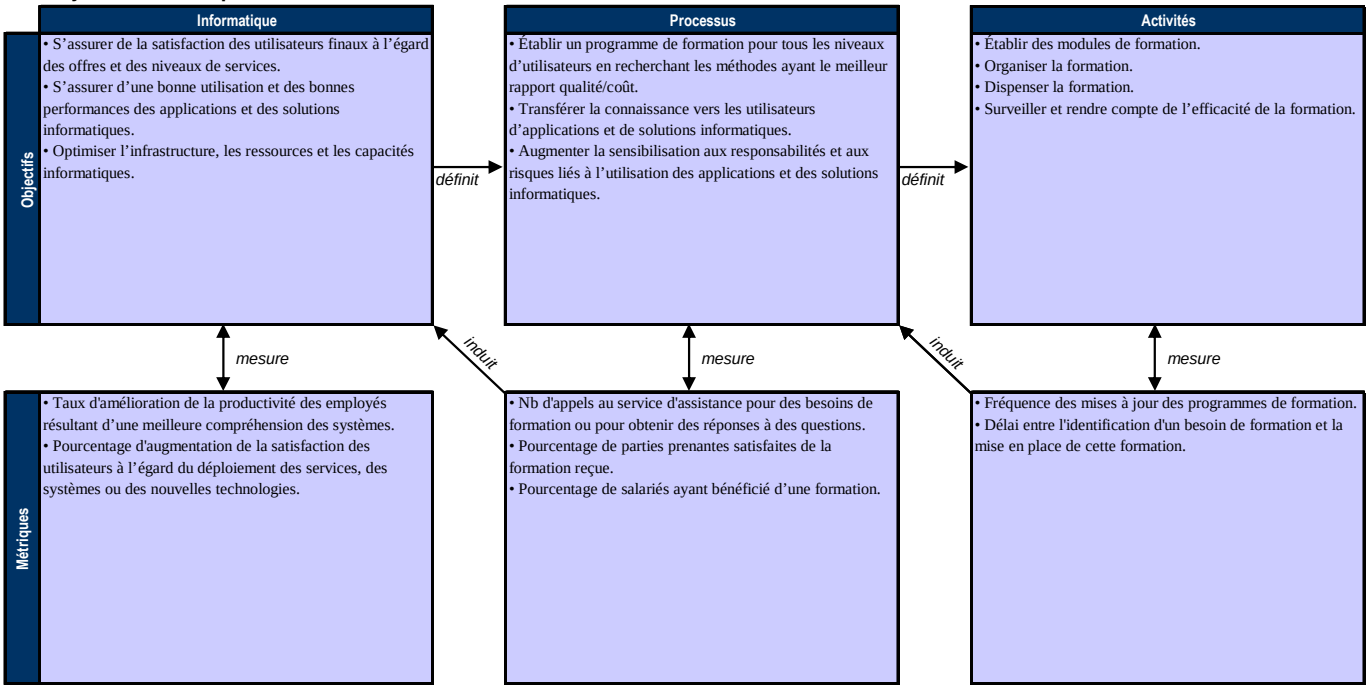
Sorties	Vers
Rapports sur la performance des processus	SE1
Mises à jour de la documentation requise	AI4

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité	Service formation
Identifier et caractériser les besoins de formation des utilisateurs.			C	A	R	C	C	C	C	C	C	R
Construire un programme de formation.			C	A	R	C	I	C	C	C	I	R
Diriger les activités de sensibilisation, d'enseignement et de formation.			I	A	C	C	I	C	C	C	I	R
Évaluer la formation.			I	A	R	C	I	C	C	C	I	R
Identifier et évaluer les meilleures méthodes et les meilleurs outils pour dispenser la formation.			I	A/R	R	C	C	C	C	C	C	R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS7 Instruire et former les utilisateurs

La gestion du processus *Instruire et former les utilisateurs* qui répond à l'exigence des métiers vis-à-vis de l'informatique *permettre une utilisation efficace et efficiente des applications et des solutions informatiques et assurer le respect des politiques et des procédures par les utilisateurs* est :

0 Inexistante quand

Il y a une absence totale de programme d'enseignement et de formation. L'entreprise n'a même pas conscience que la formation est une problématique à traiter, et elle ne communique pas sur ce sujet.

1 Initialisée, au cas par cas quand

On constate que l'entreprise a reconnu le besoin d'un programme d'enseignement et de formation, mais il n'y a pas de processus standardisé. En l'absence d'un programme organisé, les employés trouvent et suivent des formations de leur côté. Certaines de ces formations traitent des questions d'éthique du comportement, de sensibilisation à la sécurité des systèmes et aux pratiques de sécurité. L'approche globale du management manque complètement de cohésion, et la communication sur ces thèmes reste sporadique et sans méthode.

2 Reproductible mais intuitive quand

On a conscience du besoin d'un programme d'enseignement et de formation et des processus associés dans l'ensemble de l'entreprise. On commence à trouver des formations dans les plans de performance individuels des employés. Les processus se sont multipliés au point que des formations informelles et des enseignements ont recours à de formateurs différents qui traitent des mêmes questions avec des approches différentes. Certains cours traitent des questions d'éthique du comportement, de sensibilisation à la sécurité des systèmes et des pratiques de sécurité. On se repose beaucoup sur les connaissances de certains individus. Cependant on communique sur les difficultés d'ordre général et sur le besoin de les traiter.

3 Définie quand

Le programme d'enseignement et de formation est élaboré et fait l'objet de communications, et les employés et le management identifient les besoins de formation et les documentent. On standardise et documente les processus d'enseignement et de formation. On mobilise des budgets, des ressources, des équipements et des formateurs pour ces programmes. On donne des cours formels aux employés sur l'éthique du comportement, sur la sensibilisation à la sécurité des systèmes et sur les pratiques de sécurité. La plupart des processus d'enseignement et de formation font l'objet d'une surveillance, mais le management ne détecte vraisemblablement pas tous les écarts par rapport à ces processus. On n'analyse qu'occasionnellement les problèmes de formation et d'enseignement.

4 Gérée et mesurable quand

Il existe un programme complet de formation et d'enseignement qui donne des résultats mesurables. Les responsabilités sont clairement attribuées et la propriété des processus est établie. L'enseignement et la formation font partie des plans de carrière des employés. Le management favorise la tenue de sessions d'enseignement et de formation, et y assiste. Tous les employés reçoivent une formation sur les conduites éthiques et sur la sensibilisation à la sécurité des systèmes. Tous les employés reçoivent une formation adéquate sur les pratiques de sécurité à l'occasion de laquelle ils apprennent à protéger les systèmes des défaillances affectant la disponibilité, la confidentialité et l'intégrité. Le management veille à la conformité en vérifiant et en mettant constamment à jour les processus et les contenus des programmes de formation et d'enseignement. Les processus s'améliorent et on applique les meilleures pratiques internes.

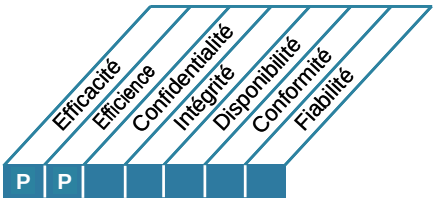
5 Optimisée quand

La formation et l'enseignement débouchent sur une amélioration des performances individuelles. Ils sont devenus des composants essentiels des plans de carrière des employés. On mobilise les budgets, ressources, équipements et formateurs qui permettent de mener à bien les programmes de formation et d'enseignement. On perfectionne les processus qui s'améliorent en permanence, tirant profit des meilleures pratiques externes et en se comparant aux autres entreprises sur l'échelle de maturité. On fait l'analyse causale de tous les problèmes et écarts qui surviennent de façon à trouver rapidement des solutions efficaces. L'attitude vis-à-vis des questions d'éthique et des principes de sécurité des systèmes est positive. On utilise largement l'informatique, de façon intégrée et optimisée pour fournir des outils aux programmes de formation et d'enseignement, et pour en automatiser certaines fonctions. On mobilise des formateurs externes et on s'inspire des résultats des tests comparatifs.

DESCRIPTION DU PROCESSUS

DS8 Gérer le service d'assistance client et les incidents

Apporter des réponses efficaces et au bon moment aux requêtes et aux problèmes des utilisateurs exige un processus bien conduit de gestion du service d'assistance et de gestion des incidents. Ce processus comporte la mise en place d'un service d'assistance qui s'occupe de l'enregistrement et de l'escalade des incidents, de l'analyse des tendances et des causes, et des solutions. L'intérêt de l'entreprise passe par l'amélioration de la productivité grâce à la résolution rapide des demandes des utilisateurs. Par ailleurs les métiers peuvent rechercher les causes premières (comme une formation insuffisante des utilisateurs) au moyen de comptes-rendus efficaces.



Le contrôle du processus informatique

Gérer le service d'assistance client et les incidents

qui répond à l'exigence des métiers vis-à-vis de l'informatique

permettre une utilisation efficace des systèmes informatiques en apportant les analyses et les solutions aux demandes, questions et incidents soulevés par les utilisateurs finaux.

en se concentrant sur

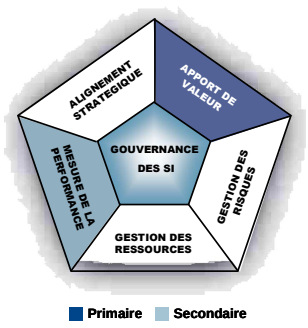
une fonction assistance client professionnelle avec des réponses rapides, des procédures d'escalade claires et des analyses de résolution d'incidents et de tendances

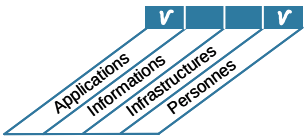
atteint son objectif en

- installant et en faisant fonctionner un service d'assistance
- surveillant et en rendant compte des tendances
- définissant des critères et des procédures d'escalade clairs

et est mesuré par

- le niveau de satisfaction des utilisateurs à l'égard de l'assistance de premier niveau
- le pourcentage d'incidents résolus dans une limite de temps convenue/acceptable
- le taux d'abandon des demandes





OBJECTIFS DE CONTRÔLE

DS8 Gérer le service d'assistance client et les incidents

DS8.1 Service d'assistance client
Mettre en place un service client qui doit faire l'interface entre l'utilisateur et l'informatique, pour enregistrer, communiquer et analyser tous les appels, les rapports d'incidents, les demandes de services et d'information. Il faut des procédures de surveillance et d'escalade basées sur les niveaux de services définis dans les conventions de services appropriées ; cela doit permettre de classer tout problème ou incident rapporté, demande de service ou d'information et de lui attribuer des priorités. Mesurer la satisfaction des utilisateurs finaux à l'égard de la qualité du service d'assistance client et des services informatiques.

DS8.2 Enregistrement des demandes des clients
Mettre en place une fonction et un système qui permette d'enregistrer et de suivre les appels, les incidents, les demandes de services et les besoins en information. Cette fonction doit travailler en étroite association avec des processus tels que la gestion des incidents, des problèmes, des changements, des capacités et de la disponibilité. Les incidents doivent être classés selon une priorité métier et une priorité de service, et dirigés vers l'équipe de gestion de problèmes appropriée quand nécessaire. Les clients doivent être tenus informés de l'état d'avancement de leurs demandes.

DS8.3 Escalade des incidents
Mettre en place des procédures d'assistance client de façon à ce que les incidents qui ne peuvent pas être immédiatement résolus soient transmis au niveau de support supérieur approprié dans les limites prévues par les conventions de services, et que des solutions de contournement soient identifiées si nécessaire. S'assurer que la propriété des incidents et la surveillance du cycle de vie restent entre les mains du service d'assistance client pour les incidents qui concernent les utilisateurs, quelle que soit l'équipe informatique qui travaille à la résolution des problèmes.

DS8.4 Clôture des incidents
Mettre en place des procédures de surveillance de la résolution des demandes des clients dans les temps. Lorsque l'incident a été résolu, s'assurer que le service d'assistance client enregistre les étapes de sa résolution et confirmer que la solution apportée a reçu l'agrément du client Enregistrer également les incidents non résolus (erreurs connues et palliatifs) et en effectuer le rapport de façon à disposer d'informations pour une gestion correcte des problèmes.

DS8.5 Rapports et analyse des tendances
Produire des rapports de l'activité du service d'assistance client pour permettre au management de mesurer la performance du service et les temps de réponse, et d'identifier les tendances ou les problèmes récurrents, de façon à ce que le service s'améliore en permanence.

GUIDE DE MANAGEMENT

DS8 Gérer le service d'assistance client et les incidents

De	Entrées
AI4	Manuels utilisateur, d'exploitation, d'assistance, technique et d'administration
AI6	Autorisation de modification
AI7	Éléments de configuration mis à disposition
DS1	CS et CE
DS4	Seuils incidents/sinistres
DS5	Définition des incidents de sécurité
DS9	Configuration informatique/détail des actifs
DS10	Problèmes connus, erreurs connues et solutions de contournement
DS13	Tickets d'incidents

Sorties	Vers						
Demande de service/demande de modification	AI6						
Rapports d'incidents	DS10						
Rapports sur la performance des processus	SE1						
Rapports sur la satisfaction des utilisateurs	DS7	SE1					

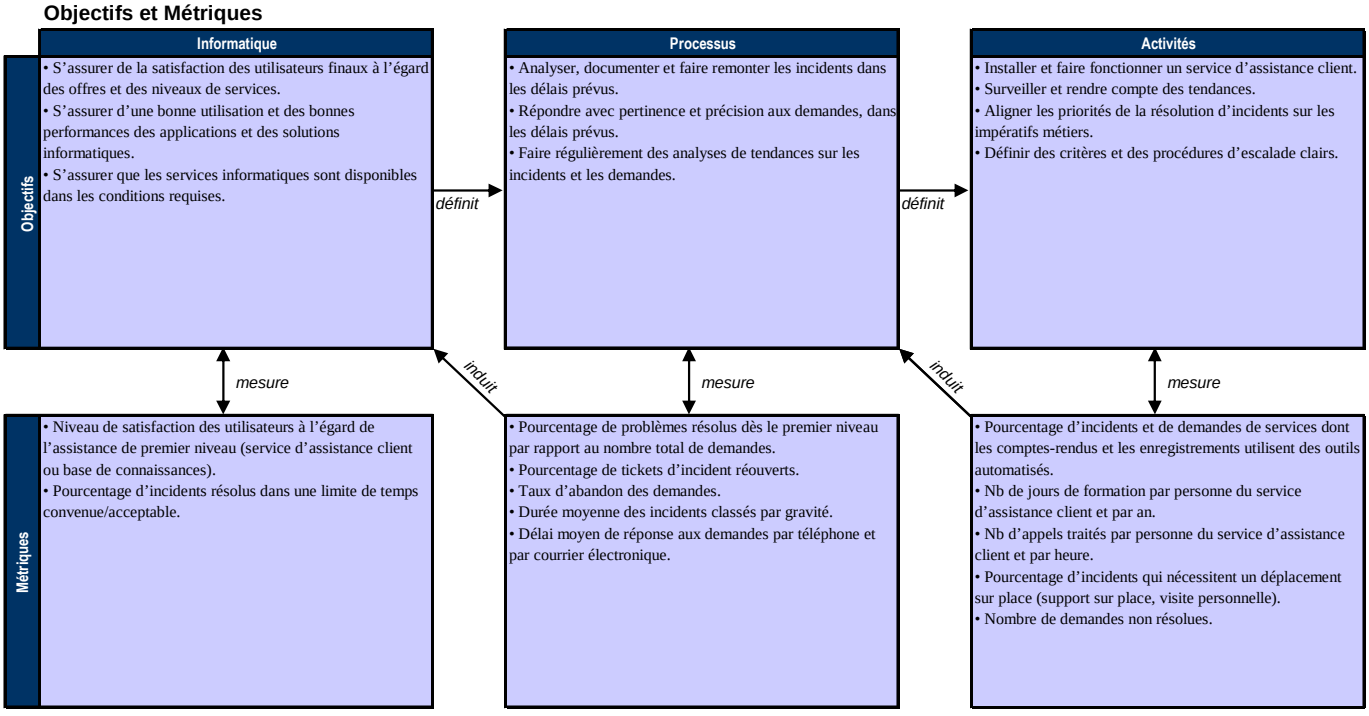
Tableau RACI

Fonctions

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité	Responsable assistance/incidents
Créer une classification (gravité et conséquences) et des procédures d'escalade (fonctionnelles et hiérarchiques).				C	C	C	C	C	C		C	A/R
Détecter et enregistrer les incidents/demandes de services/demandes d'information.												A/R
Classer et investiguer les demandes et faire les diagnostics.				I		C	C	C			I	A/R
Trouver les solutions, les appliquer et clôturer l'incident.					I	R	R	R			C	A/R
Informer les utilisateurs (ex. état d'avancement).				I	I							A/R
Produire des rapports pour le management.	I			I	I	I			I		I	A/R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS8 Gérer le service d'assistance client et les incidents

La gestion du processus *Gérer le service d'assistance client et les incidents* qui répond à l'exigence des métiers vis-à-vis de l'informatique *permettre une utilisation efficace des systèmes informatiques en apportant les analyses et les solutions aux demandes, questions et incidents soulevés par les utilisateurs finaux* est :

0 Inexistante quand

Les utilisateurs n'ont pas d'interlocuteurs désignés pour répondre à leurs questions et problèmes. Il n'existe aucun processus de gestion des incidents. L'entreprise ne réalise pas que c'est une problématique à traiter.

1 Initialisée, au cas par cas quand

Le management reconnaît qu'un processus s'appuyant sur des outils et du personnel est nécessaire pour répondre aux demandes des utilisateurs et gérer la résolution des incidents. Il n'y a cependant pas de processus standardisé, et on ne fournit d'assistance qu'au cas par cas. Le management n'organise pas de suivi des demandes des utilisateurs, des incidents ou des tendances. On n'a pas prévu de processus d'escalade pour résoudre les problèmes.

2 Reproductible mais intuitive quand

L'entreprise est consciente du besoin d'un service d'assistance client et d'un processus de gestion des incidents. Il existe une forme d'assistance informelle grâce à un réseau d'individus qui ont un bon niveau de connaissances. Ces personnes disposent de certains outils d'aide à la résolution des incidents qui leur sont communs. Il n'y a pas de formation formelle, ni de communication sur les procédures standard, et la responsabilité est laissée aux individus.

3 Définie quand

On reconnaît et on accepte le besoin d'un service d'assistance client et d'un processus de gestion des incidents. On standardise et documente les procédures et des formations informelles ont lieu. On laisse cependant aux individus l'initiative de se former et de se conformer aux normes. Les Foires Aux Questions (FAQ) et les guides utilisateurs se sont développés, mais c'est à chacun de les trouver et de s'y conformer éventuellement. On consigne à la main les questions et les incidents soulevés et on les suit individuellement, mais cette activité ne donne pas lieu à des rapports formels. On ne chiffre pas les questions et incidents soulevés qui ont reçu une réponse en temps opportun et il est vraisemblable que certains problèmes ne trouvent pas de solutions. Les utilisateurs ont reçu des informations claires sur ce qu'ils doivent faire en cas de problème ou d'incident : comment faire un rapport et à qui.

4 Gérée et mesurable quand

On comprend pleinement les avantages d'un processus de gestion des incidents à tous les niveaux de l'entreprise, et on met en place le service d'assistance client en le structurant en unités adéquates. Les outils et les techniques sont automatisés et on dispose d'une base de connaissances centralisée. L'équipe du service d'assistance client a des contacts étroits avec celle qui s'occupe de la résolution des problèmes. Les responsabilités sont claires et on surveille l'efficacité du service. On a mis en place des procédures de communication, d'escalade et de résolution des incidents, et on le fait savoir. On forme les personnels d'assistance et on améliore les processus au moyen de logiciels spécifiques. Le management a mis au point des métriques pour apprécier la performance du service d'assistance client.

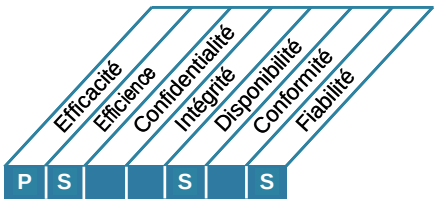
5 Optimisée quand

Le processus de gestion des incidents et la fonction d'assistance client sont en place, et bien organisés ; l'état d'esprit est orienté vers l'assistance au client avec une attention à ses besoins, les connaissances nécessaires et le désir de l'aider. Les métriques sont systématiquement évaluées et font l'objet de rapports. Des FAQ riches, exhaustives, font partie intégrante de la base de connaissances. Les utilisateurs disposent d'outils qui leur permettent de réaliser des auto-diagnostics et de résoudre eux-mêmes certains incidents. Les conseils sont professionnels, et les incidents sont résolus rapidement au travers d'un processus d'escalade structuré. Le management utilise un outil intégré pour les statistiques de performances du processus de gestion des incidents et de la fonction d'assistance client. Les processus se sont hissés au niveau des meilleures pratiques du secteur, grâce aux résultats de l'analyse des indicateurs de performance, aux améliorations permanentes et aux tests comparatifs avec d'autres entreprises.

DESCRIPTION DU PROCESSUS

DS9 Gérer la configuration

Assurer l'intégrité des configurations matérielles et logicielles exige de constituer et de tenir à jour un référentiel de configuration précis et complet. Ce processus doit comporter la collecte des informations de la configuration initiale, l'établissement de configurations de base, la vérification et l'audit des informations de configuration, et la mise à jour du référentiel de configuration lorsque c'est nécessaire. Une gestion efficace de la configuration facilite une plus grande disponibilité du système, la réduction des problèmes de production et une résolution plus rapide de ceux-ci.



Le contrôle du processus informatique

Gérer la configuration

qui répond à l'exigence des métiers vis-à-vis de l'informatique

optimiser l'infrastructure, les ressources et les capacités informatiques, et justifier les investissements informatiques

en se concentrant sur

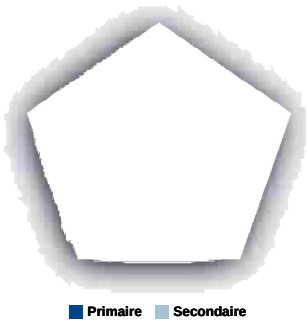
la mise en place et la mise à jour d'un référentiel précis et complet des attributs de configuration des actifs informatiques et des configurations de base, et leur comparaison avec la configuration réelle.

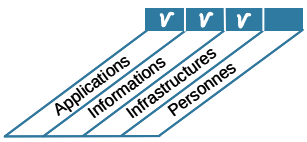
atteint son objectif en

- constituant un référentiel centralisé de tous les éléments de configuration
- identifiant les éléments de configuration et en les maintenant à jour
- vérifiant l'intégrité des données de configuration

et est mesuré par

- le nombre de problèmes de conformité métiers dus à une mauvaise configuration des matériels et logiciels
- le nombre de différences entre le référentiel de configuration et les configurations réelles
- le pourcentage de licences achetées qui ne sont pas prises en compte par le référentiel





OBJECTIFS DE CONTRÔLE

DS9 Gérer la configuration

DS9.1 Référentiel de configuration et configuration de base
Constituer un référentiel centralisé et mettre en place un outil pour recenser toutes les informations qui concernent les éléments de configuration. Surveiller et enregistrer tous les actifs et les changements qui y sont apportés. Pour chaque système et chaque service tenir à jour une base des composants de sa configuration pour pouvoir s'y référer après une modification.

DS9.2 Identification et maintenance des éléments de configuration
Mettre en place des procédures spécifiques pour faciliter la gestion et l'enregistrement de tous les changements apportés au référentiel de configuration. Intégrer ces procédures aux procédures de gestion des changements, de gestion des incidents et de gestion des problèmes.

DS9.3 Revue d'intégrité des configurations
Passer en revue de manière périodique les données de la configuration afin de vérifier et confirmer l'intégrité de la configuration en cours par rapport à son historique. Vérifier régulièrement les logiciels installés par rapport aux politiques d'utilisation des logiciels afin d'identifier les logiciels personnels ou sans licence, ou tout nombre de licences excessif par rapport aux contrats de licence en cours. Rédiger un rapport et agir pour corriger les erreurs ou les anomalies.

GUIDE DE MANAGEMENT

DS9 Gérer la configuration

De	Entrées
AI4	Manuels utilisateur, d'exploitation, d'assistance, technique et d'administration
AI7	Eléments de configuration mis à disposition
DS4	Eléments de configuration informatique critiques

Sorties	Vers						
Configuration informatique/détail des actifs	DS8	D10	DS13				
Demande de modification (où et comment faire la modification)	AI6						
Rapports sur la performance des processus	SE1						

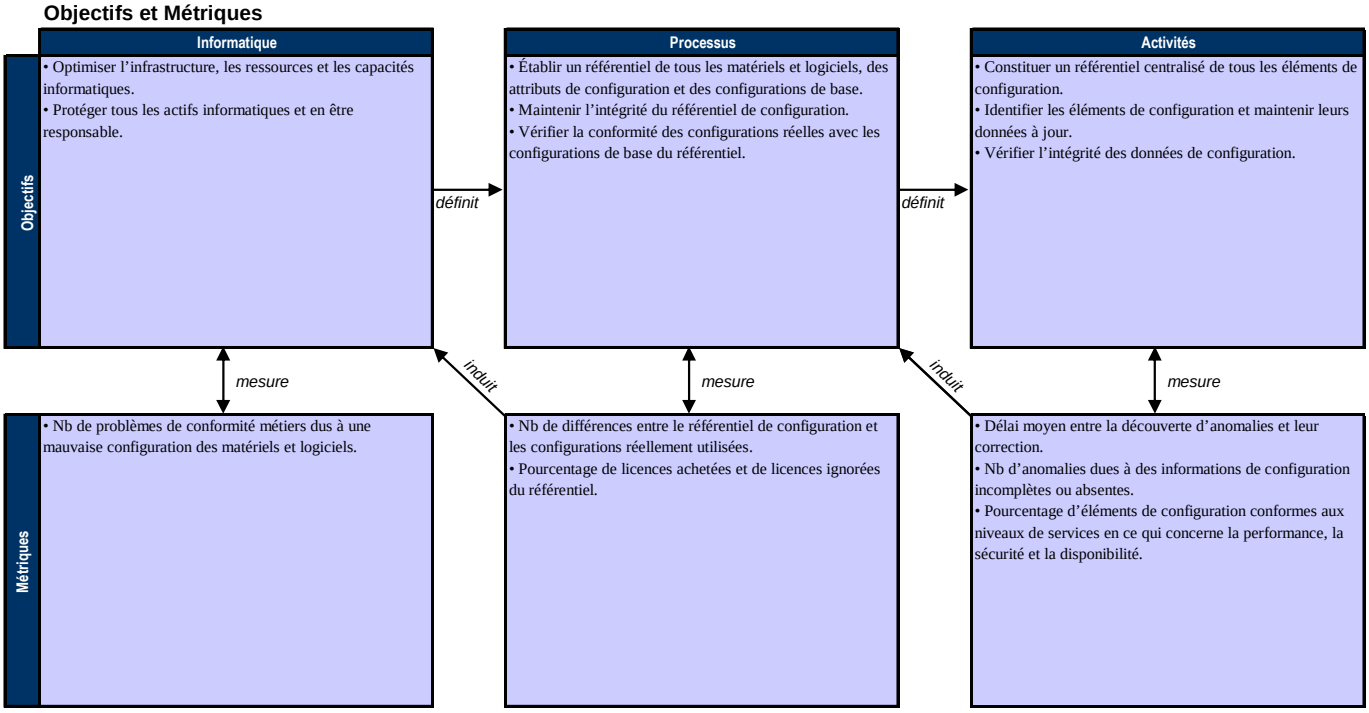
Tableau RACI

Fonctions

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité	Responsable configuration
Développer les procédures de planification de la gestion des configurations.					C	A	C	I	C		C	R
Collecter les informations des configurations initiales et établir les configurations de base.						C	C	C			I	A/R
Vérifier et auditer les informations de configuration (y compris détection des logiciels non autorisés).		I				A			I		I	A/R
Mettre à jour le référentiel de configuration.						R	R	R			I	A/R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS9 Gérer la configuration

La gestion du processus *Gérer la configuration* qui répond à l'exigence des métiers vis-à-vis de l'informatique *optimiser l'infrastructure, les ressources et les capacités informatiques, et justifier les investissements informatiques* est :

0 Inexistante quand

Le management ne voit pas d'intérêt à disposer d'un processus capable de gérer la configuration matérielle et logicielle et de faire des rapports.

1 Initialisée, au cas par cas quand

On reconnaît le besoin d'une gestion de la configuration. Les tâches de base de cette gestion, comme tenir à jour les inventaires des matériels et des logiciels, sont accomplies sur initiatives individuelles. Il n'existe pas de pratiques standard.

2 Reproductible mais intuitive quand

Le management est conscient du besoin de contrôler la configuration informatique et comprend les avantages d'une information exacte et complète sur la configuration, mais on se fie implicitement aux connaissances et aux compétences du personnel technique. On utilise jusqu'à un certain point des outils de gestion de configuration, mais ils diffèrent selon les plates-formes. De plus aucune pratique standard n'est définie. Le contenu des données de configuration est limité et ne concerne pas les processus liés les uns aux autres comme la gestion des changements et des incidents.

3 Définie quand

On documente, standardise et communique les procédures et les pratiques de travail, mais chacun décide de suivre ou non une formation, et d'appliquer ou non les normes. De plus, on est en train de mettre en place des outils de gestion des configurations communs aux différentes plates-formes. Il est peu vraisemblable que l'on détecte les cas de non-respect des procédures, et les vérifications physiques ne sont pas systématiques. On a recours à certains automatismes pour permettre de tracer plus facilement les modifications des matériels et des logiciels. Les données de configurations sont utilisées par des processus liés les uns aux autres.

4 Gérée et mesurable quand

Le besoin de gérer la configuration est reconnu à tous les niveaux de l'entreprise, et les bonnes pratiques continuent à évoluer. On communique sur les procédures et les normes, on les inclut dans les formations, et on veille à leur respect ; les cas de non-respect sont surveillés, détectés et font l'objet de rapports. On utilise des outils automatisés comme la technologie push pour imposer les normes et améliorer la stabilité des systèmes. Les systèmes de gestion de configuration recouvrent effectivement la plus grande partie des actifs informatiques et permettent une bonne gestion des versions et du contrôle de la distribution des matériels et des logiciels. On pratique systématiquement les vérifications physiques et l'analyse des anomalies ; on recherche les causes initiales des anomalies.

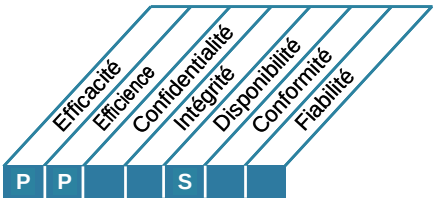
5 Optimisée quand

Tous les actifs informatiques sont gérés au sein d'un système de gestion centralisé des configurations qui contient toute l'information nécessaire sur les composants, leurs interrelations et l'historique de leur évolution. Les données de configuration sont conformes aux descriptifs fournis par les fournisseurs. Les processus reliés entre eux sont pleinement intégrés, et ils utilisent et mettent à jour les données de configuration de façon automatique. Les rapports d'audits de base fournissent pour chaque élément matériel et logiciel les données essentielles pour les réparations, la maintenance, la garantie, la mise à niveau, et les évaluations techniques. On applique les règles destinées à limiter l'installation de logiciels non autorisés. Le management prévoit les réparations et les mises à niveau à partir de rapports d'analyses qui proposent un planning des évolutions et qui précisent les possibilités d'actualisation des technologies. Chaque actif informatique est protégé par un suivi et une surveillance individuels contre le vol, le mauvais usage et les usages abusifs.

DESCRIPTION DU PROCESSUS

DS10 Gérer les problèmes

Une gestion efficace des problèmes exige de les identifier, de les classer, d'analyser leurs causes initiales et de leur trouver des solutions. Le processus de gestion des problèmes implique aussi de formuler des recommandations d'amélioration, de tenir à jour les enregistrements des problèmes et de vérifier où en sont les actions correctives. Un processus efficace de gestion des problèmes favorise la disponibilité des systèmes, améliore les niveaux de services, réduit les coûts, répond mieux aux besoins des clients et augmente donc leur satisfaction.



Le contrôle du processus informatique

Gérer les problèmes

qui répond à l'exigence des métiers vis-à-vis de l'informatique

assurer la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services, réduire les défauts des solutions et de la fourniture de services et diminuer la quantité de travail à refaire.

en se concentrant sur

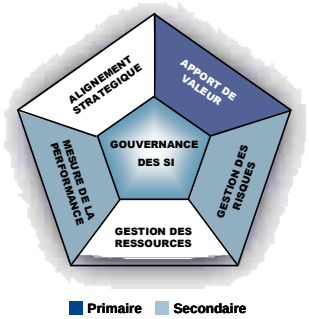
l'enregistrement, le suivi et la résolution des problèmes d'exploitation, la recherche des causes initiales de tous les problèmes significatifs, et la définition de solutions pour les problèmes d'exploitation identifiés.

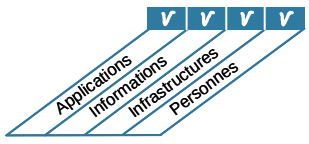
atteint son objectif en

- faisant l'analyse causale des problèmes identifiés
- analysant les tendances
- assumant la propriété des problèmes et en faisant avancer leur résolution

et est mesuré par

- le nombre de problèmes récurrents qui ont des conséquences sur l'activité
- le pourcentage de problèmes résolus dans les délais requis
- la fréquence des rapports ou des mises à jour concernant un problème persistant, en fonction de la gravité du problème





OBJECTIFS DE CONTRÔLE

DS10 Gérer les problèmes

DS10.1 Identification et classification des problèmes
Mettre en place des processus pour rapporter et classer les problèmes qui ont été identifiés comme relevant de la gestion des incidents. Les étapes de la classification des problèmes sont similaires à celles de la classification des incidents ; elles consistent à déterminer la catégorie, l'impact, l'urgence et la priorité. Répartir les problèmes selon les groupes ou domaines auxquels ils appartiennent (par ex. matériel, logiciel, logiciel d'assistance). Ces groupes peuvent correspondre aux responsabilités dans l'entreprise, ou au service auquel appartient l'utilisateur ou le client, et doivent servir à déterminer l'équipe d'assistance à laquelle ils seront affectés.

DS10.2 Suivi et résolution des problèmes
S'assurer que le système de gestion des problèmes fournit les outils de pistes d'audit adéquats qui permettent de suivre, d'analyser et de déterminer les causes initiales de tous les problèmes rapportés en prenant en compte :

- Tous les éléments de configuration associés
- Les problèmes et les incidents non résolus
- Les erreurs connues et soupçonnées
- Le repérage des tendances en matière de problèmes

Trouver et initier des solutions viables qui s'appliquent aux causes initiales, en suscitant des demandes de modification par l'intermédiaire du processus de gestion des changements. Au cours du processus de résolution, les responsables de la gestion des problèmes doivent obtenir des rapports réguliers de l'équipe de gestion des modifications sur la progression de la résolution des problèmes et des erreurs. La gestion des problèmes doit surveiller en continu les conséquences sur les services utilisateurs des erreurs et des problèmes connus. Dans le cas où ces conséquences deviendraient graves, l'équipe de gestion des problèmes doit faire remonter le problème, peut-être à un niveau de direction approprié, pour augmenter la priorité de la demande de modification, ou pour mettre en œuvre une modification d'urgence selon le cas. Suivre la progression de la résolution du problème conformément aux contrats de services.

DS10.3 Clôture des problèmes
Mettre en place une procédure pour clôturer les enregistrements de problèmes, soit après confirmation de l'élimination réussie de l'erreur connue, soit après un accord avec les métiers sur la façon de trouver une solution alternative.

DS10.4 Intégration de la gestion de la configuration, des incidents et des problèmes
Pour assurer une gestion efficace des problèmes et faciliter le progrès, intégrer les processus de gestion de la configuration, de gestion des incidents et de gestion des problèmes.

GUIDE DE MANAGEMENT

DS10 Gérer les problèmes

De	Entrées
AI6	Autorisation de modification
DS8	Rapports d'incidents
DS9	Configuration informatique/détail des actifs
DS13	Historiques des erreurs

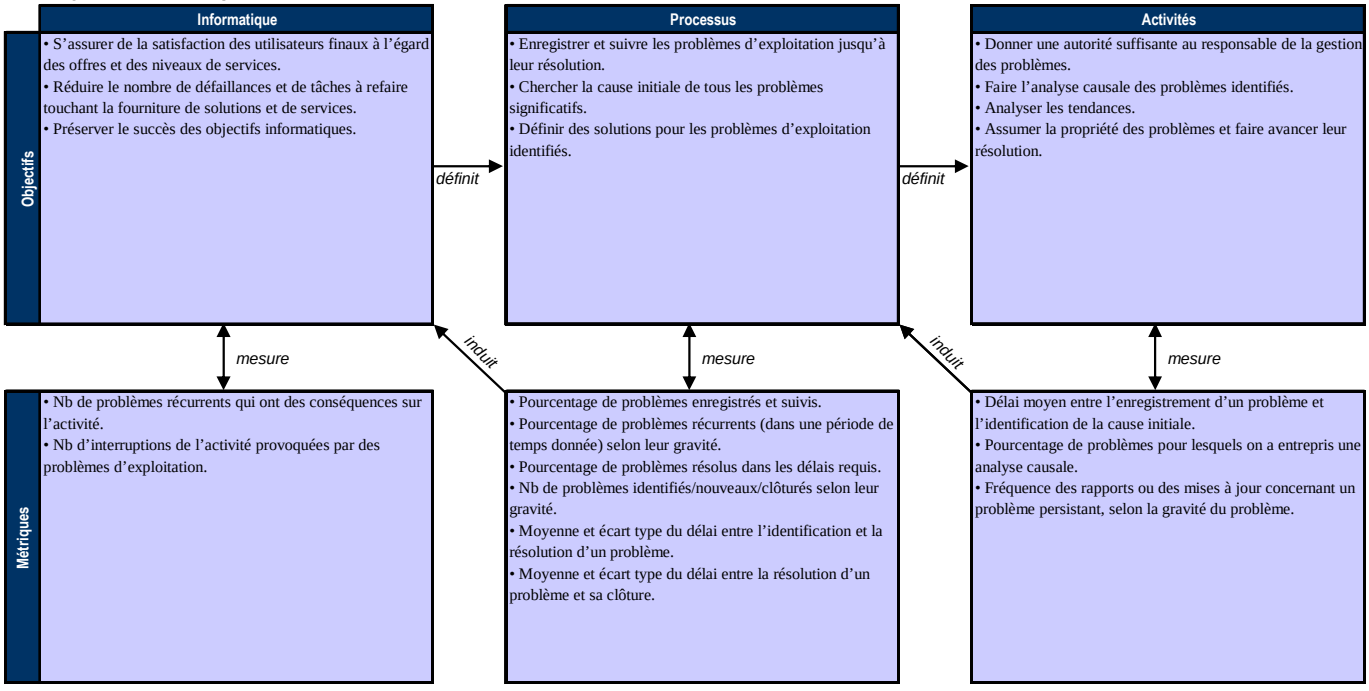
Sorties	Vers
Demandes de modification	AI6
Historiques des problèmes	AI6
Rapports sur la performance des processus	SE1
Problèmes connus, erreurs connues et solutions de contournement	DS8

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité	Resp. gestion des problèmes
Identifier et classer les problèmes.			I	I	C	A	C	C			I	R
Effectuer les analyses causales.						C		C				A/R
Résoudre les problèmes.					C	A	R	R		R	C	C
Passer en revue la situation en cours des problèmes.			I	I	C	A/R	C	C		C	C	R
Émettre des recommandations d'amélioration, et établir une demande de modification en rapport.					I	A	I	I		I		R
Tenir à jour les enregistrements des problèmes.					I	I		I			I	A/R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS10 Gérer les problèmes

La gestion du processus *Gérer les problèmes* qui répond à l'exigence des métiers vis-à-vis de l'informatique *assurer la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services, réduire les défauts des solutions et de la fourniture de services et diminuer la quantité de travail à refaire* est :

0 Inexistante quand

On n'a pas conscience du besoin de gérer les problèmes, car on ne fait pas de différence entre les problèmes et les incidents. Il n'y a donc pas de tentatives pour identifier les causes initiales des incidents.

1 Initialisée, au cas par cas quand

Le personnel reconnaît le besoin de gérer les problèmes et d'éliminer les causes. Des personnes clés apportent leur aide pour des problèmes qui relèvent de leur spécialité, mais la responsabilité de la gestion des problèmes n'est pas attribuée. L'information n'est pas partagée, ce qui fait naître des problèmes supplémentaires et une perte de temps productif pendant qu'on cherche des réponses.

2 Reproductible mais intuitive quand

On est largement conscient du besoin et de l'avantage de gérer les problèmes liés aux SI, aussi bien dans les unités métiers qu'au sein de la fonction informatique. Le processus de résolution évolue et est désormais entre les mains de quelques individus clés qui ont la responsabilité d'identifier et de résoudre les problèmes. L'information est partagée parmi les employés de façon informelle et en fonction des circonstances. Le niveau de services fournis à la communauté des utilisateurs est variable, et est entravé par le manque de connaissances structurées accessibles au responsable de la gestion des problèmes.

3 Définie quand

Le besoin d'un système intégré de gestion des problèmes efficace est accepté et soutenu par le management, et on dispose de budgets pour le personnel et pour la formation. Les processus de résolution et d'escalade ont été standardisés. La recherche et l'enregistrement des problèmes et de leurs solutions sont répartis au sein de l'équipe de traitement des problèmes de façon fragmentaire ; on utilise les outils disponibles, mais il n'y a pas de centralisation. On ne détectera vraisemblablement pas les écarts par rapport aux normes et aux standards établis. L'information est partagée par le personnel de façon proactive et formelle. Le management passe les incidents en revue et fait une analyse de l'identification et de la résolution des problèmes, mais de façon limitée et informelle.

4 Gérée et mesurable quand

Tous les niveaux de l'entreprise ont compris le processus de gestion des problèmes. On a clairement réparti les responsabilités et la propriété du processus. On a documenté les méthodes et les procédures, on les a communiquées et on a mesuré leur efficacité. La majorité des problèmes sont identifiés, enregistrés et rapportés, et leur résolution est mise en chantier. On cultive et on entretient le niveau de connaissances et de compétence ; on l'élève à des niveaux de plus en plus élevés du fait que la fonction résolution des problèmes est considérée comme un atout essentiel pour atteindre les objectifs informatique et pour l'amélioration des services informatiques. La gestion des problèmes est bien intégrée aux processus qui lui sont liés tels que gestion des incidents, des changements, de la disponibilité et de la configuration ; elle aide les clients à gérer les données, les équipements et l'exploitation. On s'est mis d'accord sur les ICP et le ICO du processus de gestion des problèmes.

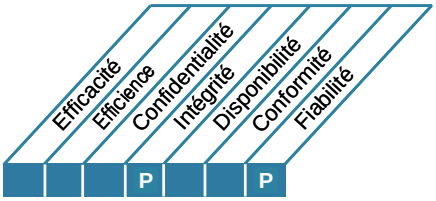
5 Optimisée quand

Le processus de gestion des problèmes évolue : il est désormais capable d'anticiper à plus long terme, contribuant ainsi aux objectifs des SI. On anticipe et on prévient les problèmes. On entretient les connaissances grâce à des contacts réguliers avec les fournisseurs et les experts sur des types de problèmes passés ou à venir. L'enregistrement, le compte rendu et l'analyse des problèmes et de leur résolution sont automatisés et pleinement intégrés à la gestion des données de configuration. On mesure régulièrement les objectifs. La plupart des systèmes ont été équipés de mécanismes de détection et d'alertes automatiques qui sont suivis et évalués en permanence. On analyse le processus de gestion des problèmes pour son amélioration continue en fonction des mesures et on en fait des comptes-rendus aux parties prenantes.

DESCRIPTION DU PROCESSUS

DS11 Gérer les données

Une gestion efficace des données impose d'identifier les exigences qui les concernent. Le processus de gestion des données nécessite aussi de mettre en place des procédures efficaces pour gérer la médiathèque, les sauvegardes et la restauration des données, et l'élimination des médias de façon appropriée. Une gestion efficace des données aide à garantir la qualité et la disponibilité au moment opportun des données métiers.



Le contrôle du processus informatique

Gérer les données

qui répond à l'exigence des métiers vis-à-vis de l'informatique

optimiser l'utilisation de l'information et s'assurer qu'elle est disponible lorsqu'on en a besoin

en se concentrant sur

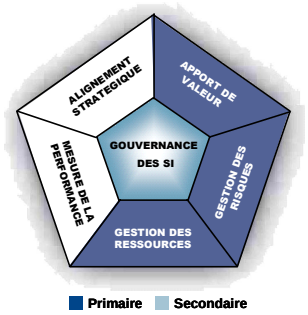
l'exhaustivité, l'exactitude, la disponibilité et la protection des données

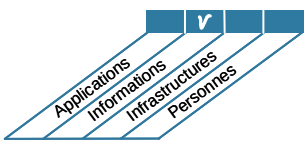
atteint son objectif en

- sauvegardant les données et en testant leur restauration
- gérant le stockage des données sur site et hors site
- disposant d'un moyen sûr d'éliminer les données et le matériel

et est mesuré par

- le pourcentage d'utilisateurs satisfaits de la disponibilité des données
- le pourcentage de restaurations des données réussies
- le nombre d'incidents au cours desquels des données sensibles ont été restaurées après la mise au rebut des médias





OBJECTIFS DE CONTRÔLE

DS11 Gérer les données

DS11.1 Exigences des métiers pour la gestion des données
Vérifier qu'on reçoit toutes les données attendues d'un traitement et qu'elles sont traitées complètement, avec justesse, en temps opportun et que tous les résultats sont fournis conformément aux exigences des métiers. Prendre en compte les besoins de redémarrage et de retraitement.

DS11.2 Dispositifs de stockage et de conservation
Définir et mettre en place des procédures efficaces et efficientes de stockage, de conservation et d'archivage des données en réponse aux objectifs des métiers ainsi qu'aux exigences de la politique de sécurité de l'entreprise et aux exigences réglementaires.

DS11.3 Système de gestion de la médiathèque
Définir et mettre en place des procédures pour tenir à jour un inventaire des médias stockés et archivés de façon à s'assurer qu'ils sont utilisables et garantir leur intégrité.

DS11.4 Mise au rebut
Définir et mettre en œuvre des procédures permettant de s'assurer que les exigences des métiers en termes de protection de données sensibles et de logiciels sont satisfaites lors de la mise au rebut ou du transfert de données et de matériel.

DS11.5 Sauvegarde et restauration
Définir et mettre en place des procédures pour la sauvegarde et la restauration des systèmes, des applications, des données et de la documentation conformes aux exigences des métiers et au plan de continuité.

DS11.6 Exigences de sécurité pour la gestion des données
Définir et mettre en place des politiques et procédures pour identifier et mettre en œuvre les exigences de sécurité applicables à la réception, au traitement, au stockage physique et à la sortie de données conformément aux objectifs des métiers, aux exigences de la politique de sécurité de l'entreprise et aux exigences réglementaires.

GUIDE DE MANAGEMENT

DS11 Gérer les données

De	Entrées
PO2	Dictionnaire des données ; classifications attribuées aux données
AI4	Manuels utilisateur, d'exploitation, d'assistance, technique et d'administration
DS1	CE
DS4	Plans de stockage et de protection des sauvegardes
DS5	Plan et politiques de sécurité informatique

Sorties	Vers
Rapports sur la performance des processus	SE1
Instructions d'exploitation pour la gestion des données	DS13

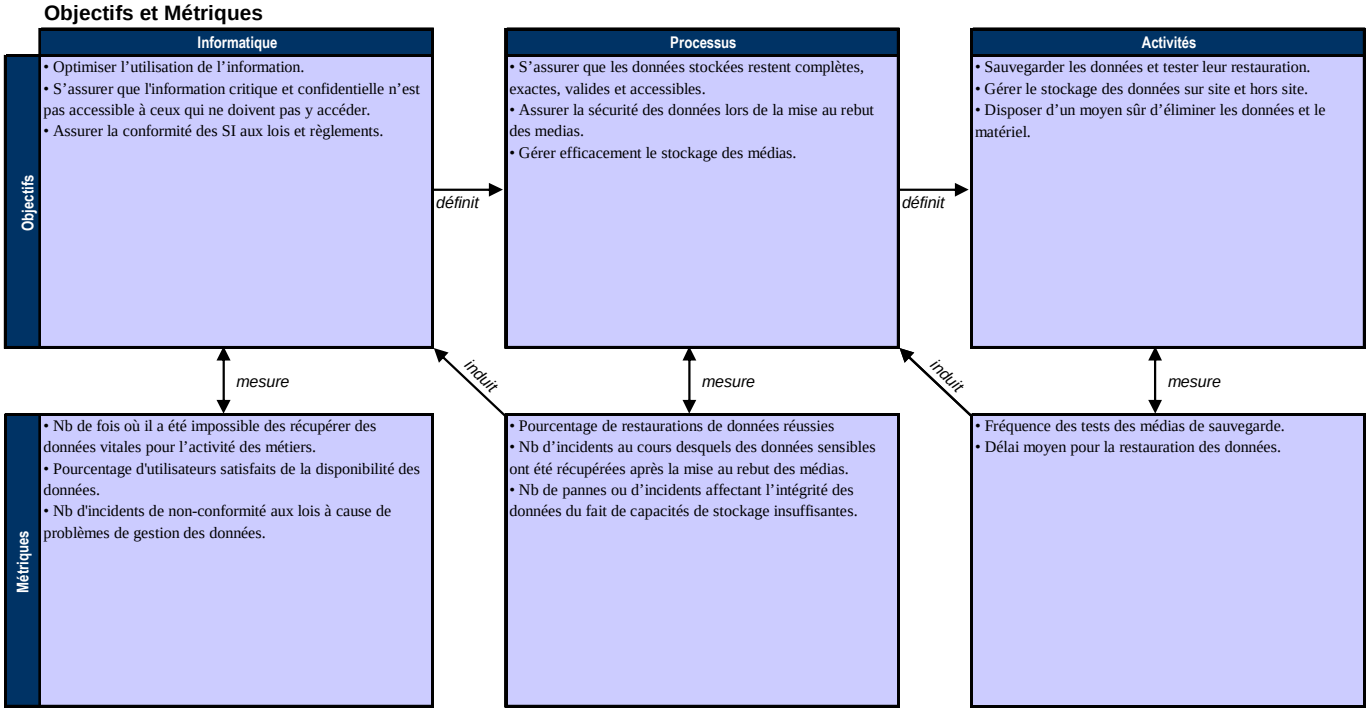
Tableau RACI

Fonctions

Activités	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Traduire en procédures les exigences de stockage et de conservation des données.				A	I	C	R				C
Définir, tenir à jour et mettre en place les procédures pour gérer la médiathèque.				A		R	C	C	I		C
Définir, tenir à jour et mettre en place les procédures pour une mise au rebut sécurisée des médias et des équipements.				A	C	R			I		C
Sauvegarder les données selon le plan prévu.				A		R					
Définir, tenir à jour et mettre en place les procédures de restauration des données.				A	C	R	C	C			I

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS11 Gérer les données

La gestion du processus *Gérer les données* qui répond à l'exigence des métiers vis-à-vis de l'informatique *optimiser l'utilisation de l'information et s'assurer qu'elle est disponible lorsqu'on en a besoin* est :

0 Inexistante quand

Les données ne sont pas considérées comme des ressources ni comme des actifs de l'entreprise. Elles n'ont pas de propriétaire, et personne n'est individuellement responsable de leur gestion. La qualité et la sécurité des données sont faibles ou nulles.

1 Initialisée, au cas par cas quand

L'entreprise reconnaît le besoin d'une gestion efficace des données. Il existe une approche au cas par cas pour spécifier les exigences de sécurité concernant la gestion des données, mais il n'existe pas de procédures formelles de communication. Il n'y a pas de formation sur la gestion des données. La responsabilité de la gestion des données n'est pas claire. Les procédures de sauvegarde/restauration et les dispositifs de mise au rebut sont en place.

2 Reproductible mais intuitive quand

La conscience du besoin d'une gestion précise des données existe dans l'ensemble de l'entreprise. On commence à attribuer la propriété des données à haut niveau. Les exigences de sécurité pour la gestion des données sont documentées par des individus clés. On fait une certaine surveillance des activités clés de gestion des données au sein de l'informatique (par ex. sauvegarde, restauration, destruction). On a attribué de façon informelle les responsabilités de la gestion des données à des individus clés de l'informatique.

3 Définie quand

On a compris et accepté le besoin de gestion des données dans toute l'organisation. La responsabilité de la gestion des données est établie. La propriété des données est attribuée au groupe responsable qui contrôle l'intégrité et la sécurité. Les procédures de gestion des données sont formalisées au sein de l'informatique et on utilise certains outils de sauvegarde/restauration et de mise au rebut des équipements. Une certaine surveillance de la gestion des données est en place. Les métriques de base de performance sont définies. On commence à voir des formations pour le personnel en charge de la gestion des données.

4 Gérée et mesurable quand

On comprend le besoin de gérer les données et on accepte les actions nécessaires à cet objectif dans l'entreprise. Les responsabilités de la propriété et de la gestion des données sont clairement définies, attribuées et communiquées dans l'entreprise. On a formalisé les procédures, elles sont largement connues, et on partage les connaissances. On commence à utiliser les outils disponibles. Les indicateurs de performance et d'objectifs sont adoptés en accord avec les clients et surveillés au moyen d'un processus bien défini. Une formation formalisée à l'intention du personnel de gestion des données est en place.

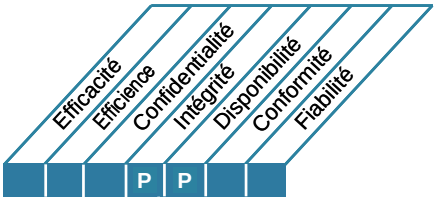
5 Optimisée quand

Le besoin de gérer les données et toutes les actions nécessaires à cet objectif sont compris et acceptés dans l'entreprise. On analyse de façon proactive les besoins et les exigences futurs. On a clairement établi les responsabilités de la propriété des données et de leur gestion, elles sont largement connues dans l'entreprise et révisées lorsque c'est opportun. On a formalisé les procédures, elles sont largement connues, et le partage les connaissances est devenu une pratique standard. On utilise des outils sophistiqués et automatisés au maximum pour la gestion des données. Les indicateurs de performance et d'objectifs sont adoptés en accord avec les clients, ils sont liés aux objectifs des métiers et régulièrement surveillés au moyen d'un processus bien défini. On explore en permanence les opportunités d'amélioration. On a institutionnalisé la formation du personnel de gestion des données.

DESCRIPTION DU PROCESSUS

DS12 Gérer l'environnement physique

La protection des équipements informatiques et du personnel exige des installations matérielles bien conçues et bien gérées. Le processus de gestion de l'environnement matériel comporte la définition des exigences du site physique, le choix des installations adéquates et la conception de processus efficaces de surveillance des facteurs environnementaux et de gestion des accès physiques. La gestion efficace de l'environnement physique réduit les risques d'interruption de l'activité du fait de dommages subis par le matériel informatique et par le personnel.



Le contrôle du processus informatique

Gérer l'environnement physique

qui répond à l'exigence des métiers vis-à-vis de l'informatique

protéger les actifs informatiques et les données métiers et réduire le risque d'interruption de l'activité

en se concentrant sur

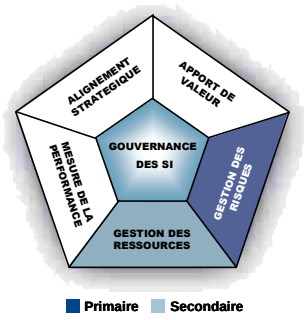
la fourniture et la maintenance d'un environnement physique adapté pour protéger l'accès aux ressources informatiques, leur détérioration ou leur vol

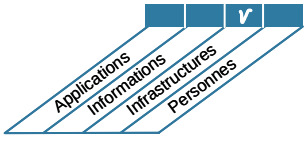
atteint son objectif en

- mettant en place des mesures de sécurité
- sélectionnant et en gérant les installations

et est mesuré par

- le nombre d'interruptions de service dues à des incidents touchant l'environnement physique
- le nombre d'incidents dus à des problèmes de sécurité physique ou à des pannes
- la fréquence des évaluations et des revues du risque physique





OBJECTIFS DE CONTRÔLE

DS12 Gérer l'environnement physique

DS12.1 Sélection du site et agencement
Définir et sélectionner les sites physiques des équipements informatiques en conformité avec la stratégie informatique elle-même liée à la stratégie des métiers. La sélection et la conception de l'agencement d'un site doivent prendre en compte les risques liés aux sinistres d'origine naturelle ou humaine, ainsi que les lois et règlements concernant par exemple la médecine du travail et les réglementations sur la sécurité.

DS12.2 Mesures de sécurité physique
Définir et mettre en place des mesures de sécurité physique conformes aux exigences des métiers pour sécuriser le site et les actifs physiques. Les mesures de sécurité physique doivent permettre de prévenir, détecter et réduire de manière efficace les risques liés au vol, à la température, à l'incendie, à la fumée, à l'eau, aux vibrations, au terrorisme, au vandalisme, aux pannes d'électricité, aux produits chimiques et aux explosifs.

DS12.3 Accès physique
Définir et mettre en place les procédures d'autorisation, de limitation et de suppression d'accès aux sites, bâtiments et zones selon les besoins des métiers, sans oublier les cas d'urgence. Les accès aux sites, bâtiments et zones doivent être justifiés, autorisés, enregistrés et faire l'objet d'une surveillance. Cela doit s'appliquer à toutes les personnes qui entrent sur le site, y compris le personnel permanent ou temporaire, les clients, les fournisseurs, les visiteurs et tout autre tiers.

DS12.4 Protection contre les risques liés à l'environnement
Élaborer et mettre en place des mesures de protection contre les facteurs environnementaux. Installer des équipements et des dispositifs spécialisés pour surveiller et contrôler l'environnement.

DS12.5 Gestion des installations matérielles
Gérer les installations, y compris les équipements électriques et de communication, conformément aux lois et règlements, aux exigences techniques et métiers, aux spécifications des fournisseurs, et aux règles concernant la santé et la sécurité.

GUIDE DE MANAGEMENT

DS12 Gérer l'environnement physique

De	Entrées
PO2	Classifications attribuées aux données
PO9	Évaluation des risques
AI3	Exigences de l'environnement physique

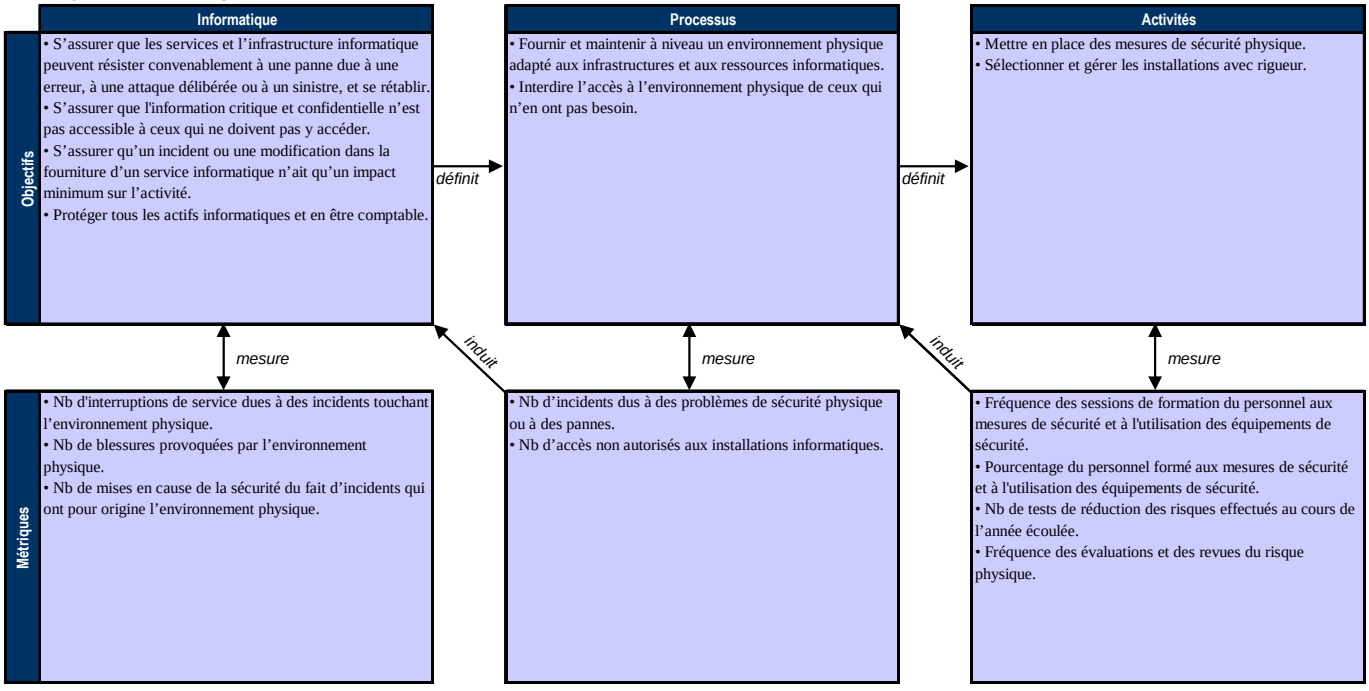
Sorties	Vers
Rapports sur la performance des processus	SE1

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir le niveau de protection physique requis.					C	A/R	C				C
Choisir le site et se le faire attribuer (centre de traitement, bureaux etc.).	I	C	C	C	C	A/R	C		C	C	C
Mettre en place des mesures relatives à l'environnement physique.					I	A/R	I	I			C
Gérer l'environnement physique (y compris maintenance, surveillance, comptes-rendus).						A/R	C				
Définir et mettre en place les procédures d'accès physique, d'autorisation et de mise à jour.				C	I	A/R	I	I	I		C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS12 Gérer l'environnement physique

La gestion du processus *Gérer l'environnement physique* qui répond à l'exigence des métiers vis-à-vis de l'informatique de *protéger les actifs informatiques et les données métiers et réduire le risque d'interruption de l'activité* est :

0 Inexistante quand

Personne n'a conscience de la nécessité de protéger les installations ou les investissements en ressources informatiques. On n'exerce ni surveillance ni contrôle sur les facteurs de risques environnementaux comme le feu, la poussière, l'électricité ou les excès de chaleur ou d'humidité.

1 Initialisée, au cas par cas quand

L'entreprise admet qu'il est nécessaire pour l'activité professionnelle de mettre en place un environnement physique adapté qui protège les ressources et le personnel contre les dangers d'origine naturelle ou humaine. La gestion des installations et des équipements ne dépend que des compétences et aptitudes de certains individus clés. Le personnel peut circuler dans les locaux sans restriction. Le management ne surveille pas le contrôle de l'environnement des installations ni les mouvements du personnel.

2 Reproductible mais intuitive quand

Les contrôles de l'environnement sont mis en place et suivis par le personnel d'exploitation. La sécurité physique est un processus informel, initié par un petit groupe d'employés très sensibles à la sécurité des installations matérielles. Les procédures de maintenance des installations ne sont pas bien documentées et s'appuient sur les bonnes pratiques de quelques individus. Les objectifs de sécurité physique ne sont basés sur aucune norme formelle, et le management ne s'assure pas que les objectifs sont atteints.

3 Définie quand

Le besoin de maintenir un environnement informatique contrôlé est compris et accepté dans l'entreprise. Les contrôles environnementaux, la maintenance préventive et la sécurité physique sont des postes budgétaires approuvés et suivis par les dirigeants. On applique des restrictions d'accès, et seul le personnel accrédité peut accéder aux installations informatiques. On enregistre les visiteurs, et on les escorte si cela paraît nécessaire. Les installations matérielles ne se font pas remarquer et ne sont pas identifiables au premier coup d'œil. Les autorités civiles surveillent la conformité avec les règles d'hygiène et de sécurité. L'entreprise a contracté une assurance risques, mais l'effort pour optimiser son coût est minime.

4 Gérée et mesurable quand

Le besoin de maintenir un environnement informatique contrôlé apparaît comme une évidence dans la structure de l'entreprise et dans l'attribution du budget. Les exigences de sécurité de l'environnement et des installations sont documentées, et les accès sont strictement contrôlés et surveillés. On a désigné les responsables et les propriétaires, et on a fait connaître leurs noms. Le personnel qui travaille sur les installations est complètement formé aux situations d'urgence ainsi qu'aux pratiques d'hygiène et de sécurité. Des mécanismes de contrôle standardisés sont en place pour restreindre les accès aux installations et pour agir sur les facteurs d'environnement et de sécurité. Le management surveille l'efficacité des contrôles et leur conformité aux normes établies. Le management a mis au point des objectifs et des métriques pour évaluer la gestion de l'environnement informatique. La possibilité de rétablir les ressources informatiques fait partie du processus de gestion des risques de l'entreprise. On intègre l'information pour optimiser la couverture des assurances et leur coût.

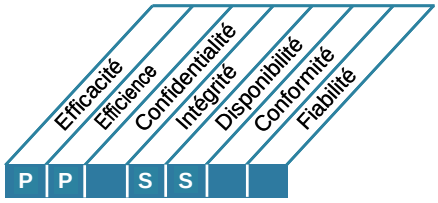
5 Optimisée quand

Il existe un plan à long terme qui concerne les installations nécessaires à l'environnement informatique de l'entreprise. On a défini pour toutes les installations des normes qui s'appliquent au choix des sites, à la construction, au gardiennage, au personnel de sécurité, aux systèmes mécaniques et électriques, à la protection contre les risques liés à l'environnement (ex. feu, foudre, inondations...). Toutes les installations sont inventoriées et classées en conformité avec le processus continu de gestion des risques de l'entreprise. Les accès sont strictement contrôlés et surveillés en permanence en fonction des besoins professionnels, et les visiteurs sont systématiquement escortés. L'environnement est surveillé et contrôlé au moyen de matériels spécialisés, et personne n'est présent dans les locaux techniques. On évalue et on mesure régulièrement les objectifs. Les programmes de maintenance préventive suivent en pratique un respect strict des plannings et on fait régulièrement subir des tests aux équipements sensibles. La stratégie et les normes qui concernent les installations sont alignées sur les objectifs de disponibilité des services informatiques, et elles font partie intégrante de la planification de la continuité de l'activité de l'entreprise, et de la gestion de crise. Le management passe en revue et optimise les installations régulièrement en s'appuyant sur les objectifs et les métriques, et il profite des occasions qui se présentent pour améliorer la contribution des SI aux métiers.

DESCRIPTION DU PROCESSUS

DS13 Gérer l'exploitation

Pour un traitement complet et exact des données il faut une gestion efficace des procédures de traitement des données et une maintenance appliquée du matériel informatique. Ce processus implique de définir des politiques et des procédures d'exploitation nécessaires à une gestion efficace des traitements programmés, de protéger les sorties sensibles, de surveiller l'infrastructure et d'effectuer une maintenance préventive du matériel. La gestion efficace de l'exploitation aide à maintenir l'intégrité des données et à réduire les délais et les coûts d'exploitation informatique.



Le contrôle du processus informatique

Gérer l'exploitation

qui répond à l'exigence des métiers vis-à-vis de l'informatique

maintenir l'intégrité des données et garantir que l'infrastructure informatique peut résister/se rétablir en cas d'erreurs ou de défaillances

en se concentrant sur

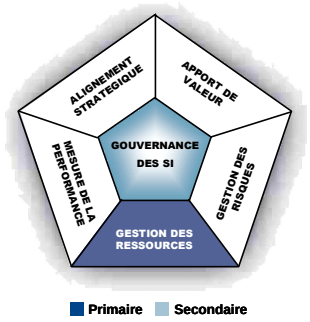
la gestion des niveaux de services d'exploitation pour les traitements programmés, la protection des sorties sensibles, et la surveillance et la maintenance de l'infrastructure

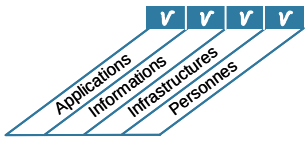
atteint son objectif en

- exploitant l'environnement informatique conformément aux niveaux de services convenus et aux instructions définies
- assurant la maintenance de l'infrastructure informatique

et est mesuré par

- le nombre de contrats de services ayant eu à pâtir d'incidents d'exploitation
- le nombre d'heures d'inactivité non prévues provoquées par des incidents d'exploitation
- le pourcentage d'actifs matériels pris en compte dans les programmes de maintenance préventive





OBJECTIFS DE CONTRÔLE

DS13 Gérer l'exploitation

DS13.1 Procédures et instructions d'exploitation
Définir, mettre en place et tenir à jour des procédures standard pour l'exploitation informatique, en s'assurant que le personnel connaît bien toutes les tâches d'exploitation qui dépendent de lui. Les procédures d'exploitation doivent tenir compte des changements d'équipes (passation des consignes formalisée, états d'avancement, problèmes d'exploitation, procédures d'escalade et rapports sur les responsabilités en cours) pour répondre aux contrats de services convenus et garantir la continuité de l'exploitation.

DS13.2 Planification des travaux
Organiser la planification des travaux, processus et tâches selon la séquence la plus efficace, en optimisant le débit et l'utilisation des ressources pour répondre aux exigences des métiers.

DS13.3 Surveillance de l'infrastructure informatique
Définir et mettre en place des procédures pour surveiller l'infrastructure informatique et les événements qui s'y rapportent. S'assurer qu'un historique suffisant des opérations est stocké dans les journaux d'exploitation pour permettre la reconstruction, la revue et l'analyse des séquences chronologiques des traitements et des autres activités liées à ces traitements ou leur apportant un soutien.

DS13.4 Documents sensibles et dispositifs de sortie
Mettre en place des dispositifs de sécurité physique appropriés, les pratiques de comptabilité et de gestion d'inventaires pour les actifs informatiques sensibles, comme les formulaires spéciaux, les effets de commerce, les imprimantes spécialisées et les systèmes d'identification.

DS13.5 Maintenance préventive du matériel
Définir et mettre en place des procédures pour garantir la maintenance en temps opportun de l'infrastructure afin de réduire la fréquence et les conséquences de défaillances ou de dégradation des performances.

GUIDE DE MANAGEMENT

DS13 Gérer l'exploitation

De	Entrées
AI4	Manuels utilisateur, d'exploitation, d'assistance, technique et d'administration
AI7	Plans de mises en production, de publication et de diffusion de logiciels
DS1	CS et CE
DS4	Plan de stockage et de protection des sauvegardes
DS9	Configuration informatique/détail des actifs
DS11	Instructions d'exploitation pour la gestion des données

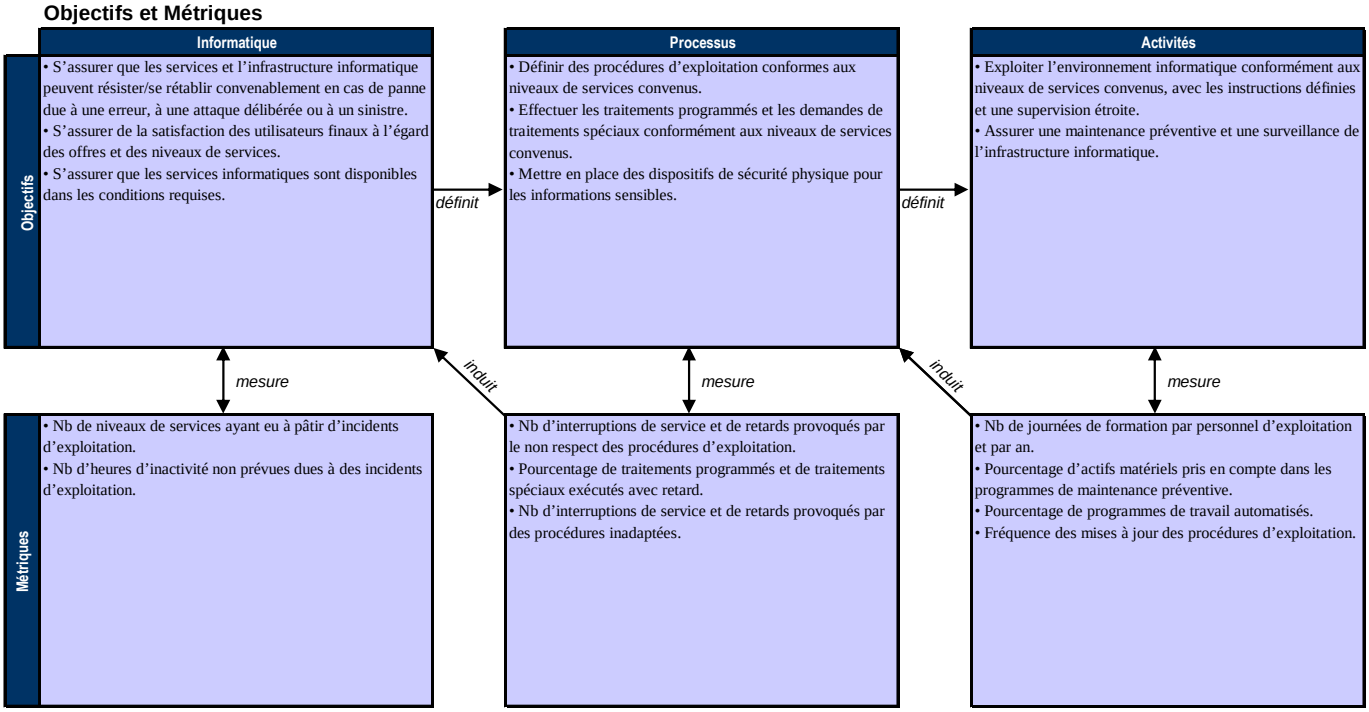
Sorties	Vers
Tickets d'incidents	DS8
Historiques des erreurs	DS10
Rapports sur la performance des processus	SE1

Tableau RACI

Activités \ Fonctions	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Créer/modifier les procédures d'exploitation (comme manuels, listes de contrôle, planning des changements d'équipes, documentation pour la passation des consignes, procédures d'escalade etc.).						A/R					I
Programmer la charge de travail et les traitements par lots.					C	A/R	C	C			
Surveiller l'infrastructure et le traitement, et résoudre les problèmes.						A/R					I
Gérer les sorties et en assurer la sécurité (par exemple papier, supports électroniques).						A/R					C
Appliquer les correctifs et les modifications au planning et à l'infrastructure.					C	A/R	C	C			C
Mettre en place un processus pour préserver les systèmes d'authentification des intrusions, des pertes et du vol.				A		R			I		C
Planifier et effectuer une maintenance préventive.						A/R					

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

DS13 Gérer l'exploitation

La gestion du processus *Gérer l'exploitation* qui répond à l'exigence des métiers vis-à-vis de l'informatique *maintenir l'intégrité des données et garantir que l'infrastructure informatique peut résister/se rétablir en cas d'erreurs ou de défaillances* est :

0 Inexistante quand

L'entreprise ne consacre ni temps ni ressources à la mise en place des éléments de base d'une activité d'assistance informatique ou d'activités d'exploitation informatique.

1 Initialisée, au cas par cas quand

L'entreprise admet qu'il faut structurer les fonctions de support informatique. Cependant on n'a établi que peu de procédures standard, et les activités d'exploitation n'interviennent qu'au cas par cas. La plus grande partie de l'exploitation n'est pas formellement planifiée et les demandes de traitements informatiques sont acceptées sans validation préalable. Les ordinateurs, les systèmes et les applications qui assistent les processus métiers sont souvent interrompus, retardés, indisponibles. Les employés perdent du temps à attendre des ressources disponibles. Les résultats des traitements sortent parfois à des endroits inattendus ou pas du tout.

2 Reproductible mais intuitive quand

L'entreprise est consciente du rôle essentiel que joue l'exploitation informatique en assurant des fonctions d'assistance informatique. On attribue au cas par cas les budgets pour les outils informatiques. L'assistance de l'informatique aux autres fonctions est informelle et intuitive. On dépend largement des compétences et des aptitudes de certains individus. Les instructions précisant ce qu'il faut faire, quand, et dans quel ordre ne sont pas documentées. Il existe des formations d'exploitant et il existe quelques normes officielles de fonctionnement.

3 Définie quand

La nécessité d'une gestion de l'exploitation informatique est comprise et acceptée dans l'entreprise. On attribue les ressources correspondantes, et certaines formations sont faites sur le tas. Les fonctions répétitives sont formellement définies, standardisées, documentées et diffusées. Les événements et les résultats des travaux achevés sont enregistrés, avec des comptes-rendus succincts au management. On introduit l'utilisation d'outils de planification automatique et autres pour limiter les interventions humaines. On introduit des contrôles pour la mise en traitement de nouveaux travaux. On développe une politique formelle pour réduire le nombre d'événements imprévus. Les contrats de maintenance et de services avec les fournisseurs sont encore de nature informelle.

4 Gérée et mesurable quand

On a clairement défini les responsabilités de l'exploitation informatique et des activités de support, et on en a désigné les propriétaires. On a dégagé pour l'exploitation des ressources dans les budgets d'investissements et dans les ressources humaines. La formation est formalisée et permanente. Les plannings et les tâches sont documentés et diffusés à la fois au sein de la fonction informatique et aux clients métiers. Il est possible de mesurer et de surveiller les activités quotidiennes en relation avec les contrats de performance standard et les niveaux de services convenus. On relève et on corrige rapidement tout écart par rapport aux normes établies. Le management surveille l'utilisation des ressources informatiques et la bonne fin des travaux et des tâches assignées. Il existe un effort constant pour améliorer le niveau d'automatisation des processus comme moyen d'amélioration continue. On a établi des contrats formels de maintenance et de services avec les fournisseurs. L'alignement est total avec les processus de gestion des problèmes et de la capacité, entre autres grâce à l'analyse des causes des échecs et des erreurs.

5 Optimisée quand

Le support informatique et l'exploitation sont efficaces, efficients et suffisamment souples pour atteindre les niveaux de services souhaités, avec des pertes de productivité minimales. Les processus de gestion de l'exploitation sont standardisés et documentés dans une base de connaissances, et sont sujets à de continuelles améliorations. Les processus automatisés qui supportent les systèmes fonctionnent sans à-coups et contribuent à un environnement stable. On analyse tous les problèmes et les échecs pour trouver les causes initiales. Des réunions régulières avec l'équipe de gestion des changements permettent d'inclure en temps utile des modifications dans les plannings de production. L'âge et les disfonctionnements des matériels sont analysés en coopération avec les fournisseurs, et la maintenance devient essentiellement préventive.

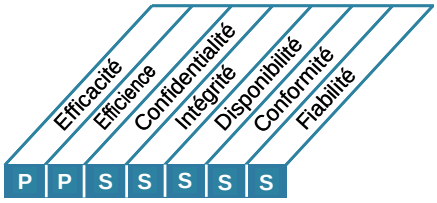
SURVEILLER ET EVALUER

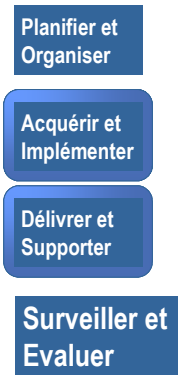
SE1 Surveiller et évaluer la performance des SI
SE2 Surveiller et évaluer le contrôle interne
SE3 S'assurer de la conformité aux obligations externes
SE4 Mettre en place une gouvernance des SI

DESCRIPTION DU PROCESSUS

SE1 Surveiller et évaluer les performances des SI

Une gestion efficace des SI exige un processus de surveillance. Ce processus inclut la définition d'indicateurs pertinents de performance, la publication systématique et en temps opportun de rapports sur la performance, et une réaction rapide aux anomalies. Il faut une surveillance pour s'assurer qu'on fait ce qu'il faut conformément aux orientations et aux politiques définies.





Le contrôle du processus informatique

Surveiller et évaluer la performance des SI

qui répond à l'exigence des métiers vis-à-vis de l'informatique

transparence et compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services informatiques conformément aux exigences de la gouvernance

en se concentrant sur

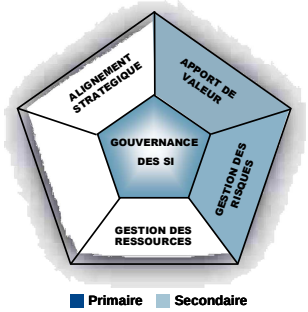
la surveillance des métriques des processus et leurs comptes-rendus, et la recherche et la mise en place d'actions destinées à améliorer la performance

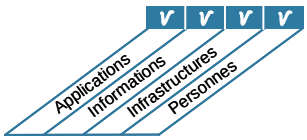
atteint son objectif en

- collationnant des rapports de performance et en les traduisant en rapports de gestion
- comparant les performances aux objectifs convenus et en mettant en place des actions correctrices lorsque c'est nécessaire

et est mesuré par

- la satisfaction du management et des responsables de la gouvernance à propos des rapports de performance
- le nombre d'actions d'améliorations suscitées par les activités de surveillance le nombre de processus critiques surveillés





OBJECTIFS DE CONTRÔLE

SE1 Surveiller et évaluer la performance des SI

SE1.1 Approche de la surveillance
Constituer un référentiel et une approche générale de la surveillance qui définisse l'étendue, la méthodologie et le processus à suivre pour mesurer la délivrance de solutions et de services informatiques et surveiller la contribution des SI aux métiers. Intégrer ce référentiel au système de gestion des performances de l'entreprise.

SE1.2 Définition et collationnement des données de surveillance
En associant les métiers, définir un ensemble équilibré d'objectifs de performance et les faire approuver par les métiers et par les autres parties prenantes concernées. Mettre en place des analyses comparatives pour définir les objectifs et recenser les données nécessaires à collecter pour mesurer ces objectifs. Mettre en place les processus pour collecter des données exactes au bon moment et rendre compte de la progression vers les objectifs visés.

SE1.3 Méthode de surveillance
Mettre en place une méthode de surveillance (par ex. tableau de bord équilibré) qui prend en compte les objectifs, enregistre les mesures, offre une vision condensée générale de la performance des SI et est compatible avec le système de surveillance de l'entreprise.

SE1.4 Évaluation de la performance
Comparer périodiquement les performances aux objectifs, analyser les causes des écarts et initier des actions correctives pour traiter les causes sous-jacentes. De temps en temps, réaliser des analyses causales de ces écarts.

SE1.5 Comptes-rendus destinés au conseil d'administration et à la direction générale
Produire à la direction générale des rapports sur la contribution des SI aux métiers, particulièrement en ce qui concerne la performance du portefeuille de l'entreprise, les programmes d'investissements dépendant de l'informatique et la performance des solutions et services délivrés par chacun des programmes. Les rapports indiquent dans quelle mesure les objectifs prévus ont été atteints, les ressources budgétisées utilisées, les objectifs de performance prévus atteints et les risques réduits. Anticiper sur la revue qui en sera faite par la direction générale en proposant des actions correctives pour remédier aux écarts les plus importants. Fournir les rapports à la direction générale et lui demander un retour après revue.

SE1.6 Actions correctives
Définir et entreprendre les actions correctives qui s'appuient sur la surveillance, l'évaluation et le compte-rendu de la performance. Cela implique un suivi de toutes les actions de surveillance, de compte-rendu et d'évaluation par :

- L'examen, la discussion et l'élaboration de propositions d'actions correctives par le management
- L'attribution de la responsabilité de l'action corrective
- Le suivi des résultats de cette action.

GUIDE DE MANAGEMENT

SE1 Surveiller et évaluer la performance des SI

De	Entrées
PO5	Rapports coûts/bénéfices
PO10	Rapports sur la performance des projets
AI6	Rapports sur le statut des changements
DS1-13	Rapports sur la performance des processus
DS8	Rapports sur la satisfaction des utilisateurs
SE2	Rapport sur l'efficacité des contrôles informatiques
SE3	Rapports sur la conformité des activités informatiques aux exigences légales et réglementaires externes
SE4	Etat de situation de la gouvernance des SI

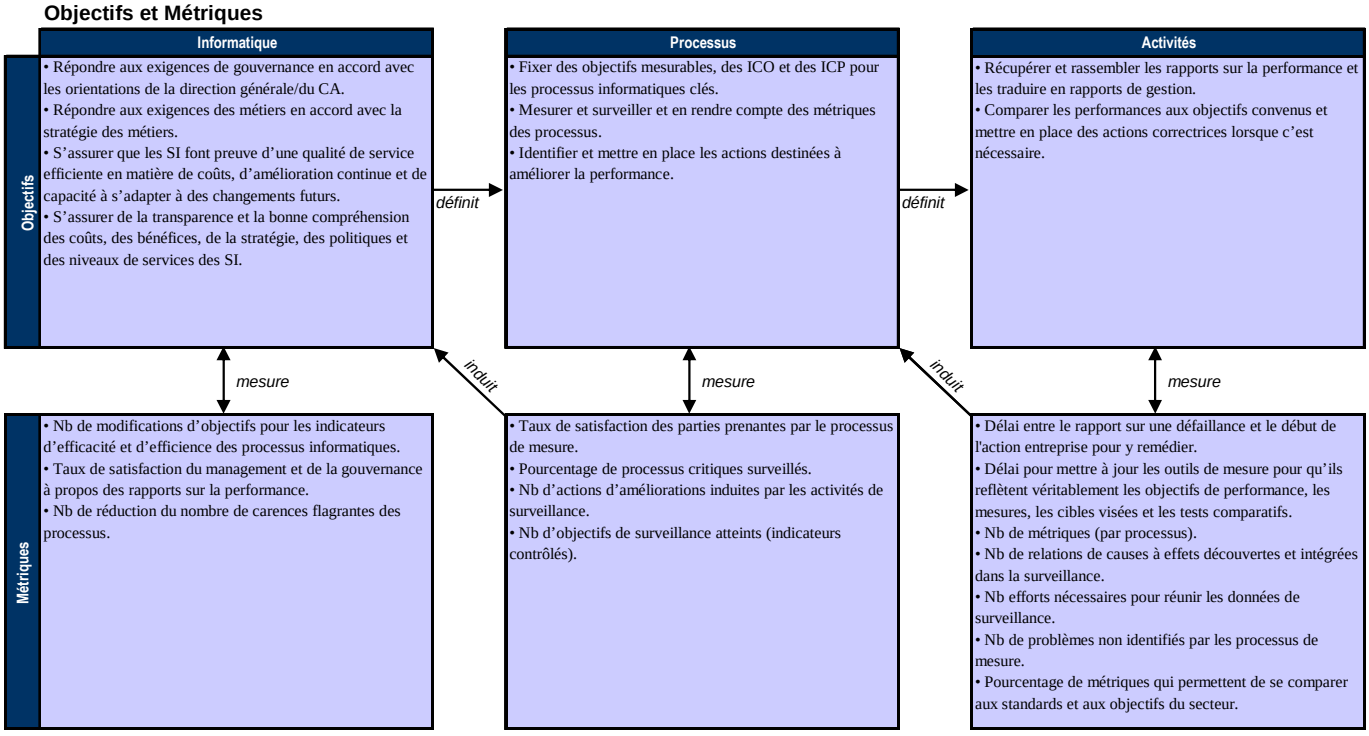
Sorties	Vers						
Entrée de la performance dans le planning SI	PO1	PO2	DS1				
Plans d'actions correctives	PO4	PO8					
Historique des événements de risque et des tendances	PO9						
Rapports sur la performance des processus	SE2						

Tableau RACI

Activités \ Fonctions	CA	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Bâtir l'approche de surveillance.		A	R	C	R	I	C	I	C	I		C
Identifier et faire la liste des objectifs mesurables qui vont dans le sens des objectifs métiers.		C	C	C	A	R	R		R			
Créer des tableaux de bord.					A		R	C	R	C		
Évaluer la performance.			I	I	A	R	R	C	R	C		
Rendre compte de la performance.	I	I	I	R	A	R	R	C	R	C		I
Identifier et surveiller les actions destinées à améliorer la performance.					A	R	R	C	R	C		C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

SE1 Surveiller et évaluer la performance des SI

La gestion du processus *Surveiller et Évaluer les performances des SI* qui répond à l'exigence des métiers vis-à-vis de l'informatique *transparence et compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services informatiques conformément aux exigences de la gouvernance* est :

0 Inexistante quand

L'entreprise n'a pas mis en place de processus de surveillance. La DSI n'exerce pas de façon indépendante de surveillance des projets ou des processus. On ne dispose pas en temps opportun de rapports utiles ou précis. On ne reconnaît pas le besoin de fixer des objectifs clairs pour les processus.

1 Initialisée, au cas par cas quand

Le management reconnaît le besoin de collecter et d'évaluer des informations pour la surveillance des processus. On n'a pas défini de normes pour la collecte des informations et l'évaluation des processus. La surveillance est mise en place et les métriques sont choisies au cas par cas, en fonction des besoins de projets et de processus informatiques spécifiques. La surveillance est généralement mise en place suite à un incident qui a causé des pertes ou une gêne à l'entreprise. La fonction comptable surveille les mesures financières de base concernant les SI.

2 Reproductible mais intuitive quand

On identifie les mesures de base à surveiller. Il existe des méthodes et des techniques de collecte et d'évaluation mais les processus ne sont pas adoptés dans l'ensemble de l'entreprise. L'interprétation des résultats de la surveillance se base sur les compétences d'individus clés. On choisit et on met en place des outils limités pour collecter les informations, mais sans planification.

3 Définie quand

Le management communique et met en place des processus de surveillance standard. Des programmes d'enseignement et de formation sur la surveillance sont mis en place. On développe et formalise une base de connaissances qui conserve l'historique des performances. L'évaluation est encore faite individuellement pour certains projets et certains processus informatiques, mais elle n'est pas généralisée. On met en place des outils de suivi des processus et des niveaux de services internes à l'informatique. On précise comment mesurer la contribution de l'informatique aux performances de l'entreprise, en utilisant des critères financiers et opérationnels traditionnels. On définit des mesures de performance, des mesures non financières, des mesures stratégiques, des mesures de la satisfaction des clients et de niveaux de services spécifiques à l'informatique. On définit un cadre de référence pour mesurer la performance.

4 Gérée et mesurable quand

Le management définit les marges de tolérance acceptables pour les processus. Les rapports sur les résultats de la surveillance sont standardisés et normalisés. On intègre des outils de mesure à tous les projets et processus informatisés. Les systèmes de reporting de gestion de la fonction informatique de l'entreprise sont formalisés. On intègre des outils automatiques de collecte et de surveillance des informations sur l'activité dans toute l'entreprise et on les mobilise pour faire le suivi des applications, des systèmes et des processus. Le management est capable d'évaluer la performance en se basant sur des critères approuvés par les parties prenantes. Les mesures effectuées par la fonction informatique sont conformes aux objectifs généraux de l'entreprise.

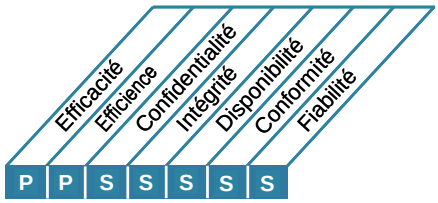
5 Optimisée quand

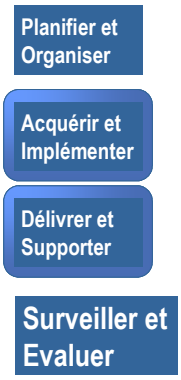
On développe un processus continu d'amélioration de la qualité pour mettre à niveau les standards et les politiques de surveillance à l'échelle de l'entreprise et pour adopter les meilleures pratiques de la profession. Tous les processus de surveillance sont optimisés et travaillent pour les objectifs généraux de l'entreprise. On utilise couramment des métriques inspirées par les métiers pour mesurer les performances et on les intègre dans les schémas d'évaluation stratégiques comme le tableau de bord équilibré. La surveillance et l'amélioration permanente des processus sont conformes aux plans d'amélioration des processus métiers dans l'ensemble de l'entreprise. Les tests comparatifs avec les autres entreprises et avec les principaux concurrents se sont formalisés et utilisent des critères de comparaison bien compris.

DESCRIPTION DU PROCESSUS

SE2 Surveiller et évaluer le contrôle interne

Établir un programme efficace de contrôle interne de l'informatique impose de bien définir un processus de surveillance. Ce processus comporte la surveillance et les rapports sur les anomalies relevées, les résultats des autoévaluations et des revues par des tiers. Un des bénéfices essentiel de la surveillance du contrôle interne est de fournir l'assurance d'une exploitation efficace et efficiente et la conformité aux lois et réglementations en vigueur.





Le contrôle du processus informatique

Surveiller et évaluer le contrôle interne

qui répond à l'exigence des métiers vis-à-vis de l'informatique

protéger la réalisation des objectifs de l'informatique et garantir la conformité aux lois et réglementations applicables aux SI

en se concentrant sur

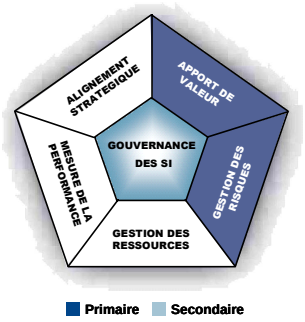
la surveillance des processus de contrôle interne pour les activités liées aux SI et identifier les actions qui permettront des améliorations

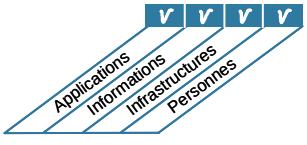
atteint son objectif en

- définissant un système de contrôle interne intégré au référentiel des processus informatiques
- surveillant et en rendant compte de l'efficacité des contrôles internes des SI
- rapportant au management les anomalies détectées par les contrôles pour action

et est mesuré par

- le nombre de manquements majeurs au contrôle interne
- le nombre d'initiatives visant à l'amélioration du contrôle
- le nombre des autoévaluations de contrôle interne et l'éventail d'activités couvertes





OBJECTIFS DE CONTRÔLE

SE2 Surveiller et évaluer le contrôle interne

SE2.1 Surveillance du référentiel de contrôle interne
Surveiller, comparer à l'aide d'analyses et améliorer de façon continue l'environnement de contrôle de l'informatique et le référentiel de contrôle pour atteindre les objectifs de l'entreprise.

SE2.2 Revue générale
Surveiller et évaluer l'efficacité et l'efficience des revues de contrôle interne effectuées par le management de l'informatique.

SE2.3 Anomalies détectées par le contrôle
Identifier les anomalies détectées par le contrôle, les analyser et en identifier les causes sous-jacentes. Faire remonter les anomalies et en produire un rapport pertinent aux parties prenantes. Mettre en place les actions correctives nécessaires.

SE2.4 Autoévaluation du contrôle
Vérifier que les contrôles du management sur les processus informatiques, les politiques et les contrats sont complets et efficaces et réalisés au moyen d'un programme permanent d'autoévaluation.

SE2.5 Assurance de contrôle interne
Obtenir en fonction des besoins l'assurance supplémentaire de l'exhaustivité et de l'efficacité des contrôles internes par des revues effectuées par des tiers.

SE2.6 Contrôle interne des tiers
Évaluer la situation des contrôles internes des fournisseurs de services externe. Confirmer que les fournisseurs de services externes se conforment aux exigences légales et réglementaires, ainsi qu'à leurs obligations contractuelles.

SE2.7 Actions correctives
Définir, initier, mettre en place et suivre les actions correctives résultant des évaluations et les rapports de contrôle.

GUIDE DE MANAGEMENT

SE2 Surveiller et évaluer le contrôle interne

De	Entrées
SE1	Rapports sur la performance des processus

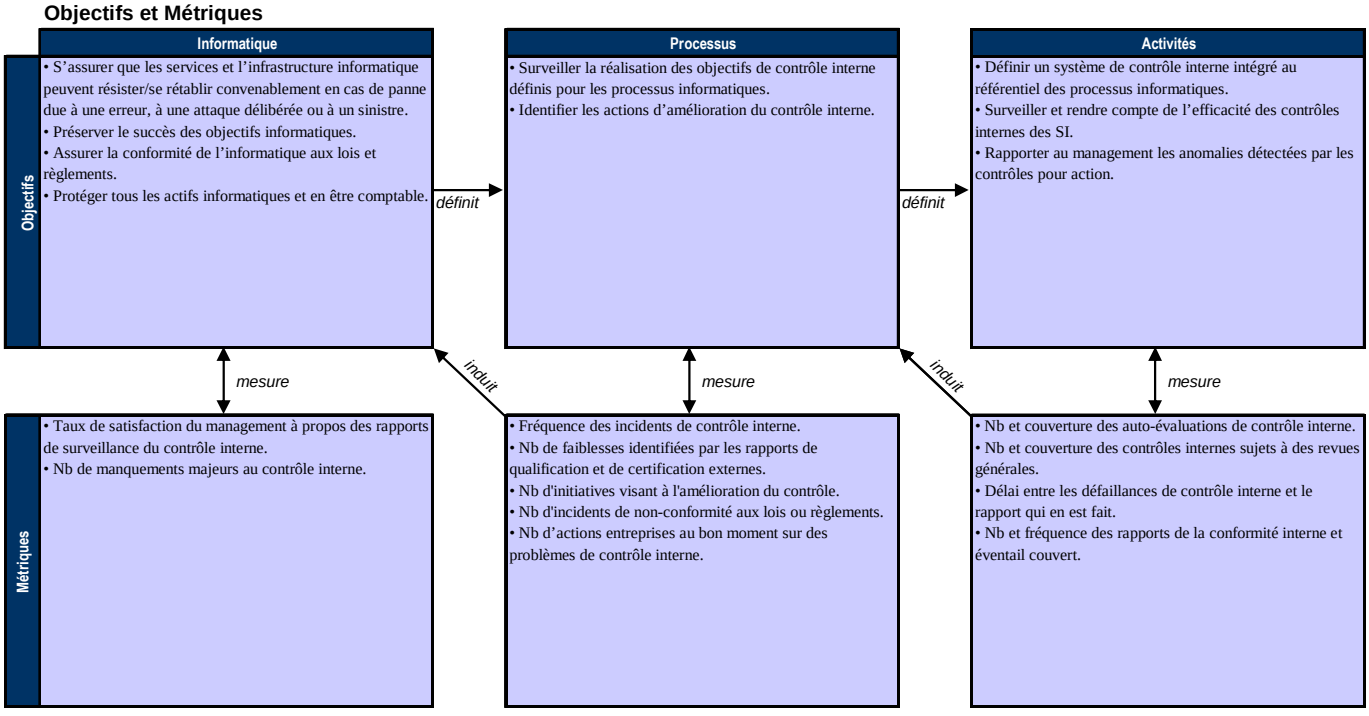
Sorties	Vers						
Rapports sur l'efficacité des contrôles des SI	PO4	PO6	SE1	SE4			

Tableau RACI

Activités \ Fonctions	CA	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Surveiller et contrôler les activités du contrôle interne des SI.					A		R		R	R		R
Surveiller le processus d'auto-évaluation.				I	A		R		R	R		C
Surveiller la performance des revues indépendantes, des audits et des investigations.				I	A		R		R	R		C
Surveiller le processus d'obtention d'une assurance sur les contrôles opérés par des tiers.		I	I	I	A		R		R	R		C
Surveiller le processus d'identification et d'évaluation des anomalies détectées.		I	I	I	A	I	R		R	R		C
Surveiller le processus d'identification et de correction des anomalies détectées.		I	I	I	A	I	R		R	R		C
Rendre compte aux principales parties prenantes.	I	I	I		A/R							I

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

SE2 Surveiller et évaluer le contrôle interne

La gestion du processus *Surveiller et Évaluer le contrôle interne* qui répond à l'exigence des métiers vis-à-vis de l'informatique *protéger la réalisation des objectifs de l'informatique et garantir la conformité aux lois et réglementations applicables aux SI* est :

0 Inexistante quand

L'entreprise n'a pas les procédures qu'il faut pour surveiller l'efficacité des contrôles internes. Il n'y a pas de méthode de reporting pour les contrôles internes. Les questions de sécurité opérationnelle informatique et d'assurance de contrôle interne ne sont en général pas évoquées. Le management et les employés ne sont globalement pas sensibilisés aux contrôles internes.

1 Initialisée, au cas par cas quand

Le management admet le besoin d'une assurance régulière sur le management de l'informatique et son contrôle. On se fie lorsque le besoin s'en fait sentir à des compétences individuelles pour évaluer l'adéquation du contrôle interne. La direction informatique n'a pas formellement désigné de responsable pour la vérification de l'efficacité des contrôles internes. Les évaluations du contrôle interne de l'informatique sont faites à l'occasion des audits financiers traditionnels, avec des méthodologies et des compétences qui ne reflètent pas les besoins de la fonction informatique.

2 Reproductible mais intuitive quand

L'entreprise utilise des rapports de contrôle informels pour initier des actions correctives. L'évaluation du contrôle interne dépend des compétences d'individus clés. L'entreprise prend de plus en plus conscience du besoin de surveillance du contrôle interne. La direction des SI surveille régulièrement l'efficacité de ce qu'elle pense être les contrôles internes les plus sensibles. On commence à utiliser des méthodologies et des outils de surveillance des contrôles internes, mais sans plan. On identifie les facteurs de risques spécifiques à l'environnement informatique grâce aux compétences d'individus clés.

3 Définie quand

Le management apporte son soutien à la surveillance du contrôle interne, et l'a institutionnalisée. On développe des politiques et des procédures pour évaluer et rendre compte des activités de surveillance du contrôle interne. On définit un programme d'enseignement et de formation à la surveillance du contrôle interne. On définit un processus d'autoévaluation des contrôles internes et de revues d'assurance qui précisent les rôles et responsabilités des responsables métiers et de la direction des SI. On utilise des outils qui ne sont cependant pas intégrés à tous les processus. On met en œuvre des politiques d'évaluation des risques informatiques selon des référentiels de contrôle développés spécifiquement pour les SI. On définit des politiques spécifiques d'acceptation et de réduction des risques.

4 Gérée et mesurable quand

Le management met en place un référentiel de surveillance du contrôle interne de l'informatique. L'entreprise établit des niveaux de tolérance pour les processus de surveillance du contrôle interne. On met en place des outils pour standardiser les évaluations et pour que les contrôles détectent automatiquement les anomalies. Une fonction de contrôle interne informatique est formellement mise en place. Elle renferme des professionnels spécialisés et certifiés et utilise un référentiel de contrôle formel approuvé par la direction générale. Les informaticiens particulièrement compétents participent régulièrement aux évaluations de contrôle interne. On constitue une base de connaissances des mesures issues de la surveillance du contrôle interne pour en conserver l'historique. On organise des évaluations par des pairs de cette surveillance.

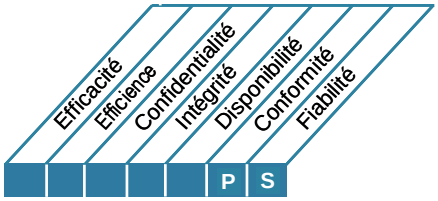
5 Optimisée quand

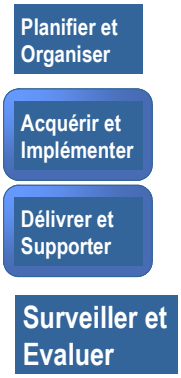
Le management établit un programme continu d'amélioration de la surveillance du contrôle interne à l'échelle de l'entreprise qui prend en compte l'expérience et les bonnes pratiques de la profession. L'entreprise utilise des outils modernes intégrés, lorsque c'est adapté, qui permettent une évaluation efficace des contrôles informatiques critiques et une détection rapide des incidents de surveillance des contrôles informatiques. On a formellement institutionnalisé le partage des connaissances spécifiques à la fonction informatique. On a formalisé des tests comparatifs sur la base des standards et des bonnes pratiques de la profession.

DESCRIPTION DU PROCESSUS

SE3 S'assurer de la conformité aux obligations externes

Un processus de revue est nécessaire pour garantir efficacement la conformité aux lois, aux règlements et aux obligations contractuelles. Ce processus implique d'identifier les obligations de conformité, d'évaluer et d'optimiser la réponse à donner, d'avoir l'assurance d'être conforme aux obligations et, au final, d'intégrer les rapports sur la conformité des SI à ceux du reste de l'entreprise.





Le contrôle du processus informatique

S'assurer de la conformité aux obligations externes

qui répond à l'exigence des métiers vis-à-vis de l'informatique

d'assurer la conformité aux lois, aux règlements et aux obligations contractuelles

en se concentrant sur

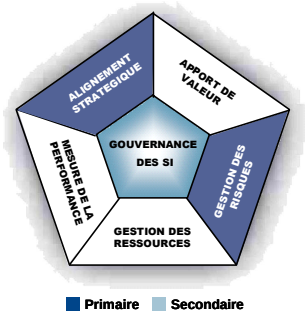
identifier toutes les lois, réglementations et contrats applicables et le niveau de conformité des SI à cet égard, et optimiser les processus informatiques pour réduire le risque de non-conformité

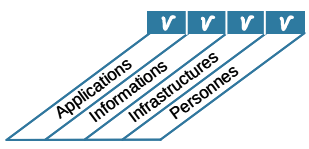
atteint son objectif en

- faisant la liste des obligations légales, réglementaires et contractuelles concernant les SI
- évaluant l'impact des obligations réglementaires
- surveillant la conformité aux obligations et en rendant compte

et est mesuré par

- coût de la non-conformité des SI, en comptant les régularisations et les pénalités
- temps moyen entre l'identification d'un problème de conformité à des exigences externes et sa résolution
- fréquence des revues de conformité





OBJECTIFS DE CONTRÔLE

SE3 S'assurer de la conformité aux obligations externes

SE3.1 Identification des obligations externes : lois, règlements et contrats
Identifier, de façon permanente, les obligations externes auxquelles il faut se conformer : lois nationales et internationales, réglementations et autres, de façon à les prendre en compte dans les politiques, normes, procédures et méthodologies informatiques de l'entreprise.

SE3.2 Optimisation de la réponse aux obligations externes
Réviser et optimiser les politiques, normes, procédures et méthodologies informatiques pour s'assurer que les exigences légales, réglementaires et contractuelles sont prises en compte et font l'objet d'une communication.

SE3.3 Évaluation de la conformité aux obligations externes
Valider la conformité des politiques, normes, procédures et méthodologies informatiques aux obligations externes.

SE3.4 Assurance positive de la conformité
Obtenir l'assurance du respect de la conformité par toutes les politiques internes issues de directives internes ou d'obligations externes légales, réglementaires et contractuelles et en rendre compte. S'assurer que toutes les actions correctives ont été entreprises en temps opportun par le propriétaire du processus responsable pour traiter tous les manquements à la conformité.

SE3.5 Intégration des rapports
Intégrer les rapports de l'informatique sur les obligations légales, réglementaires et contractuelles aux résultats similaires d'autres fonctions métiers.

GUIDE DE MANAGEMENT

SE3 S'assurer de la conformité aux obligations externes

De	Entrées
*	Exigences légales et réglementaires

* Entrées externes à CobiT

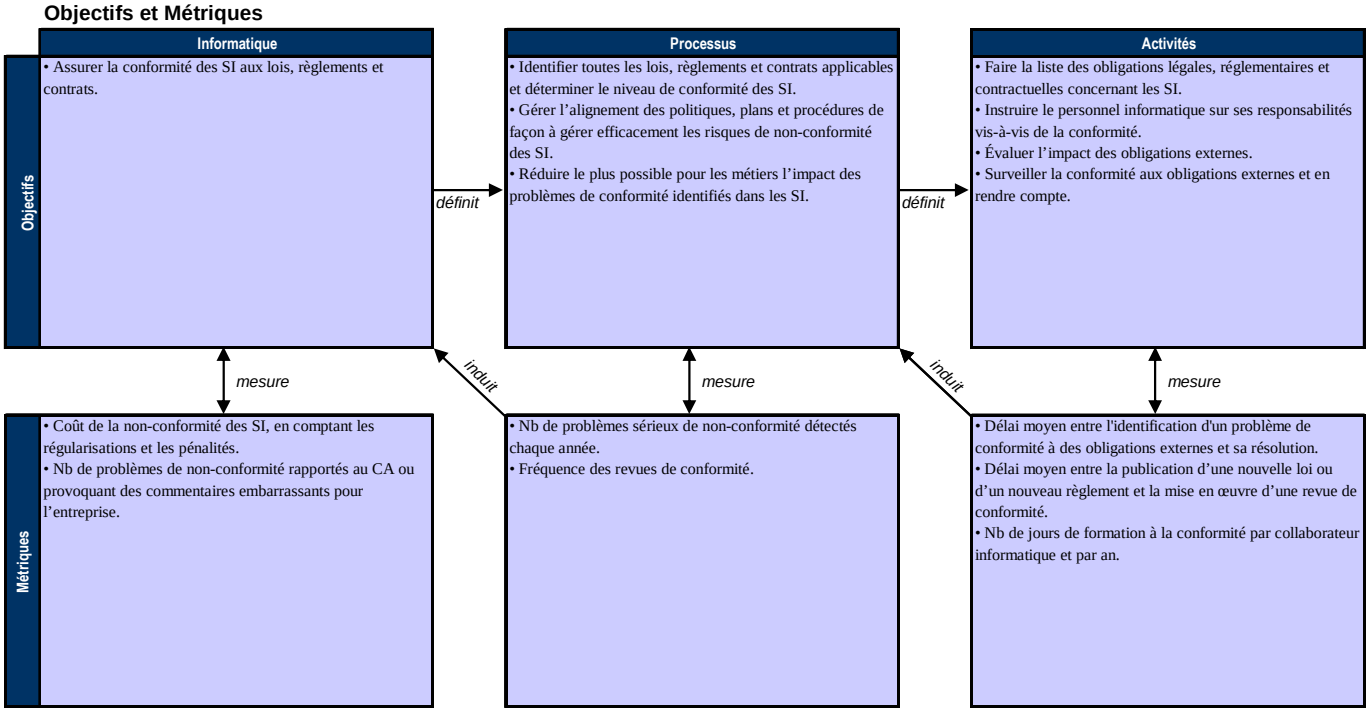
Sorties	Vers						
Catalogue des exigences légales/réglementaires concernant la fourniture de services informatiques	PO4	SE4					
Rapport sur la conformité des activités informatiques aux exigences légales et réglementaires externes	SE1						

Tableau RACI

Activités \ Fonctions	CA	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Définir et mettre en œuvre un processus pour identifier les exigences légales, contractuelles, politiques et réglementaires.					A/R	C	I	I	I	C	I	R
Évaluer la conformité des activités informatiques aux politiques, plans et procédures informatiques.	I	I	I	I	A/R	I	R	R	R	R	R	R
Rendre compte de l'assurance positive de la conformité des activités informatiques aux politiques, plans et procédures informatiques.					A/R	C	C	C	C	C	C	R
Fournir les entrées permettant d'aligner les politiques, les plans et les procédures sur les exigences de conformité.					A/R	C	C	C	C	C		R
Intégrer les rapports des SI sur les exigences réglementaires aux résultats similaires d'autres fonctions métiers.					A/R		I	I	I	R	I	R

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

SE3 S'assurer de la conformité aux obligations externes

La gestion du processus *S'assurer de la conformité aux obligations externes* qui répond à l'exigence des métiers vis-à-vis de l'informatique *d'assurer la conformité aux lois, aux règlements et aux obligations contractuelles* est :

0 Inexistante quand

Il y a peu de prise de conscience des obligations externes relatives aux SI, et aucun processus ne concerne la mise en conformité vis-à-vis des obligations légales, réglementaires et contractuelles.

1 Initialisée, au cas par cas quand

On est conscient des conséquences des obligations réglementaires, contractuelles et légales pour l'entreprise. On suit des processus informels pour maintenir la conformité, mais seulement lorsque le besoin est mis en évidence par de nouveaux projets, des audits ou des revues.

2 Reproductible mais intuitive quand

Le besoin de se conformer aux obligations externes est compris et on communique sur ce thème. Lorsque ce besoin de mise en conformité est récurrent, comme dans les réglementations financières ou la législation sur la vie privée, on a mis en place des procédures individuelles avec un suivi annuel. Il n'y a, cependant, pas d'approche standard. On se repose beaucoup sur les connaissances et la responsabilité des individus, et on peut s'attendre à des erreurs. La formation sur ces questions reste informelle.

3 Définie quand

On développe, documente et communique les politiques, plans, procédures et processus destinés à assurer la conformité aux obligations réglementaires, contractuelles et légales, mais on ne les suit pas toujours, et certaines peuvent être obsolètes ou difficiles à mettre en œuvre. Il y a peu de surveillance et la conformité à certaines exigences n'est pas assurée. Des formations sont programmées sur les obligations légales et réglementaires affectant l'entreprise, et sur les processus de mise en conformité définis. Il existe des contrats standards pro-forma et des processus légaux pour minimiser les risques qui découlent des responsabilités liées aux contrats.

4 Gérée et mesurable quand

On a pleinement compris les problèmes et les risques liés aux obligations externes, et le besoin d'assurer la conformité à tous les niveaux. Il existe un programme de formation formel qui permet de s'assurer que tous les personnels sont conscients de leurs obligations en matière de mise en conformité. Les responsabilités sont claires et la notion de propriété du processus est comprise. Le processus comprend une revue de l'environnement pour mettre en évidence les obligations externes et les changements en cours. On a mis en place un mécanisme qui permet de relever les cas de non-conformité, d'appliquer les pratiques internes, et de prendre des mesures correctives. Les causes de non-conformité sont analysées selon un processus standardisé dans le but de mettre en place des solutions durables. On utilise les bonnes pratiques internes standard pour des besoins spécifiques, tels que les réglementations en vigueur et les contrats de services récurrents.

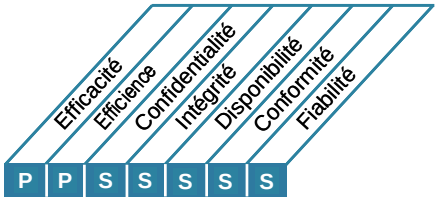
5 Optimisée quand

Pour se conformer aux obligations externes on applique un processus efficace et bien organisé basé sur une seule fonction centrale qui permet d'informer et de coordonner toute l'organisation. On connaît bien les obligations externes applicables ; on se tient informé de leurs évolutions, on anticipe les changements et on prépare des solutions nouvelles. L'entreprise participe à des groupes de discussion externes avec des groupes professionnels ou des instances de régulation pour comprendre et influencer les obligations externes qui l'affecte. On développe les meilleures pratiques pour assurer la conformité aux obligations externes, ce qui se traduit par un très petit nombre de cas de non-conformité. Il existe un système de suivi centralisé à l'échelle de l'entreprise qui permet au management de documenter le flux de travail (workflow) et de mesurer et d'améliorer l'efficacité du processus de surveillance de la conformité. On utilise un processus d'autoévaluation des obligations externes, et on l'améliore pour l'amener au niveau des bonnes pratiques. Le style et la culture du management de l'entreprise en ce qui concerne la conformité sont suffisamment forts, et les processus sont suffisamment bien développés pour que la formation se limite aux nouveaux personnels et aux changements significatifs.

DESCRIPTION DU PROCESSUS

SE4 Mettre en place une gouvernance des SI

Mettre en place un référentiel de gouvernance efficace impose de définir des structures organisationnelles, des processus, un leadership, des rôles et des responsabilités pour s'assurer que les investissements informatiques de l'entreprise sont alignés sur ses stratégies et ses objectifs et qu'ils travaillent pour eux.



Le contrôle du processus informatique

Mettre en place une gouvernance des SI

qui répond à l'exigence des métiers vis-à-vis de l'informatique

intégrer la gouvernance des SI aux objectifs de gouvernance de l'entreprise et se conformer aux lois, règlements et contrats

en se concentrant sur

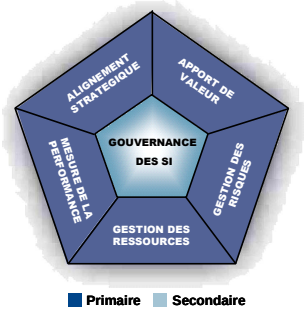
la rédaction de rapports au CA sur la stratégie, les performances et les risques des SI, et la réponse aux exigences de gouvernance conformément aux orientations du CA

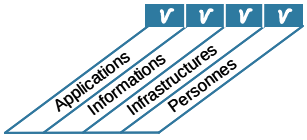
atteint son objectif en

- établissant un référentiel de gouvernance des SI intégré à la gouvernance de l'entreprise
- obtenant une assurance indépendante sur la situation de la gouvernance des SI

et est mesuré par

- la fréquence des rapports au CA sur les SI à l'intention des parties prenantes (entre autres sur la maturité)
- la fréquence des rapports de la DSI au CA (entre autres sur la maturité)
- la fréquence des revues indépendantes de conformité des SI





OBJECTIFS DE CONTRÔLE

SE4 Mettre en place une gouvernance des SI

SE4.1 Mise en place d'un cadre de gouvernance des SI
Définir, mettre en place et aligner le cadre de gouvernance des SI sur celui de l'entreprise et sur son environnement de contrôle. Baser le référentiel de gouvernance sur un processus et un modèle de contrôle de l'informatique adéquats. Éviter toute ambiguïté au niveau des responsabilités et des pratiques qui dégraderait le contrôle interne et la surveillance. Veiller à la conformité aux lois et règlements du cadre de gouvernance, à son alignement sur les objectifs et la stratégie de l'entreprise ainsi qu'à sa contribution en la matière. Rendre compte sur toutes les composantes de la gouvernance des SI.

SE4.2 Alignement stratégique
Faciliter la compréhension par les instances dirigeantes et le management des questions stratégiques concernant les SI comme le rôle des SI, les perspectives offertes par les technologies et leurs capacités. S'assurer qu'on comprend aussi bien du côté des métiers que des SI la contribution potentielle des SI à la stratégie des métiers. Travailler avec le CA et les instances en charge de la gouvernance comme le comité stratégique informatique pour proposer au management des orientations pour les SI, en s'assurant que la stratégie et les objectifs sont répercutés aux unités métiers et aux fonctions informatiques, et que la confiance se développe entre les métiers et l'informatique. Faciliter l'alignement des SI sur les métiers pour la stratégie et le fonctionnement opérationnel, en encourageant la co-responsabilité entre les métiers et l'informatique dans la prise de décisions et l'obtention de bénéfices des investissements dépendants de l'informatique.

SE4.3 Apport de valeur
S'assurer que les programmes d'investissements dépendants de l'informatique et les autres actifs et services informatiques apportent le plus de valeur possible au service de la stratégie et des objectifs de l'entreprise. S'assurer que les résultats des métiers attendus des investissements informatiques et que la totalité des efforts nécessaires pour obtenir ces résultats soient compris, que des analyses de rentabilité complètes et cohérentes soient effectuées et approuvées par les parties prenantes, que les actifs et les investissements soient gérés tout au long de leur cycle de vie, et qu'il existe une gestion active des bénéfices à réaliser, comme la contribution à de nouveaux services, des gains d'efficience et une réactivité accrue aux demandes des clients. Imposer une approche disciplinée de la gestion des portefeuilles, des programmes et des projets, en insistant pour que les métiers assument la propriété de tous les investissements dépendants de l'informatique et que l'informatique assure l'optimisation des coûts de fourniture de capacités et de services informatiques.

SE4.4 Gestion des ressources
Surveiller l'investissement, l'utilisation et l'affectation des actifs informatiques au moyen d'évaluations régulières des actions et de l'exploitation informatique pour s'assurer d'une gestion adéquate des ressources et de leur alignement sur les objectifs stratégiques actuels ainsi que sur les besoins des métiers.

SE4.5 Gestion des risques
Travailler avec le CA pour définir l'appétence de l'entreprise pour le risque informatique et obtenir l'assurance raisonnable que les pratiques de gestion des risques sont adéquates pour s'assurer que le niveau de risque informatique actuel n'excède pas le niveau d'appétence au risque du CA. Intégrer les responsabilités de gestion du risque dans l'entreprise, en s'assurant que les métiers et l'informatique évaluent régulièrement les risques informatiques, leurs conséquences et en rendent compte, et que la position de l'entreprise vis-à-vis du risque informatique est transparente pour les parties prenantes.

SE4.6 Mesure de la performance
Valider que les objectifs informatiques convenus ont été atteints ou dépassés, ou que la progression vers ces objectifs est conforme aux attentes. Réviser les actions correctives prises par le management pour les cas où les objectifs convenus n'ont pas été atteints ou la progression non conforme aux attentes. Rendre compte au CA de la performance des portefeuilles, des programmes et des SI en l'étayant par des rapports pour permettre à la direction générale de passer en revue la progression de l'entreprise vers les objectifs fixés.

SE4.7 Assurance indépendante
Obtenir une assurance indépendante (interne ou externe) sur la conformité des SI aux lois et règlements dont ils relèvent, aux politiques, normes et procédures de l'entreprise, aux pratiques généralement acceptées, et à la performance de l'informatique en termes d'efficacité et d'efficience.

GUIDE DE MANAGEMENT

SE4 Mettre en place une gouvernance des SI

De	Entrées
PO4	Référentiel des processus informatiques
PO5	Rapports coûts/bénéfices
PO9	Évaluations des risques et rapports associés
SE2	Rapport sur l'efficacité des contrôles des SI
SE3	Catalogue des exigences légales/réglementaires concernant la fourniture de services informatiques

Sorties	Vers						
Améliorations du référentiel des processus	PO4						
Etat de situation de la gouvernance des SI	PO1	SE1					
Résultats attendus des investissements métiers qui s'appuient sur les SI	PO5						
Orientation stratégique de l'entreprise pour les SI	PO1						
Appétence de l'entreprise pour le risque informatique	PO9						

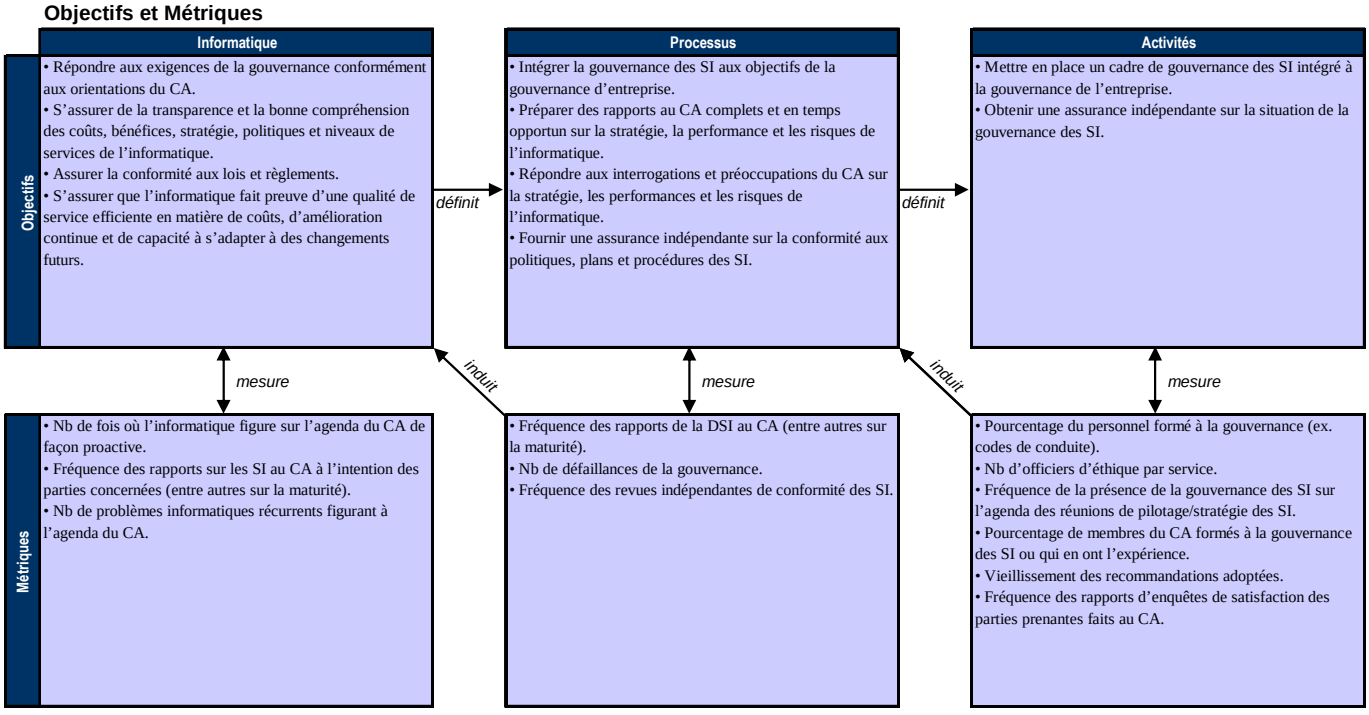
Tableau RACI

Fonctions

Activités	CA	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif des SI	Bureau projet	Conformité, Audit, Risques et Sécurité
Mettre en place la supervision et l'aide de la direction et du CA sur les activités informatiques.	A	R	C	C	C							C
Réviser, approuver, aligner et communiquer les performances, la stratégie, les ressources et la gestion des risques de l'informatique avec la stratégie des métiers.	A	R	I	I	R							C
Obtenir une évaluation périodique indépendante de la performance et de la conformité aux politiques, plans et procédures.	A	R	C	I	C		I	I	I	I	I	R
Résoudre les problèmes détectés par les évaluations indépendantes et assurer la mise en œuvre des recommandations adoptées par le management.	A	R	C	I	C		I	I	I	I	I	R
Générer un rapport sur la gouvernance des SI.	A	C	C	C	R	C	I	I	I	I	I	C

Un tableau **RACI** identifie qui est **R**esponsable, **A**pprouve, est **C**onsulté et/ou **I**nformé.

Objectifs et Métriques



MODÈLE DE MATURITÉ

SE4 Mettre en place une gouvernance des SI

La gestion du processus *Mettre en place une gouvernance des SI* qui répond à l'exigence des métiers vis-à-vis de l'informatique *Intégrer la gouvernance des SI aux objectifs de gouvernance de l'entreprise et se conformer aux lois, règlements et contrats* est :

0 Inexistante quand

Il y a un manque complet de tout processus identifiable de gouvernance des SI. L'entreprise n'envisage même pas qu'il puisse y avoir là un problème à examiner et il n'y a donc pas de communication sur ce thème.

1 Initialisée, au cas par cas quand

On admet qu'il existe des problèmes de gouvernance des SI à traiter. Il existe des approches individuelles au cas par cas. L'approche du management est réactive, et la communication sur ces questions ainsi que la manière de les traiter sont sporadiques et ne montrent aucune méthode. Le management n'a qu'une idée vague de la façon dont l'informatique contribue aux performances de l'activité. Le management ne réagit que lorsqu'un incident a causé des pertes ou une gêne à l'entreprise.

2 Reproductible mais intuitive quand

On est conscient des problèmes de gouvernance des SI. Cette activité, ainsi que les indicateurs de performance, sont en cours de développement, et incluent la planification informatique et les processus de délivrance et de surveillance. On sélectionne, par des décisions individuelles, certains processus informatiques pour les améliorer. Le management détermine les étalons de mesure de base de la gouvernance des SI ainsi que les méthodes et techniques d'évaluation, cependant ce processus n'est pas encore adopté dans l'ensemble de l'entreprise. La communication sur les normes de la gouvernance et sur les responsabilités est laissée à l'initiative individuelle. Certaines personnes pilotent des processus de gouvernance au sein de différents projets et processus informatiques. Les processus, les outils et des métriques pour mesurer la gouvernance des SI sont limités et ne sont pas toujours utilisés faute de bien connaître leurs fonctionnalités.

3 Définie quand

Le management comprend l'importance et le besoin de gouvernance des SI et il en fait part à l'entreprise. On développe un premier ensemble d'indicateurs de gouvernance des SI pour lesquels on définit et documente les liens entre les mesures de résultats et les inducteurs de performance. On standardise et documente les procédures. Le management fait de la communication sur ces procédures standardisées et des formations sont mises en place. On définit des outils d'aide à la supervision de la gouvernance des SI. On définit des tableaux de bord qui font partie du tableau de bord équilibré des SI. On laisse cependant à chacun l'initiative de se former, d'adopter et d'appliquer les normes. Les processus sont éventuellement surveillés, mais les anomalies, même si elles sont traitées par des initiatives individuelles, ne seront vraisemblablement pas détectées par le management.

4 Gérée et mesurable quand

Les principes de gouvernance des SI sont pleinement compris à tous les niveaux. On a clairement compris qui était le client, on a défini les responsabilités et on les surveille au moyen de contrats de services. Les responsabilités sont clairement attribuées et la propriété des processus est établie. Les processus informatiques et la gouvernance des SI sont alignés à la fois sur la stratégie de l'entreprise et sur celle des SI. L'amélioration des processus informatiques est basée avant tout sur une analyse chiffrée des résultats, et il est possible de surveiller et de mesurer la conformité aux métriques des procédures et des processus. Toutes les parties prenantes des processus sont conscientes des risques, mais aussi de l'importance de l'informatique et des opportunités qu'elle peut offrir. Le management définit les marges de tolérance acceptables pour les processus. L'utilisation des technologies est encore limitée, principalement tactique, et basée sur des techniques éprouvées et sur l'utilisation imposée d'outils standard. La gouvernance des SI est intégrée à la planification stratégique et opérationnelle et aux processus de surveillance. On enregistre et on fait le suivi des indicateurs de performance pour toutes les activités de gouvernance des SI, ce qui conduit à des améliorations à l'échelle de l'entreprise. On sait clairement à qui a été attribuée la responsabilité générale de la performance des processus clés, et la mesure de cette performance sert de base à la récompense du management.

5 Optimisée quand

La compréhension des principes de gouvernance des SI et de leur mise en œuvre est de bon niveau et orientée vers l'avenir. La formation et la communication s'appuient sur des concepts et des techniques de pointe. On perfectionne les processus pour les amener au niveau des meilleures pratiques de la profession, grâce aux résultats d'améliorations continues et à la comparaison avec les autres entreprises basée sur les modèles de maturité. La mise en place de politiques informatiques conduit à une organisation, à des personnels et des processus qui s'adaptent rapidement et qui sont en plein accord avec les exigences de la gouvernance des SI. On pratique l'analyse causale de tous les problèmes et de toutes les anomalies, et on trouve rapidement des solutions efficaces qu'on met en œuvre sans tarder. On utilise l'informatique largement et de façon intégrée et optimisée pour automatiser les flux de travail et fournir des outils qui améliorent la qualité et l'efficacité. On sait quels sont les risques et les avantages des processus informatiques, on cherche le bon équilibre et on communique sur ce thème dans l'entreprise. On mobilise des experts externes et on pratique des tests comparatifs pour se guider. La surveillance, l'autoévaluation, et la communication à propos des attentes de la gouvernance se répandent dans toute l'entreprise, et on utilise les technologies au mieux pour faciliter les mesures, l'analyse, la communication et la formation. Il y a un lien stratégique entre la gouvernance d'entreprise et celle des SI, mobilisant les ressources technologiques, humaines et financières pour accroître l'avantage concurrentiel de l'entreprise. Les activités de gouvernance des SI sont intégrées au processus de gouvernance de l'entreprise.

ANNEXE I

TABLEAUX PERMETTANT DE FAIRE LE LIEN ENTRE LES OBJECTIFS MÉTIERS ET LES OBJECTIFS INFORMATIQUES

Cette annexe donne une vision globale de la façon dont les objectifs des métiers génériques sont liés aux objectifs informatiques, aux processus informatiques et aux critères d'information. Il y a trois tableaux :

1. Le premier tableau met en regard des objectifs des métiers, présentés selon les quatre dimensions du tableau de bord équilibré, les objectifs informatiques et les critères d'information. Cela aide à montrer, pour un objectif métier générique donné, les objectifs informatiques qui assistent typiquement cet objectif et les critères d'information COBIT qui sont en rapport avec cet objectif métier. Les 17 objectifs métiers pris en compte ne doivent pas être considérés comme l'ensemble des objectifs métiers possibles mais comme un extrait d'objectifs métiers pertinents ayant un impact certain sur les SI (objectifs métiers relatifs à l'informatique).
2. Le second tableau met en regard les objectifs informatiques, les processus informatiques COBIT impliqués, et les critères d'information sur lesquels se base chaque objectif de l'informatique.
3. Le troisième tableau inverse la lecture en montrant pour chaque processus informatique les objectifs informatiques concernés.

Les tableaux aident à visualiser le champ d'application de COBIT et les relations générales entre COBIT et les facteurs qui influent sur l'activité, permettant aux objectifs métiers typiquement relatifs à l'informatique d'être reliés aux processus informatiques dont ils ont besoin, via les objectifs informatiques. Les tableaux se basent sur des objectifs génériques. Ils doivent donc être utilisés comme un guide et adaptés aux spécificités de l'entreprise.

Pour permettre de faire le lien avec les critères d'information utilisés pour les exigences métiers de la 3è édition de COBIT, les tableaux donnent aussi une indication des principaux critères d'information relatifs aux objectifs métiers et informatiques.

Notes :

1. Les critères d'information des diagrammes des objectifs métiers sont conçus à partir d'une synthèse entre les critères des objectifs Les critères d'information des diagrammes des objectifs métiers sont conçus à partir d'une synthèse entre les critères des objectifs informatiques concernés et une évaluation subjective de ceux qui sont les plus pertinents pour les objectifs métiers. Nous n'avons pas essayé d'indiquer s'ils étaient primaires ou secondaires. Ils ne sont qu'indicatifs, et les utilisateurs peuvent suivre un processus similaire lorsqu'ils évaluent leurs propres objectifs métiers.
2. Les références aux critères d'information primaires et secondaires se basent sur une synthèse entre les critères de chaque processus informatique et une évaluation subjective de ce qui est primaire et secondaire pour l'objectif informatique, puisque certains processus ont plus d'impact que d'autres sur l'objectif informatique. Ils ne sont qu'indicatifs, et les utilisateurs peuvent suivre un processus similaire lorsqu'ils évaluent leurs propres objectifs informatiques

ANNEXE 1 – TABLEAUX PERMETTANT DE FAIRE LE LIEN ENTRE LES OBJECTIFS MÉTIERS ET LES OBJECTIFS INFORMATIQUES

LIER LES OBJECTIFS METIERS AUX OBJECTIFS INFORMATIQUES

		Objectifs métiers	Objectifs Informatiques								Critères d'information CobiT						
											Efficacité	Efficience	Confidentialité	Intégrité	Disponibilité	Conformité	Fiabilité
Perspective financière	1	Obtenir un bon retour sur investissement des investissements informatiques pour les métiers	24									✓					
	2	Gérer les risques métiers liés aux SI	2	14	17	18	19	20	21	22		✓	✓	✓			
	3	Améliorer la gouvernance de l'entreprise et la transparence	2	18													✓
Perspective client	4	Améliorer l'orientation client et le service client	3	23							✓						
	5	Offrir des produits et des services compétitifs	5	24							✓	✓					
	6	Assurer la continuité et la disponibilité des services	10	16	22	23					✓				✓		
	7	Développer l'agilité pour s'adapter aux modifications des exigences des métiers	1	5	25						✓	✓					
	8	Réussir à optimiser les coûts de la fourniture de services	7	8	10	24						✓					
	9	Obtenir de l'information fiable et utile pour prendre des décisions stratégiques	2	4	12	20	26				✓			✓			✓
Perspective interne	10	Améliorer et maintenir à niveau le fonctionnement des processus métiers	6	7	11						✓	✓					
	11	Abaisser les coûts des processus	7	8	13	15	24					✓					
	12	Assurer la conformité aux lois, réglementations et contrats externes	2	19	20	21	22	26	27				✓			✓	
	13	Assurer la conformité aux politiques internes	2	13									✓			✓	
	14	Gérer les changements métiers	1	5	6	11	28				✓	✓					
	15	Améliorer et maintenir la productivité opérationnelle et celle du personnel	7	8	11	13					✓	✓					
Perspective apprentissage et croissance	16	Gérer l'innovation produit et métiers	5	11	28						✓	✓					
	17	Se procurer et conserver un personnel compétent et motivé	9								✓	✓					

LIER LES OBJECTIFS INFORMATIQUES AUX PROCESSUS INFORMATIQUES

	Objectifs Informatiques	Processus										Critères d'information COBIT						
												Efficacité	Efficience	Confidentialité	Intégrité	Disponibilité	Conformité	Fiabilité
1	Réagir aux exigences métiers en accord avec la stratégie métiers	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	SE1	P	P		S	S		
2	Réagir aux exigences de la gouvernance en accord avec les orientations du CA	PO1	PO4	PO10	SE1	SE4						P	P					
3	S'assurer de la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			P	P		S	S		
4	Optimiser l'utilisation de l'information	PO2	DS11										S		P			S
5	Donner de l'agilité à l'informatique	PO2	PO4	PO7	AI3							P	P		S			
6	Déterminer comment traduire les exigences métiers de fonctionnement et de contrôle en solutions automatisées efficaces et efficientes	AI1	AI2	AI6								P	P				S	
7	Acquérir et maintenir fonctionnels des systèmes applicatifs intégrés et standardisés	PO3	AI2	AI5								P	P				S	
8	Acquérir et maintenir opérationnelle une infrastructure informatique intégrée et standardisée	AI3	AI5									S	P					
9	Se procurer et conserver les compétences nécessaires à la mise en œuvre de la stratégie informatique	PO7	AI5									P	P					
10	S'assurer de la satisfaction réciproque dans les relations avec les tiers	DS2										P	P	S	S	S	S	S
11	S'assurer de l'intégration progressive des solutions informatiques aux processus métiers	PO2	AI4	AI7								P	P		S	S		
12	S'assurer de la transparence et la bonne compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services des SI	PO5	PO6	DS1	DS2	DS6	SE1	SE3				P	P				S	S
13	S'assurer d'une bonne utilisation et des bonnes performances des applications et des solutions informatiques	PO6	AI4	AI7	DS7	DS8						P	S					
14	Protéger tous les actifs informatiques et en être comptable	PO9	DS5	DS9	DS12	SE2						S	S	P	P	P	S	S
15	Optimiser l'infrastructure, les ressources et les capacités informatiques	PO3	AI3	DS3	DS7	DS9						S	P					
16	Réduire le nombre de défauts et de retraitements touchant la fourniture de solutions et de services	PO8	AI4	AI6	AI7	DS10						P	P		S	S		
17	Protéger l'atteinte des objectifs informatiques	PO9	DS10	SE2								P	P	S	S	S	S	S
18	Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et aux ressources informatiques	PO9										S	S	P	P	P	S	S
19	S'assurer que l'information critique et confidentielle n'est pas accessible à ceux qui ne doivent pas y accéder	PO6	DS5	DS11	DS12									P	P	S	S	S
20	S'assurer que les transactions métiers automatisées et les échanges d'informations sont fiables	PO6	AI7	DS5								P			P	S	S	
21	S'assurer que les services et l'infrastructure informatique peuvent résister/se rétablir convenablement en cas de panne due à une erreur, à une attaque délibérée ou à un sinistre	PO6	AI7	DS4	DS5	DS12	DS13	SE2				P	S		S	P		
22	S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'ait qu'un impact minimum sur l'activité	PO6	AI6	DS4	DS12							P	S		S	P		
23	S'assurer que les services informatiques sont disponibles dans les conditions requises	DS3	DS4	DS8	DS13							P	P			P		
24	Améliorer la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise	PO5	DS6									S	P					S
25	Livrer les projets en temps et dans les limites budgétaires en respectant les standards de qualité	PO8	PO10									P	P		S			S
26	Maintenir l'intégrité de l'information et de l'infrastructure de traitement	AI6	DS5									P	P		P	P		S
27	Assurer la conformité de l'informatique aux lois et règlements	DS11	SE2	SE3	SE4									S	S		P	S
28	S'assurer que l'informatique fait preuve d'une qualité de service efficiente en matière de coûts, d'amélioration continue et de capacité à s'adapter à des changements futurs	PO5	DS6	SE1	SE3							P	P					P

Page volontairement laissée blanche

OBJECTIFS INFORMATIQUES POUR CHAQUE PROCESSUS INFORMATIQUE

		1 Réagir aux exigences métier en accord avec la stratégie métier	2 Réagir aux exigences de la gouvernance en accord avec les orientations du CA	3 S'assurer de la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services	4 Optimiser l'utilisation de l'information	5 Donner de l'agilité à l'informatique	6 Déterminer comment traduire les exigences métier de fonctionnement et de contrôle en solutions automatisées efficaces et efficientes	7 Acquérir et maintenir fonctionnels des systèmes applicatifs intégrés et standardisés	8 Acquérir et maintenir opérationnelle une infrastructure informatique intégrée et standardisée	9 Se procurer et conserver les compétences nécessaires à la mise en œuvre de la stratégie informatique	10 S'assurer de la satisfaction réciproque dans les relations avec les tiers	11 Intégrer progressivement des solutions informatiques aux processus métier	12 S'assurer de la transparence et la bonne compréhension des coûts, bénéfices, stratégie, politiques et niveaux de services des SI	13 S'assurer d'une bonne utilisation et des bonnes performances des applications et des solutions informatiques	14 Protéger tous les actifs informatiques et en être comptable	15 Optimiser l'infrastructure, les ressources et les capacités informatiques	16 Réduire le nombre de défauts et de retraitements touchant la fourniture de solutions et de services	17 Protéger l'atteinte des objectifs informatiques	18 Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et aux ressources informatiques	19 S'assurer que l'information critique et confidentielle n'est pas accessible à ceux qui ne doivent pas y accéder	20 S'assurer que les transactions métier automatisées et les échanges d'informations sont fiables	21 S'assurer que les services et l'infrastructure informatique peuvent résister et se rétablir après une défaillance due à une erreur, à une attaque délibérée ou à un sinistre	22 S'assurer qu'un incident ou une modification dans la fourniture d'un service informatique n'ait qu'un impact minimum sur l'activité	23 S'assurer que les services informatiques sont disponibles dans les conditions requises	24 Améliorer la rentabilité de l'informatique et sa contribution à la profitabilité de l'entreprise	25 Livrer les projets en temps et dans les limites budgétaires en respectant les standards de qualité	26 Maintenir l'intégrité de l'information et de l'infrastructure de traitement	27 Assurer la conformité de l'informatique aux lois et réglements	28 S'assurer que l'informatique fait preuve d'une qualité de service, répondant aux exigences et besoins de l'utilisateur continue et de capacité à s'adapter à des changements futurs
PO1	Définir un plan informatique stratégique	✓	✓																											
PO2	Définir l'architecture de l'information	✓			✓	✓						✓																		
PO3	Déterminer l'orientation technologique							✓								✓														
PO4	Définir les processus, l'organisation et les relations de travail	✓	✓			✓																								
PO 5	Gérer les investissements informatiques												✓												✓					✓
PO6	Faire connaître les buts et les orientations du management												✓	✓						✓	✓	✓	✓							
PO7	Gérer les ressources humaines de l'informatique					✓				✓																				
PO8	Gérer la qualité			✓													✓									✓				
PO9	Évaluer et gérer les risques														✓			✓	✓											
PO10	Gérer les projets	✓	✓																							✓				
AI1	Trouver des solutions informatiques	✓					✓																							
AI2	Acquérir des applications et en assurer la maintenance						✓	✓																						
AI3	Acquérir une infrastructure technique et en assurer la maintenance					✓			✓							✓														
AI4	Faciliter le fonctionnement et l'utilisation			✓								✓		✓			✓													
AI5	Acquérir des ressources informatiques							✓	✓	✓															✓					
AI6	Gérer les changements	✓					✓										✓									✓				
AI7	Installer et valider les solutions et les modifications	✓										✓		✓			✓					✓	✓							
DS1	Définir et gérer les niveaux de services	✓		✓									✓																	
DS2	Gérer les services tiers			✓							✓		✓																	
DS3	Gérer la performance et la capacité	✓														✓									✓					
DS4	Assurer un service continu																						✓	✓	✓					
DS5	Assurer la sécurité des systèmes														✓						✓	✓	✓				✓			
DS6	Identifier et imputer les coûts												✓												✓					✓
DS7	Instruire et former les utilisateurs			✓										✓		✓														
DS8	Gérer le service d'assistance client et les incidents			✓										✓												✓				
DS9	Gérer la configuration														✓	✓														
DS10	Gérer les problèmes			✓													✓	✓												
DS11	Gérer les données				✓															✓								✓		
DS12	Gérer l'environnement physique														✓					✓			✓	✓						
DS13	Gérer l'exploitation			✓																			✓		✓					
SE1	Surveiller et évaluer la performance des SI	✓	✓										✓																	✓
SE2	Surveiller et évaluer le contrôle interne														✓			✓					✓						✓	
SE3	S'assurer de la conformité aux obligations externes																												✓	
SE4	Mettre en place une gouvernance des SI		✓										✓																✓	✓

ANNEXE I

ANNEXE II

RELATIONS DES PROCESSUS INFORMATIQUES AVEC LES DOMAINES DE LA GOUVERNANCE DES SI, LE COSO, LES RESSOURCES INFORMATIQUES COBIT ET LES CRITÈRES D'INFORMATION COBIT

Cette annexe met en regard les processus informatiques de COBIT et les cinq domaines de la gouvernance des SI, les composantes du COSO, les ressources informatiques et les critères d'information. Le tableau propose aussi un indicateur de l'importance relative (Haute, Moyenne, Basse) qui se base sur une évaluation comparative disponible sur COBIT Online. Cette grille montre sur une seule page et au niveau général comment le cadre de référence de COBIT fait référence aux exigences du COSO et de la gouvernance des SI, et montre les relations entre les processus informatiques et les critères d'information. P indique une relation primaire, S une relation secondaire. S'il n'y a ni P ni S, cela ne veut pas dire qu'il n'y a pas de relation, mais qu'elle est moins importante ou marginale. Ces valeurs se basent sur les résultats d'études et sur l'opinion d'experts, et ne sont que des indications. Les utilisateurs doivent décider quels sont les processus importants dans leur propre entreprise.

ANNEXE II

RELATIONS DES PROCESSUS INFORMATIQUES AVEC LES DOMAINES DE LA GOUVERNANCE DES SI, LE COSO, LES RESSOURCES INFORMATIQUES COBIT ET LES CRITÈRES D'INFORMATION COBIT

			Domaine de la gouvernance des SI					COSO					Ressources SI COBIT				Critères d'information COBIT						
		IMPORTANCE	Alignement stratégique	Apport de valeur	Gestion des ressources	Gestion des risques	Mesures de la performance	Environnement de contrôle	Evaluation des risques	Activités de contrôle	Information et communication	Surveillance	Applications	Informations	Infrastructures	Personnes	Efficacité	Efficience	Confidentialité	Intégrité	Disponibilité	Conformité	Fiabilité
Planifier et Organiser																							
PO1	Définir un plan informatique stratégique	H	P		S	S			P		S	S					P	S					
PO2	Définir l'architecture de l'information	B	P	S	P	S				P	P						S	P	S	P			
PO3	Déterminer l'orientation technologique	M	S	S	P	S			S	P	S						P	P					
PO4	Définir les processus, l'organisation et les relations de travail	B	S		P	P		P			S	S					P	P					
PO 5	Gérer les investissements informatiques	M	S	P	S		S		S	P							P	P					S
PO6	Faire connaître les buts et les orientations du management	M	P			P		P			P						P					S	
PO7	Gérer les ressources humaines de l'informatique	B	P		P	S	S	P			S						P	P					
PO8	Gérer la qualité	M	P	S		S		P		P	S	P					P	P		S			S
PO9	Évaluer et gérer les risques	H	P			P			P								S	S	P	P	P	S	S
PO10	Gérer les projets	H	P	S	S	S	S	S	S	P		S					P	P					
Acquérir et Implémenter																							
AI1	Trouver des solutions informatiques	M	P	P	S	S				P							P	S					
AI2	Acquérir des applications et en assurer la maintenance	M	P	P		S				P							P	P		S			S
AI3	Acquérir une infrastructure technique et en assurer la maintenance	B			P					P							S	P		S	S		
AI4	Faciliter le fonctionnement et l'utilisation	B	S	P	S	S				P	S						P	P		S	S	S	S
AI5	Acquérir des ressources informatiques	M		S	P					P							S	P				S	
AI6	Gérer les changements	H		P	S				S	P		S					P	P		P	P		S
AI7	Installer et valider les solutions et les modifications	M	S	P	S	S	S			P	S	S					P	S		S	S		
Délivrer et Supporter																							
DS1	Définir et gérer les niveaux de services	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2	Gérer les services tiers	B		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3	Gérer la performance et la capacité	B	S	S	P	S	S			P		S					P	P			S		
DS4	Assurer un service continu	M	S	P	S	P	S	S		P	S						P	S			P		
DS5	Assurer la sécurité des systèmes	H				P				P	S	S							P	P	S	S	S
DS6	Identifier et imputer les coûts	B		S	P		S			P								P					P
DS7	Instruire et former les utilisateurs	B	S	P		S		P			S						P	S					
DS8	Gérer le service d'assistance client et les incidents	B	S	P			S	S			P	P					P	P					
DS9	Gérer la configuration	M		P		S				P							P	S			S		S
DS10	Gérer les problèmes	M		P		S				P	S	S					P	P			S		
DS11	Gérer les données	H		P	P	P				P										P			P
DS12	Gérer l'environnement physique	B			S	P			S	P										P	P		
DS13	Gérer l'exploitation	B			P					P	S						P	P		S	S		
Surveiller et Evaluer																							
SE1	Surveiller et évaluer la performance des SI	H					P				S	P					P	P	S	S	S	S	S
SE2	Surveiller et évaluer le contrôle interne	M		P		P						P					P	P	S	S	S	S	S
SE3	S'assurer de la conformité aux obligations externes	H	P			P				P	S	S										P	S
SE4	Mettre en place une gouvernance des SI	H	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

Note La grille du COSO est basée sur le référentiel original COSO. Cette grille s'applique aussi en général à *l'Enterprise Risk Management-Integrated Framework*, publié ensuite par le COSO, qui élargit le contrôle interne, apportant un éclairage plus robuste et plus étendu sur le sujet plus large de la gestion du risque dans l'entreprise. Bien que COBIT ne soit pas conçu pour remplacer le référentiel de contrôle interne original du COSO (il l'intègre, en fait), les utilisateurs de COBIT peuvent choisir de se référer à ce référentiel de gestion du risque dans l'entreprise à la fois pour satisfaire leurs besoins de contrôle interne et pour évoluer vers un processus plus complet de gestion du risque.

Page volontairement laissée blanche

ANNEXE III

MODÈLE DE MATURITÉ POUR LE CONTRÔLE INTERNE

L'annexe III propose un modèle de maturité générique qui montre la situation de l'environnement de contrôle interne et ce qui existe comme contrôles internes dans une entreprise. Elle montre comment la gestion du contrôle interne, et la conscience du besoin de mettre en place de meilleurs contrôles internes, font typiquement progresser d'un niveau donné à un niveau optimisé. Ce modèle propose un guide général pour aider les utilisateurs de COBIT à juger de ce qui est nécessaire pour des contrôles internes efficaces de l'informatique et pour les aider à positionner leur entreprise par rapport au modèle de maturité.

MODÈLE DE MATURITÉ POUR LE CONTRÔLE INTERNE

Niveau de maturité	Situation de l'environnement de contrôle interne	Mise en place de contrôles internes
0 Inexistant	On ne reconnaît pas le besoin d'un contrôle interne. Le contrôle ne fait pas partie de la culture ou de la mission de l'entreprise. Il existe un risqué élevé de défaillances des contrôles et d'incidents.	On n'est pas décidé à évaluer le besoin d'un contrôle interne. On traite les incidents quand ils surviennent.
1 Initialisé, au cas par cas	On reconnaît en partie le besoin d'un contrôle interne. L'approche du risque et des exigences de contrôle se fait au cas par cas, est mal organisée, sans communication ni surveillance. On ne sait pas identifier les défaillances. Les employés ne sont pas conscients de leurs responsabilités.	On n'est pas conscient du besoin d'une évaluation de ce qui est nécessaire pour les contrôles de l'informatique. Lorsqu'on en fait, ce n'est qu'au cas par cas, à un niveau général et en réaction à des incidents sérieux. Les évaluations ne concernent que les incidents avérés.
2 Reproductible, mais intuitif	Les contrôles sont en place, mais ils ne sont pas documentés. Leur fonctionnement dépend des connaissances et des motivations d'individus particuliers. L'évaluation de l'efficacité n'est pas bien faite. Les contrôles ont de nombreuses faiblesses et on ne les utilise pas comme il faut ; les conséquences peuvent être graves. Les actions du management pour résoudre les problèmes du contrôle ne sont ni hiérarchisées ni logiques. Les employés ne sont pas toujours conscients de leurs responsabilités à l'égard du contrôle.	L'évaluation des besoins en contrôles n'a lieu que lorsqu'il est nécessaire de déterminer, pour certains processus informatiques particuliers, le niveau actuel de maturité des contrôles, la cible visée, et l'écart qui existe. On utilise une approche informelle d'atelier de travail, avec les responsables de l'informatique et l'équipe impliquée dans le processus pour définir une approche adéquate des contrôles pour ce processus, et pour convenir d'un plan d'action.
3 Défini	Les contrôles sont en place, et ils sont correctement documentés. On évalue périodiquement l'efficacité fonctionnelle et le nombre de problèmes n'est ni très élevé ni très bas. En revanche, le processus d'évaluation n'est pas documenté. Bien que le management soit capable de traiter couramment les problèmes de contrôle, certaines faiblesses persistent qui pourraient encore avoir de graves conséquences. Les employés sont conscients de leurs responsabilités à l'égard des contrôles.	On a identifié les processus informatiques critiques en fonction d'inducteurs de valeur et de risques. On fait une analyse détaillée pour déterminer les exigences de contrôle et les causes des carences, et pour trouver des possibilités d'amélioration. En plus d'ateliers organisés, on utilise des outils et on pratique des entretiens pour enrichir l'analyse et pour s'assurer que les processus d'évaluation et d'amélioration sont bien attribués à un propriétaire et que celui-ci les met en œuvre.
4 Géré et mesurable	Il existe un environnement de gestion du contrôle interne et du risque efficace. On fait fréquemment une évaluation documentée des contrôles. De nombreux contrôles sont automatisés et régulièrement examinés. Le management détecte la plupart des problèmes liés aux contrôles, mais ce n'est pas systématique. Il existe un suivi sérieux qui permet de traiter les faiblesses reconnues des contrôles. L'informatique est utilisée de façon limitée et tactique pour automatiser les contrôles.	L'aspect critique des processus informatiques est régulièrement déterminé avec le soutien et l'accord complets des propriétaires de processus métiers concernés. L'évaluation des exigences de contrôle se base sur la politique et sur le niveau de maturité de ces processus, selon une analyse complète et chiffrée qui implique les parties prenantes les plus concernées. On sait clairement qui a la responsabilité finale de ces évaluations et on vérifie qu'il l'assume. Les stratégies d'amélioration s'appuient sur des analyses de rentabilité. On vérifie constamment si la performance aboutit au résultat souhaité. On organise occasionnellement des revues de contrôles externes.
5 Optimisé	L'entreprise a un programme général risque/contrôle qui permet de résoudre les problèmes de façon efficace et continue. La gestion du contrôle et du risque est intégrée dans les pratiques de l'entreprise, assistée par une surveillance automatique en temps réel, et la responsabilité finale de la surveillance des contrôles, de la gestion des risques et du respect de la conformité est pleinement assumée. L'évaluation des contrôles est continue, basée sur des auto-évaluations et sur l'analyse des carences et des causes. Les employés s'impliquent activement dans l'amélioration des contrôles.	Les modifications métiers prennent en compte la dimension critique des processus informatiques et couvrent tous les besoins de réévaluation des capacités des contrôles des processus. Les propriétaires de processus informatiques effectuent régulièrement des auto-évaluations pour confirmer que les contrôles sont au bon niveau de maturité pour satisfaire les besoins métiers, et ils prennent en compte les attributs de maturité pour trouver comment rendre les contrôles plus efficients et plus efficaces. L'entreprise se compare aux bonnes pratiques externes et cherche des conseils à l'extérieur sur l'efficacité du contrôle interne. Pour les processus cruciaux, on fait des revues indépendantes pour apporter l'assurance raisonnable que les contrôles sont au niveau de maturité désiré et qu'ils fonctionnent selon les prévisons.

Page volontairement laissée blanche

ANNEXE IV

DOCUMENTS DE RÉFÉRENCE DE COBIT 4.1

ANNEXE IV – DOCUMENTS DE RÉFÉRENCE DE COBIT 4.1

Pour les activités de développement et de mise à jour précédentes de COBIT, une importante base de 40 standards internationaux détaillés relatifs à l'informatique, de référentiels, guides et meilleures pratiques a été utilisée pour garantir l'exhaustivité de COBIT dans son approche de tous les domaines de gouvernance et de contrôle des SI.

Comme COBIT s'intéresse à ce qui est nécessaire pour une gestion et un contrôle adéquat des SI, il se positionne au niveau général. Les standards et les meilleures pratiques informatiques décrivent cependant en détail comment gérer et contrôler les aspects spécifiques de l'informatique. COBIT agit comme intégrateur de ces différents guides en réunissant les objectifs clés dans un cadre de référence général qui fait ausi le lien avec les exigences de gouvernance et les exigences des métiers.

Pour cette mise à jour de COBIT (COBIT 4.1), six des standards, référentiels et pratiques les plus reconnus mondialement ont été pris en compte comme références majeures garantissant que la couverture, la cohérence et l'alignement soient les meilleurs possibles. Ce sont :

- COSO :
  Internal Control-Integrated Framework, 1994
  Enterprise Risk Mangement-Integrated Framework, 2004
- Office of Government Commerce (OGC®):
  IT Infrastructure Library® (ITIL®), 1999-2004
- International Organisation for Standardisation :
  ISO/IEC 27000
- Software Engineering Institute (SEI®) :
  SEI Capability Maturity Model (CMM®), 1993
  SEI Capability Maturity Model Integration (CMMI®), 2000
- Project Management Institute (PMI®) :
  A Guide to the Project Management Body of Knlowledge (PMBOK®), 2004
- Information Security Forum (ISF) :
  The Standard of Good Practice for Information Security, 2003

Des références complémentaires ont été utilisées pour COBIT 4.1 :

- *IT Control Objectives for Sarbanes-Oxley : The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*, IT Governance Institute, USA, 2006
- *CISA Review Manual*, ISACA, 2006

Page volontairement laissée blanche

ANNEXE V

CORRESPONDANCE ENTRE COBIT 3ÈME ÉDITION ET COBIT 4.1

ANNEXE V – CORRESPONDANCE ENTRE COBIT 3È ÉDITION ET COBIT 4.1

Modifications au niveau du Cadre de Référence

Les modifications majeures au cadre de référence de COBIT résultant de la mise à jour COBIT 4.0 sont les suivantes :

- Le domaine S est devenu SE, pour Surveiller et Évaluer.
- S3 et S4 étaient des processus d'audit et non des processus informatiques. On les a enlevés, puisqu'ils sont correctement traités par un certain nombre de standards d'audit informatique, mais on a fourni un certain nombre de références dans la mise à jour du cadre de référence pour souligner le besoin qu'a le management de disposer des fonctions d'assurance et de les utiliser.
- SE3 est le processus qui s'intéresse à la supervision réglementaire, laquelle était auparavant couverte par PO8.
- SE4 concerne le processus de supervision des SI par la gouvernance, ce qui correspond à l'ambition de COBIT d'être un référentiel de gouvernance des SI. En positionnant ce processus en dernier, on a voulu souligner que tous les autres processus précédents contribuent au but ultime qui consiste à mettre en place une gouvernance efficace des SI dans l'entreprise.
- Du fait que PO8 a été supprimé et pour conserver la numérotation de PO9 *Évaluer les risques* et de PO10 *Gérer les projets* comme dans COBIT 3e édition, PO8 devient maintenant *Gérer la qualité*, l'ancien processus PO11. Le domaine PO a donc désormais 10 processus au lieu de 11.
- Le domaine AI a nécessité deux modifications : l'ajout d'un processus achats et le besoin d'inclure dans AI5 les aspects de la gestion des versions Ces dernières modifications ont fait penser que ce processus devrait être le dernier du domaine AI, il est donc devenu AI7. Le créneau ainsi libéré en AI5 a été utilisé pour ajouter le nouveau processus achats. Le domaine AI a désormais 7 processus au lieu de 6.

COBIT 4.1 est une version incrémentale de COBIT 4.0 comprenant :

- Une amélioration de la partie Synthèse.
- Une présentation des objectifs et des métriques dans la partie Cadre de Référence.
- De meilleures définitions des concepts essentiels. Il est important de mentionner que la définition de l'objectif de contrôle a évoluée pour devenir davantage l'exposé d'une pratique de management.
- Une amélioration des objectifs de contrôle résultant d'une mise à jour des pratiques de contrôle et de la prise en compte de Val IT. Certains objectifs de contrôle ont été regroupés et/ou réécrits pour éviter les redondances et rendre la liste des objectifs de contrôle plus cohérente. Il en a résulté une renumérotation des objectifs de contrôle restants. Quelques objectifs de contrôle ont été réécrits afin de les rendre plus cohérents et davantage tournés vers l'action. Plus précisément :
  - AI5.5 et AI5.6 ont été regroupés avec AI5.4
  - AI 7.9, AI7.10 et AI7.11 ont été regroupés avec AI7.8
  - SE3 intègre désormais la conformité aux obligations contractuelles en plus des obligations légales et réglementaires.
- Les contrôles applicatifs ont été retravaillés afin de les rendre plus efficaces, pour aider à évaluer et rendre compte de l'efficacité des contrôles. Il en résulte une liste de six contrôles applicatifs au lieu des 18 de COBIT 4.0 avec des détails additionnels provenant des *Pratiques de Contrôle COBIT, 2ème version*.
- La liste des objectifs métiers et informatiques de l'Annexe I a été améliorée sur la base d'un nouveau regard résultant des travaux de recherche menés par l'Ecole de Management de Université d'Anvers (Belgique).
- Le hors texte a été enrichi. Il intègre une liste de référence rapide des processus COBIT et le diagramme de synthèse de description des domaines a été revu afin d'intégrer une référence aux contrôles de processus et aux contrôles applicatifs du Cadre de Référence COBIT.
- Les améliorations proposées par les utilisateurs de COBIT (COBIT 4.0 et COBIT Online) ont été revues et intégrées quand cela était opportun.

Objectifs de Contrôle

Comme on peut le comprendre d'après ce que nous venons d'expliquer sur les modifications au niveau du cadre de référence et sur le travail qui a permis de clarifier et de recentrer le contenu des objectifs de contrôle, la mise à jour du cadre de référence de COBIT a significativement modifié les objectifs de contrôle. Ces composants ont été réduits de 215 à 210, parce que tous les éléments génériques ne se retrouvent désormais plus qu'au niveau du cadre de référence et ils ne sont pas reproduits pour chaque processus. De même, toutes les références aux contrôles applicatifs ont migré vers le cadre de référence, et les objectifs de contrôle spécifiques ont été regroupés dans de nouvelles rubriques. Pour aider à faire la transition dans ce contexte, les deux ensembles de tableaux qui suivent établissent des références croisées entre les nouveaux objectifs de contrôle et les anciens.

Guide de Management

On a ajouté des entrées et des sorties pour illustrer ce dont les processus ont besoin (entrées) et ce qu'en principe on attend d'eux (sorties). On a aussi présenté les activités et les responsabilités qui y sont associées. Les entrées et les objectifs activité remplacent les facteurs critiques de succès de COBIT 3e édition. Les métriques sont désormais basées sur une déclinaison cohérente d'objectifs métiers, informatique, processus et activités. Les ensembles de métriques de COBIT 3e édition ont aussi été révisés et améliorés pour les rendre plus représentatifs et plus mesurables.

Références croisées : de COBIT 3e édition à COBIT 4.1

COBIT 3e édition	COBIT 4.1
PO1 Définir un plan informatique stratégique	
1.1 Intégration des TI au plan à long et à court terme de l'entreprise	1.4
1.2 Plan informatique à long terme	1.4
1.3 Approche et structure de la planification des TI à long terme	1.4
1.4 Modifications du plan informatique à long terme	1.4
1.5 Planification à court terme de la fonction informatique	1.5
1.6 Communication des plans informatiques	1.4
1.7 Surveillance et évaluation des plans informatiques	1.3
1.8 Évaluation des systèmes existants	1.3
PO2 Définir l'architecture de l'information	
2.1 Modèle d'architecture de l'information	2.1
2.2 Dictionnaire et règles de syntaxe des données de l'entreprise	2.2
2.3 Plan de classification des données	2.3
2.4 Niveaux de sécurité	2.3
PO3 Déterminer l'orientation technologique	
PO3 Déterminer l'orientation technologique	
3.1 Planification de l'infrastructure technologique	3.1
3.2 Surveillance des tendances et de la réglementation	3.3
3.3 Secours de l'infrastructure technologique	3.1
3.4 Plans d'acquisition du matériel et des logiciels	3.1, AI3.1
3.5 Normes technologiques	3.4, 3.5
PO2 Définir l'architecture de l'information	
2.1 Modèle d'architecture de l'information	2.1
2.2 Dictionnaire et règles de syntaxe des données de l'entreprise	2.2
2.3 Plan de classification des données	2.3
2.4 Niveaux de sécurité	2.3
PO3 Déterminer l'orientation technologique	
3.1 Planification de l'infrastructure technologique	3.1
3.2 Surveillance des tendances et de la réglementation	3.3
3.3 Secours de l'infrastructure technologique	3.1
3.4 Plans d'acquisition du matériel et des logiciels	3.1, AI3.1
3.5 Normes technologiques	3.4, 3.5
PO4 Définir l'organisation et les relations de travail	
4.1 Comité de planification ou de pilotage de la fonction informatique	4.3
4.2 Position de la fonction informatique au sein de l'entreprise	4.4
4.3 Révision des réalisations de la fonction	4.5
4.4 Rôles et responsabilités	4.6
4.5 Responsabilité de l'assurance qualité	4.7
4.6 Responsabilité de la sécurité physique et logique	4.8
4.7 Statuts de propriétaire et de gardien	4.9
4.8 Propriété des données et du système	4.9
4.9 Supervision	4.10
4.10 Séparation des tâches	4.11
4.11 Gestion du personnel informatique	4.12
4.12 Description des fonctions ou des postes du personnel de la fonction informatique	4.6
4.13 Personnel clé des TI	4.13
4.14 Procédures de gestion du personnel sous contrat	4.14
4.15 Relations de travail	4.15
PO5 Gérer l'investissement informatique	
5.1 Budget annuel de fonctionnement de la fonction informatique	5.3
5.2 Surveillance des coûts et des gains	5.4
5.3 Justification des coûts et des gains	1.1, 5.4, 5.5
PO6 Faire connaître les buts et orientations du management	
6.1 Dispositif de contrôle positif de l'information	6.1
6.2 Responsabilité du management vis-à-vis des politiques	6.3, 6.4, 6.5
6.3 Communication des politiques de l'entreprise	6.3, 6.4, 6.5
6.4 Ressources utilisées pour la mise en œuvre de la politique	6.4
6.5 Maintenance des politiques	6.3, 6.4
6.6 Conformité aux politiques, aux procédures et aux standards	6.3, 6.4, 6.5
6.7 Engagement vis-à-vis de la qualité	6.3, 6.4, 6.5
6.8 Cadre de sécurité et de contrôle interne	6.2
6.9 Droits relatifs à la propriété intellectuelle	6.3, 6.4, 6.5
6.10 Politiques spécifiques	6.3, 6.4, 6.5
6.11 Sensibilisation à la sécurité informatique	6.3, 6.4, 6.5
PO7 Gérer les ressources humaines	
7.1 Recrutement et promotion du personnel	7.1
7.2 Qualification du personnel	7.2
7.3 Rôles et responsabilités	7.4
7.4 Formation	7.5
7.5 Organisation des remplacements ou formations croisées	7.6
7.6 Procédures de sécurité concernant le personnel	7.7
7.7 Évaluation des performances	7.8
7.8 Gestion des changements de poste et des départs	7.8
PO8 Se conformer aux exigences externes	
8.1 Revue des impératifs externes	SE3.1
8.2 Pratiques et procédures pour se conformer aux exigences externes	SE3.2
8.3 Conformité en matière de sécurité et d'ergonomie	SE3.1
8.4 Vie privée, propriété intellectuelle et transfert de données	SE3.1
8.5 Commerce électronique	SE3.1
8.6 Conformité des contrats d'assurance	SE3.1
PO9 Évaluer les risques	
9.1 Évaluation du risque d'entreprise	9.1, 9.2, 9.4
9.2 Approche d'évaluation des risques	9.4
9.3 Identification des risques	9.3
9.4 Evaluation des risques	9.1, 9.2, 9.3, 9.4
9.5 Plan d'action pour parer aux risques	9.5
9.6 Acceptation des risques	9.5
9.7 Choix des mesures de sauvegarde	9.5
9.8 Engagement dans l'évaluation des risques	9.1
PO10 Gérer des projets	
10.1 Structure de gestion de projets	10.2
10.2 Participation du département utilisateur à l'initialisation du projet	10.4
10.3 Appartenance à l'équipe projet et responsabilités	10.8
10.4 Définition du projet	10.5
10.5 Approbation du projet	10.6
10.6 Approbation des phases du projet	10.6
10.7 Plan directeur du projet	10.7
10.8 Plan d'assurance qualité du système	10.10
10.9 Planification des méthodes d'assurance qualité	10.12
10.10 Gestion formelle des risques du projet	10.9
10.11 Plan de test	AI7.2
10.12 Plan de formation	AI7.1
10.13 Plan de révision après mise en œuvre	10.14 (partiel)
PO11 Gérer la qualité	
11.1 Plan général de qualité	8.5
11.2 Approche de l'assurance qualité	8.1
11.3 Planification de l'assurance qualité	8.1
11.4 Révision par l'assurance qualité du respect des normes et des procédures de la fonction informatique	8.1, 8.2
11.5 Méthodologie du cycle de vie de développement des systèmes	8.2, 8.3

COBIT 3e édition	COBIT 4.1
11.6 Méthodologie du cycle de vie de développement des systèmes lors de modifications majeures à effectuer sur la technologie existante	8.2, 8.3
11.7 Mise à jour de la méthodologie du cycle de vie de développement des systèmes	8.2, 8.3
11.8 Coordination et communication	8.2
11.9 Cadre d'acquisition et de maintenance de l'infrastructure technologique	8.2
11.10 Relations avec les tiers chargés du développement	DS2.3
11.11 Normes de documentation des programmes	AI4.2, AI4.3, AI4.4
11.12 Normes de test des programmes	AI7.2, AI7.4
11.13 Normes de test des systèmes	AI7.2, AI7.4
11.14 Test en parallèle/sur pilote	AI7.2, AI7.4
11.15 Documentation des tests	AI7.2, AI7.4
11.16 Assurance qualité et évaluation du respect des normes de développement	8.2
11.17 Assurance qualité et revue de l'atteinte des objectifs de la fonction informatique	8.2
11.18 Indicateurs de qualité	8.6
11.19 Comptes-rendus des revues d'assurance qualité	8.2

COBIT 3e édition	COBIT 4.1
AI1 Trouver des solutions informatiques	
1.1 Définition des besoins d'information	1.1
1.2 Formulation des solutions alternatives	1.3, 5.1, PO1.4
1.3 Formulation de la stratégie d'achat	1.3, 5.1, PO1.4
1.4 Exigences pour les services fournis par des tiers	5.1, 5.3
1.5 Étude de faisabilité technologique	1.3
1.6 Étude de faisabilité économique	1.3
1.7 Architecture de l'information	1.3
1.8 Rapport d'analyse des risques	1.2
1.9 Contrôles du rapport coût/efficacité de la sécurité	1.1, 1.2
1.10 Conception des pistes d'audit	1.1, 1.2
1.11 Ergonomie	1.1
1.12 Sélection du logiciel système	1.1, 1.3
1.13 Contrôle des achats	5.1
1.14 Acquisition de logiciels	5.1
1.15 Maintenance des logiciels par des tiers	5.4
1.16 Programmation d'applications sous contrat	5.4
1.17 Réception des équipements	5.4
1.18 Réception de technologie	3.1, 3.2, 3.3, 5.4
AI2 Acquérir des applications et en assurer la maintenance	
2.1 Méthodes de conception	2.1
2.2 Modifications majeures d'un système existant	2.1, 2.2, 2.6
2.3 Approbation de la conception	2.1
2.4 Définition des exigences en matière de fichiers et documentation	2.2
2.5 Spécifications des programmes	2.2
2.6 Conception de la collecte des données sources	2.2
2.7 Définition et documentation des exigences de saisie	2.2
2.8 Définition des interfaces	2.2
2.9 Interface homme - machine	2.2
2.10 Définition et documentation des exigences de traitement	2.2
2.11 Définition et documentation des exigences des sorties	2.2
2.12 Les contrôles	2.3, 2.4
2.13 La disponibilité : facteur clé de la conception	2.2
2.14 Dispositions pour préserver l'intégrité des applications	2.3, DS11.5
2.15 Tests des applications	2.8, 7.4
2.16 Manuels utilisateurs et matériels de support	4.3. 4.4
2.17 Réévaluation de la conception des systèmes	2.2
AI3 Acquérir une infrastructure technologique et en assurer la maintenance	
3.1 Évaluation des nouveaux matériels et logiciels	3.1, 3.2, 3.3
3.2 Maintenance préventive du matériel	DS13.5
3.3 Sécurité des logiciels systèmes	3.1, 3.2, 3.3
3.4 Installation des logiciels systèmes	3.1, 3.2, 3.3
3.5 Maintenance des logiciels systèmes	3.3
3.6 Contrôle des modifications des logiciels systèmes	6.1, 7.3
3.7 Utilisation et surveillance des utilitaires système	3.2, 3.3, DS9.3
AI4 Développer les procédures et en assurer la maintenance	
4.1 Besoins d'exploitation et niveaux de service	4.1
4.2 Manuel des procédures utilisateurs	4.2
4.3 Manuel d'exploitation	4.4
4.4 Supports de formation	4.3, 4.4
AI5 Installer les systèmes et les valider	
5.1 Formation	7.1
5.2 Évaluation des performances des logiciels d'application	7.6, DS3.1
5.3 Plan de mise en place	7.2, 7.3
5.4 Conversion du système	7.5
5.5 Conversion des données	7.5
5.6 Stratégie et plans de tests	7.2
5.7 Test des modifications	7.4, 7.6
5.8 Critères et performances des tests en parallèle/sur pilote	7.6
5.9 Tests de recette définitive	7.7
5.10 Tests de sécurité et validation	7.6
5.11 Tests d'exploitation	7.6
5.12 Transfert en production	7.8
5.13 Évaluation de l'adéquation de l'application aux besoins des utilisateurs	7.9
5,14 Revue par le management après mise en place	7.9
AI6 Gérer les changements	
6.1 Lancement et contrôle des demandes de modification	61, 6.4
6.2 Évaluation de l'impact	6.2
6.3 Contrôle des modifications	7.9
6.4 Modifications d'urgence	6.3
6.5 Documentation et procédures	6.5
6.6 Maintenance autorisée	DS5.3
6.7 Préparation de la diffusion des logiciels	7.9
6.8 Diffusion des logiciels	7.9

COBIT 3e édition	COBIT 41
DS1 Définir et gérer des niveaux de services	
1.1 Contrat de niveaux de services	1.1
1.2 Contenu des contrats de servivce	1.3
1.3 Procédures de fonctionnement	1.1
1.4 Surveillance et comptes-rendus	1.5
1.5 Revue des conventions de niveaux de services et des contrats	1.6
1.6 Charges facturables	1.3
1.7 Programme d'amélioration de service	1.6
DS 2 Gérer des services tiers	
2.1 Interfaces fournisseurs	2.1
2.2 Titulaire de la relation	2.2
2.3 Contrats avec des tiers	AI5.2
2.4 Qualification des tiers	AI5.3
2.5 Contrat d'externalisation	AI5.2
2.6 Continuité des services	2.3
2.7 Relations sécurité	2.3
2.8 Surveillance	2.4
DS3 Gérer la performance et la capacité	
3.1 Impératifs de disponibilité et de performance	3.1
3.2 Plan de disponibilité	3.4
3.3 Surveillance et comptes-rendus	3.5
3.4 Outils de modélisation	3.1
3.5 Gestion proactive de la performance	3.3

COBIT 4.1

COBIT 3e édition	COBIT 41
3.6 Prévisions de charge de travail	3.3
3.7 Gestion de la capacité des ressources	3.2
3.8 Disponibilité des ressources	3.4
3.9 Planification des ressources	3.4
DS4 Assurer un service continu	
4.1 Plan de continuité informatique	4.1
4.2 Plan de continuité informatique : stratégie et philosophie	4.1
4.3 Contenu du plan de continuité informatique	4.2
4.4 Minimiser les besoins de continuité informatique	4.3
4.5 Maintenance du plan de continuité informatique	4.4
4.6 Test du plan de continuité informatique	4.5
4.7 Formation au plan de continuité informatique	4.6
4.8 Diffusion du plan de continuité informatique	4.7
4.9 Procédures alternatives de traitement pour le secours des départements utilisateurs	4.8
4.10 Ressources informatiques critiques	4.3
4.11 Site et matériel de secours	4.8
4.12 Sauvegarde hors site	4.9
4.13 Procédures d'évaluation après sinistre	4.10
DS5 Assurer la sécurité des systèmes	
5.1 Gestion des mesures de sécurité	5.1
5.2 Identification, authentification et accès	5.3
5.3 Sécurité d'accès en ligne aux données	5.3
5.4 Gestion des comptes utilisateurs	5.4
5.5 Revue des comptes utilisateurs par le management	5.4
5.6 Contrôle des utilisateurs sur leurs comptes	5.4, 5.5
5.7 Surveillance de la sécurité	5.5
5.8 Classification des données	PO2.3
5.9 Gestion centralisée des identifiants et des droits d'accès	5.3
5.10 Rapports d'activité sur la sécurité et les violations de la sécurité	5.5
5.11 Gestion des incidents	5.6
5.12 Procédure de revalidation	5.1
5.13 Contrôle des contreparties	5.3, CA6
5.14 Autorisation des transactions	5.3
5.15 Non-répudiation	5.11
5.16 Chemin sécurisé	5.11
5.17 Protection des fonctions de sécurité	5.7
5.18 Gestion des clefs de chiffrement	5.8
5.19 Prévention, détection et correction des virus	5.9

COBIT 3e édition	COBIT 41
5.20 Architectures de pare-feu (firewall) et connexions aux réseaux publics	5.10
5.21 Protection des valeurs électroniques	13.4
DS6 Identifier et imputer les coûts	
6.1 Charges facturables	6.1
6.2 Procédures d'évaluation des coûts	6.3
6.3 Procédures d'imputation et de refacturation aux utilisateurs	6.2, 6.4
DS7 Instruire et former les utilisateurs	
7.1 Identification des besoins de formation	7.1
7.2 Organisation de la formation	7.2
7.3 Sensibilisation et formation aux règles de sécurité	PO7.4
DS8 Aider et conseiller les clients	
8.1 Assistance " help desk"	8.1, 8.5
8.2 Enregistrement des demandes des clients	8.2, 8.3, 8.4
8.3 Escalade des demandes des clients	8.3
8.4 Surveillance du traitement	10.3
8.5 Analyse des tendances et compte-rendu	10.1
DS9 Gérer la configuration	
9.1 Enregistrement de la configuration	9.1
9.2 Configuration de base	9.1
9.3 Situation comptable	9.3
9.4 Contrôle de configuration	9.3
9.5 Logiciels non autorisés	9.3
9.6 Stockage des logiciels	AI3.4
9.7 Procédures de gestion de la configuration	9.2
9.8 Responsabilité des logiciels	9.1, 9.2
DS10 Gérer les problèmes et les incidents	
10.1 Système de gestion des problèmes	10.1, 10.2, 10.3, 10.4
10.2 Escalade des problèmes	10.2
10.3 Suivi des problèmes et piste d'audit	8.2, 10.2
10.4 Autorisations d'accès temporaires ou en urgence	5.4, 12.3, AI6.3
10.5 Priorités des traitements d'urgence	10.1, 8.3
DS11 Gérer les données	
11.1 Procédures de préparation de données	CA1
11.2 Procédures d'autorisation des documents sources	CA1
11.3 Collecte des données des documents sources	CA1
11.4 Traitement des erreurs dans les documents sources	CA1
11.5 Conservation des documents sources	DS11.2
11.6 Procédures d'autorisation d'entrée de données	CA2
11.7 Contrôles d'exactitude, d'exhaustivité et d'autorisation	CA3
11.8 Traitement des erreurs de saisie de données	CA2, CA4
11.9 Intégrité du traitement des données	CA4
11.10 Validation et préparation du traitement des données	CA4

COBIT 3e édition	COBIT 41
11.11 Gestion des erreurs de traitement des données	CA4
11.12 Traitement et conservation des fichiers de sortie	CA5, 11.2
11.13 Distribution des sorties	CA5, CA6
11.14 Réconciliation et ajustage des sorties	CA5
11.15 Revue des sorties et traitement des erreurs	CA5
11.16 Clauses de sécurité des états en sortie	11.6
11.17 Protection des informations sensibles pendant la transmission et le transport	CA6, 11.6
11.18 Protection des informations sensibles mises à disposition	11.4, CA6
11.19 Gestion du stockage	11.2
11.20 Périodes de conservation et conditions de stockage	11.2
11.21 Système de gestion de la médiathèque	11.3
11.22 Responsabilités de la gestion de la médiathèque	11.3
11.23 Sauvegarde et restauration	11.5
11.24 Travaux de sauvegarde	11.4
11.25 Stockage des sauvegardes	4.9, 11.3
11.26 Archivage	11.2
11.27 Protection des messages sensibles	11.6
11.28 Authentification et intégrité	CA6
11.29 Intégrité des transactions électroniques	5.11
11.30 Intégrité permanente des données enregistrées	11.2
DS12 Gérer les installations	
12.1 Sécurité physique	12.1, 12.2
12.2 Discrétion du site informatique	12.1, 12.2
12.3 Accompagnement des visiteurs	12.3
12.4 Santé et sécurité du personnel	12.1,12.5, SE3.1
12.5 Protection contre les risques liés à l'environnement	12.4, 12.9
12.6 Continuité de l'alimentation électrique	12.5
DS13 Gérer l'exploitation	
13.1 Procédures d'exploitation et manuels d'instructions	13.1
13.2 Documentation du processus de démarrage du système et des autres tâches d'exploitation	13.1
13.3 Planification des travaux	13.2
13.4 Travaux non planifiés	13.2
13.5 Continuité des traitements	13.1
13.6 Journaux d'exploitation	13.1
13.7 Périphériques de sortie et supports particuliers de sauvegarde	13.4
13.8 Exploitation à distance	5.11

COBIT 3e édition	COBIT 4.1
S1 Surveiller les processus	
1.1 Collecter les données de contrôle	1.2
1.2 Évaluer les performances	1.4
1.3 Évaluer la satisfaction des clients de l'informatique	1.2
1.4 Rapports de gestion	1.5
S2 Évaluer l'adéquation du contrôle interne	
2.1 Surveillance du contrôle interne	2.2
2.2 Exploitation en temps opportun des contrôles internes	2.1
2.3 Rapports sur le niveau de contrôle interne	2.2, 2.3
2.4 Assurance sur l'efficacité de la sécurité et du contrôle interne	2.4
S3 Acquérir une assurance indépendante	
3.1 Certification / Validation indépendante de la sécurité et du contrôle interne des services informatiques	2.5, 4.7
3.2 Certification / Validation indépendante des services fournis par des prestataires	2.5, 4.7
3.3 Évaluation indépendante de l'efficacité de la fonction informatique	2.5, 4.7
3.4 Évaluation indépendante des tiers fournisseurs de services	2.5, 4.7
3.5 Assurance indépendante de conformité aux lois, à la réglementation et aux engagements contractuels	2.5, 4.7
3.6 Assurance indépendante de conformité aux lois, à la réglementation et aux engagements contractuels des tiers fournisseurs de services	2.5, 2.6, 4.7
3.7 Compétence de l'assurance indépendante	2.5, 4.7
3.8 Implication proactive de l'audit	2.5, 4.7
S4 Disposer d'un audit indépendant	
4.1 Charte d'audit	2.5, 4.7
4.2 Indépendance	2.5, 4.7
4.3 Éthique et normes professionnelles	2.5, 4.7
4.4 Compétence	2.5, 4.7
4.5 Planification	2.5, 4.7
4.6 Réalisation du travail d'audit	2.5, 4.7
4.7 Rapports d'audit	2.5, 4.7
4.8 Activités de suivi	2.5, 4.7

Références croisées : de COBIT 4.1 à COBIT 3e édition

COBIT 4.1	COBIT 3e édition
PO1 Définir un plan informatique stratégique	
1.1 Gestion de la valeur des SI	5.3
1.2 Alignement métiers-informatique	Nouveau
1.3 Évaluation de la performance actuelle	1.7, 1.8
1.4 Plan informatique stratégique	1.1, 1.2, 1.3, 1.4, 1.6, AI1.2, AI1.3
1.5 Plans informatiques tactiques	1.5
1.6 Gestion du portefeuille informatique	Nouveau
PO2 Définir l'architecture de l'information	
2.1 Modèle d'architecture de l'information de l'entreprise	2.1
2.2 Dictionnaire et règles de syntaxe des données de l'entreprise	2.2
2.3 Système de classification des données	2.3, 2.4, DS5.8
2.4 Gestion de l'intégrité	Nouveau
PO3 Déterminer l'orientation technologique	
3.1 Planification de l'orientation technologique	3.1, 3.3, 3.4
3.2 Planification de l'infrastructure technologique	Nouveau
3.3 Surveillance des tendances et de la réglementation.	3.2
3.4 Standards informatiques	3.5
3.5 Comité architecture des TI	3.5
PO4 Définir les processus,l'organisation et les relations de travail	
4.1 Ca dre de référence des processus informatiques	Nouveau
4.2 Comité stratégique informatique	Nouveau
4.3 Comité de pilotage informatique	4.1
4.4 Position de la fonction informatique au sein de l'entreprise	4.2
4.5 Structure du service informatique	4.3
4.6 Rôles et responsabilités	4.4, 4.12
4.7 Responsabilité de l'assurance qualité informatique	4.5
4.8 Responsabilité du risque, de la sécurité et de la conformité	4.6
4.9 Propriété des données et du système	4.7, 4.8
4.10 Supervision	4.9
4.11 Séparation des tâches	4.10
4.12 Recrutement informatique	4.11
4.13 Personnel informatique clél	4.13
4.14 Procédures de gestion du personnel sous contrat	4.14
4.15 Relations	4.15
PO5 Gérer l'investissement informatique	
5.1 Référentiel de gestion financière	Nouveau
5.2 Définition des priorités dans le budget informatique	Nouveau
5.3 Processus de budgétisation informatique	5.1, 5.3
5.4 Gestion des coûts	5.2, 5.3
5.5 Gestion des bénéfices	5.3
PO6 Faire connaître les buts et les orientations du management	
6.1 Politique informatique et environnement de contrôle	6.1
6.2 Risque informatique pour l'entrepriqe et cadre de contrôle interne	6. 8
6.3 Gestion des politiques informatiques	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.4 Déploiement des politiques	6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
6.5 Communication des objectifs et des orientations informatiques	6.2, 6.3, 6.5, 6.6, 6.7, 6.9, 6.10, 6.11
PO7 Gérer les ressources humaines informatiques	
7.1 Recrutement et maintien du personnel	7.1
7.2 Compétences du personnel	7.2
7.3 Affectation des rôles	Nouveau
7.4 Formation	7.3, DS7.3
7.5 Dépendance à l'égard d'individus	7.4
7.6 Procédures de sécurité concernant le personnel	75
7.7 Évaluation des performances	76
7.8 Gestion des changements de poste et des départs	7.7, 7.8
PO8 Gérer la qualité	
8.1 Système de gestion de la qualité	11.2, 11.3, 11.4
8.2 Standards informatiques et pratiques qualité	11.5, 11.6, 11.7, 11.8, 1.9, 11.10, 11.16, 11.17, 11.19
8.3 Standards de développement et d'acquisition	11.5, 11.6, 11.7
8.4 Orientation client	Nouveau
8.5 Amélioration continue	Nouveau
8.6 Mesure surveillance et revue qualité	11.18
PO9 Évaluer et gérer les risques	
9.1 Référentiel de gestion des risque informatiques	9.1, 9.4, 9.8
9.2 Établissement du contexte du risque	9.1, 9.4
9.3 Identification des événements	9.3, 9.4
9.4 Évaluation des risques	9.1, 9.2, 9.4
9.5 Réponse aux risques	9.5, 9.6, 9.7
9.6 Maintenance et surveillance d'un plan d'action vis-à-vis des risques	Nouveau
PO10 Gérer des projets	
10.1 Cadre de gestion de programme	Nouveau
10.2 Cadre de gestion de projet	10.1
10.3 Approche de la gestion de projets	Nouveau
10.4 Implication des parties prenantes	10.2
10.5 Énoncé du périmètre du projet	10.4
10.6 Démarrage d'une phase du projet	10.5, 10.6
10.7 Plan de projet intégré	10.7
10.8 Ressources du projet	10.3
10.9 Gestion des risques des projets	10.10
10.10 Plan qualité du projet	10.8
10.11 Contrôle des changements du projet	Nouveau
10.12 Planification des méthodes d'assurance	10.9
10.13 Métrique, reporting et surveillance de la performance du projet	Nouveau
10.14 Clôture du projet	10.13 (partiel)

COBIT 4.1	COBIT 3e édition
AI1 Trouver des solutions informatiques	
1.1 Définition et actualisation des exigences métiers, techniques et fonctionnelles	1.1, 1.9, 1.10, 1.11, 1.12
1.2 Rapport d'analyse des risques	1.8, 1.9, 1.10
1.3 Études de faisabilité et formulation d'alternatives	1.3, 1.7, 1.12
1.4 Décision et approbation concernant les exigences et la faisabilité	Nouveau
AI2 Acquérir des applications et en assurer la maintenance	
2.1 Conception générale	2.1, 2.2
2.2 Conception détaillée	2.2, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.13, 2.17
2.3 Contrôle applicatif et auditabilité	2.12, 2.14
2.4 Sécurité et disponibilité des applications	2.12
2.5 Configuration et implémentation des logiciels applicatifs acquis	Nouveau
2.6 Mises à jour majeures des systèmes existants	2.2
2.7 Développement d'applications	Nouveau
2.8Assurance qualité des logiciels	2.15
2.9 Gestion des exigences des applications	Nouveau
2.10 Maintenance des applications	Nouveau

COBIT 4.1	COBIT 3e édition
AI3 Acquérir une infrastructure technique et en assurer la maintenance	
3.1 Plan d'acquisition d'une infrastructure technique	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 Protection et disponibilité des ressources de l'infrastructure	1.18, 3.1, 3.3, 3.4, 3.7
3.3 Maintenance de l'infrastructure	1.18, 3.1, 3.3, 3.4, 3.5, 3.7
3.4 Environnement de test de faisabilité	Nouveau
AI4 Faciliter le fonctionnement et l'utilisation	
4.1 Planification pour rendre les solutions exploitables	4.1
4.2 Transfert de la connaissance au secteur métier	PO11.11, 4.2
4.3 Transfert des connaissances aux utilisateurs finaux	PO11.11, 2.16, 4.4
4.4 Transfert des connaissances vers le personnel d'exploitation et du support	PO11.11, 2.16, 4.3, 4.4
AI5 Acquérir des ressources informatiques	
5.1 Contrôle des achats	1.2, 1.3, 1.4, 1.13, 1.14
5.2 Gestion des contrats fournisseurs	DS2.3, DS2.5
5.3 Sélection des fournisseurs	1.4, DS2.4
5.4 Acquisition de ressources informatiques	1.15, 1.16, 1.17, 1.18
AI6 Gérer les changements	
6.1 Standards et procédures de changement	3.6, 6.1

COBIT 4.1	COBIT 3e édition
6.2 Évaluation de l'impact, choix des priorités et autorisation	6.2
6.3 Modifications d'urgence	DS10, 6.4
6.4 Suivi et compte-rendu des changements	6.1
6.5 Clôture et documentation des changements	6.5
AI7 Installer et valider les solutions et les modifications	
7.1 Formation	PO10.11, PO10.12, 5.1
7.2 Programme de test	PO10.11, PO11.12, PO11.13, PO11.14, PO11.15, 5.3, 5.6
7.3 Plan d'implémentation	3.6, 5.3
7.4 Environnement de tests	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 Conversion des systèmes et des données	5.4, 5.5
7.6 Test des modifications	5.2, 5.7, 5.8, 5.10, 5.11
7.7 Tests de recette définitive	5.9
7.8 Transfert en production	5.12
7.9 Revue post-démarrage	5.13, 5.14

COBIT 4.1	COBIT 3e édition
DS1 Définir et gérer les niveaux de services	
1.1 Référentiel pour la gestion des niveaux de services	1.1, 1.3
1.2 Définition des services	Nouveau
1.3 Contrats de services	1.2
1.4 Contrats d'exploitation	Nouveau
1.5 Surveillance et comptes-rendus des niveaux de services atteints	1.4
1.6 Revue des conventions de service et des contrats	1.5, 1.6
DS 2 Gérer les services tiers	
2.1 Identification des relations avec tous les fournisseurs	2.1
2.2 Gestion des relations fournisseurs	2.2
2.3 Gestion du risque fournisseurs	PO11.10, 2.6, 2.7
2.4 Surveillance des performances fournisseurs	2.8
DS3 Gérer la performance et la capacité	
3.1 Planification de la performance et de la capacité	AI5.2, 3.1, 3.4
3.2 Performance et capacité actuelles	3.7
3.3 Performance et capacité futures	3.5, 3.6
3.4 Disponibilité des ressources informatiques	3.2, 3.8, 3.9
3.5 Surveillance et comptes rendus	3.3
DS4 Assurer un service continu	
4.1 Référentiel de continuité informatique	4.1, 4.2

COBIT 4.1	COBIT 3e édition
4.2 Plans de continuité informatique	4.3
4.3 Ressources informatiques critiques	4.4, 4.10
4.4 Maintenance du plan de continuité des SI	4.5
4.5 Tests du plan de continuité des SI	4.6
4.6 Formation au plan de continuité des SI	4.7
4.7 Diffusion du plan de continuité des SI	4.8
4.8 Restauration et redémarrage des services informatiques	4.9, 4.11
4.9 Stockage de sauvegardes hors site	4.12, 11.25
4.10 Revue après redémarrage	4.13
DS5 Assurer la sécurité des systèmes	
5.1 Gestion de la sécurité informatique	5.1, 5.12
5.2 Plan de sécurité informatique	Nouveau
5.3 Gestion des identités	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 Gestion des comptes utilisateurs	5.4, 5.5, 5.6, 5.13, 10.4
5.5 Tests de sécurité, vigilance et surveillance	5.6, 5.7, 5.10
5.6 Définition des incidents de sécurité	5.11
5.7 Protection de la technologie de sécurité	5.17
5.8 Gestion des clefs de chiffrement	5.18

COBIT 4.1	COBIT 3e édition
5.9 Prévention, détection et neutralisation des logiciels malveillants	5.19
5.10 Sécurité des réseaux	5.20
5.11 Échange de données sensibles	5.15, 5.16, 11.29, 13.8
DS6 Identifier et imputer les coûts	
6.1 Définition des services	6.1
6.2 Comptabilité de l'informatique	6.3
6.3 Modèle de coûts et facturation	6.2
6.4 Maintenance du modèle de coûts	6.3
DS7 Instruire et former les utilisateurs	
7.1 Identification des besoins en savoir et en formation	7.1
7.2 Fourniture de formation et d'enseignement	7.2
7.3 Évaluation de la formation reçue	Nouveau
DS8 Gérer le service d'assistance client et les incidents	
8.1 Servie d'assistance client	8.1
8.2 Enregistrement des demandes des clients	8.2, 10.3
8.3 Escalade des incidents	8.2, 8.3, 10.5
8.4 Clôture des incidents	8.2
8.5 Analyse des tendances	8.1
DS9 Gérer la configuration	
9.1 Référentiel de configuration et configuration de base	9.1, 9.2, 9.8
9.2 Identification et maintenance des éléments de configuration	9.7, 9.8

COBIT 4.1

COBIT 4.1	COBIT 3e édition
9.3 Revue d'intégrité des configurations	9.3, 9.4, 9.5
DS10 Gérer les problèmes	
10.1 Identification et classification des problèmes	8.5, 10.1, 10.5
10.2 Suivi et résolution des problèmes	Nouveau
10.3 Clôture des problèmes	8.4, 10.1
10.4 Intégration des modifications, de la gestion des configurations et de la gestion des problèmes	Nouveau, 10.1
DS11 Gérer les données	
11.1 Exigences métiers pour la gestion des données	Nouveau
11.2 Dispositifs de stockage et de conservation	11.12, 11.19, 11.20, 11.26, 11.30
11.3 Système de gestion de la médiathèque	11.21, 11.22, 11.25
11.4 Mise au rebut	11.18, 11.24
11.5 Sauvegarde et restauration	AI2.14, 11.23
11.6 Exigences sécurité pour la gestion des données	11.16, 11.17, 11.27
DS 12 Gérer l'environnement physique	
12.1 Sélection du site et agencement	12.1, 12.2, 12.4
12.2 Mesures de sécurité physique	12.1, 12.2
12.3 Accès physique	10.4, 12.3
12.4 Protection contre les risques liés à l'environnement	12.5
12.5 Gestion des installations matérielles	12.4, 12.6, 12.9
DS 13 Gérer l'exploitation	
13.1 Procédures et instructions d'exploitation	13.1, 13.2, 13.5, 13.6
13.2 Planification des travaux	13.3, 13.4
13.3 Surveillance de l'infrastructure informatique	Nouveau
13.4 Documents sensibles et dispositifs de sortie	5.21, 13.7
13.5 Maintenance préventive du matériel	AI3.2

COBIT 4.1	COBIT 3e édition
SE1 Surveiller et évaluer la performance des SI	
1.1 Approche de la surveillance	1.0*
1.2 Définition et collationnement des données de surveillance	1.1, 1.3
1.3 Méthode de surveillance	Nouveau
1.4 Évaluation de la performance	1.2
1.5 Comptes-rendus destinés au CA et à la DG	1.4
1.6 Actions correctives	Nouveau
SE2 Surveiller et évaluer le contrôle interne	
2.1 Surveillance du référentiel de contrôle interne	2.0*
2.2 Revue générale	2.1, 2.3
2.3 Anomalies détectées par le contrôle	Nouveau
2.4 Auto-évaluation du contrôle	2.4
2.5 Assurance de contrôle interne	Nouveau
2.6 Contrôle interne des tiers	3.6
2.7 Actions correctives	Nouveau
SE3 Garantir la conformité aux obligations externes	
3.1 Identification des obligations externes de conformité : lois, règlements et contrats	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4
3.2 Optimisation de la réponse aux obligations externes	PO8.2
3.3 Évaluation de la conformité aux obligations	Nouveau
3.4 Assurance positive de la conformité	Nouveau
3.5 intégration des rapports	Nouveau
SE4 Mettre en place une gouvernance des SI	
4.1 Mise en place d'un cadre de gouvernance des SI	Nouveau
4.2 Alignement stratégique	Nouveau
4.3 Apport de valeur	Nouveau
4.4 Gestion des ressources	Nouveau
4.5 Gestion des risques	Nouveau
4.6 Mesure de la performance	Nouveau
4.7 Assurance indépendante	Nouveau

ANNEXE VI

APPROCHE RECHERCHE ET DÉVELOPPEMENT

ANNEXE VI – APPROCHE RECHERCHE ET DÉVELOPPEMENT

Le développement du contenu du référentiel COBIT est supervisé par le Comité de Pilotage COBIT, constitué de représentants internationaux d'entreprises, d'universités, du gouvernement et de professionnels de la gouvernance, de l'assurance, du contrôle et de la sécurité. Des groupes de travail internationaux ont été mis en place dans le but de réviser dans une perspective d'assurance qualité les versions intermédiaires du travail fait en recherche et développement. Le IT Governance Institute (ITGI) a supervisé l'ensemble du projet.

Éditions précédentes de COBIT

Définis dans le Cadre de Référence COBIT de la première édition, l'application des standards internationaux, des principes directeurs, et des meilleures pratiques mises à jour par les recherches ont conduit au développement des objectifs de contrôle. Le Guide d'Audit a ensuite été conçu pour vérifier si ces objectifs de contrôle étaient correctement mis en œuvre. Pour la 1ère et la 2ème édition, la recherche a porté entre autres sur le collationnement et l'analyse de sources internationales, et a été menée à bien par des équipes européennes (Free University of Amsterdam), américaines (California Polytechnic University) et australiennes (University of New South Wales). Les chercheurs ont été chargés de la compilation, de la révision, de l'évaluation et de l'incorporation adéquate des standards internationaux dans les domaines des techniques, des codes de conduite, de la qualité, des audits et des pratiques et exigences des entreprises, pour ce qui concerne le Cadre de Référence et les objectifs de contrôles individuels. Après collationnement et analyse, on a demandé aux chercheurs d'examiner chaque domaine et chaque processus en détail, et soit de suggérer des modifications des objectifs de contrôle soit d'en proposer de nouveaux pour chaque processus considéré. La synthèse des résultats a été réalisée par le Comité de Pilotage COBIT.

Le projet de la 3ème édition de COBIT a consisté à élaborer le Guide de Management et à actualiser la 2ème édition, en fonction de références internationales soit révisées, soit nouvelles. De plus le Cadre de Référence COBIT a été révisé et enrichi pour permettre un meilleur contrôle de gestion, pour introduire la gestion de performance, et pour développer davantage la gouvernance des SI. Pour fournir au management une application du Cadre de Référence et lui permettre ainsi de faire des choix pour la mise en place de contrôles et pour améliorer ses systèmes informatiques, ainsi que pour mesurer les performances, le Guide de Management inclut des Modèles de Maturité, des Facteurs Clés de Succès, des Indicateurs Clés d'Objectif, et des Indicateurs Clés de Performance, tous liés aux Objectifs de Contrôle.

Le Guide de Management a requis un panel mondial de 40 experts du monde universitaire, gouvernemental et des professions de la gouvernance, de l'assurance, du contrôle et de la sécurité informatiques. Ces experts se sont réunis en un atelier animé par des professionnels du travail de groupe qui utilisaient des principes de développement définis par le Comité de Pilotage de COBIT. L'atelier a été activement soutenu par le Gartner Group et par PricewaterhouseCoopers, qui ont non seulement fourni le leadership intellectuel, mais ont aussi envoyé plusieurs de leurs experts en contrôle, gestion de la performance, et sécurité de l'information. Les résultats de cet atelier furent les ébauches des modèles de maturité, des facteurs clés de succès, des indicateurs clés d'objectifs, et des indicateurs clés de performances pour chacun des 34 processus de COBIT. L'assurance qualité des premières livraisons fut conduite par le Comité de Pilotage de COBIT, et les résultats ont été proposés pour consultation sur le site Internet de l'ISACA. Le Guide de Management a été constitué pour offrir un nouvel ensemble d'outils orientés management, susceptibles de s'intégrer de façon cohérente au Cadre de Référence.

L'actualisation des Objectifs de Contrôle de la 3e édition de COBIT, basée sur de nouvelles références et des références internationales révisées, a été conduite par des membres des Chapitres de l'ISACA, sous la direction de membres du Comité de Pilotage de COBIT. L'intention n'était pas de réaliser une analyse globale de tous les matériaux, ni un nouveau développement des Objectifs de Contrôle, mais de fournir un processus d'actualisation incrémentiel. Les résultats du développement du Guide de Management furent alors utilisés pour réviser le Cadre de Référence COBIT, particulièrement les considérations, buts et exposés des facteurs favorisants pour les objectifs de contrôle généraux. La version originale en anglais de COBIT 3e édition a été publiée en juillet 2000, la version en français en 2002.

Dernières activités de mise à jour du projet

Dans son effort pour faire évoluer en permanence le corpus de connaissances de COBIT, le Comité de Pilotage a organisé un travail de recherche ces deux dernières années sur plusieurs aspects de COBIT. Ces projets de recherche concernent des composantes des Objectifs de Contrôle et du Guide de Management. Ci-dessous, la liste de certains domaines spécifiquement concernés :

Recherche sur les Objectifs de Contrôle

- Alignement de bas en haut de la gouvernance des SI COBIT
- Alignement de haut en bas de la gouvernance des SI COBIT
- COBIT et les autres standards détaillés : correspondances entre COBIT, ITIL, CMM, COSO, PMBOK, ISF, *Normes de bonnes pratiques pour la sécurité de l'information* et ISO 27000 pour permettre l'harmonisation du langage, des définitions et des concepts avec ces standards

Recherche sur le Guide de Management

- Analyse causale des relations ICO-ICP
- Revue de la qualité des ICO/ICP/Facteurs Clés de Succès d'après l'analyse causale des relations ICO-ICP, en répartissant les FCS entre "ce que vous avez besoin d'obtenir des autres" et "ce que vous avez besoin de faire vous-même"
- Analyse détaillée des concepts de métriques : Développement détaillé avec des experts pour améliorer les concepts de métriques, en construisant un schéma en cascade de métriques "processus-informatique-métiers" et en définissant des critères de qualité pour les métriques
- Établissement de liens entre objectifs métiers, objectifs informatiques et processus informatiques : Recherche approfondie dans huit professions différentes conduisant à une perception plus détaillée de la façon dont les processus COBIT favorisent la réalisation d'objectifs informatiques spécifiques et, par extension, d'objectifs métiers, puis généralisation des résultats
- Revue du contenu du modèle de maturité : Garantie de cohérence et de qualité des niveaux de maturité dans chaque processus et entre les divers processus, avec de meilleures définitions des attributs du modèle de maturité

Le Comité de Pilotage COBIT a été à l'origine de tous ces projets, il les a supervisés, tandis que la gestion et le suivi au jour le jour étaient pris en charge par une équipe constituée de quelques-uns des principaux responsables de COBIT. L'avancement de la plupart des projets de recherche mentionnés a fait lourdement appel aux compétences et au bénévolat de membres de l'ISACA, d'utilisateurs de COBIT, de conseillers experts et d'universitaires. Des groupes de développement locaux ont été constitués à Bruxelles, Londres, Chicago, Canberra, Cape Town, Washington DC et Copenhague, où de 5 à 10 utilisateurs de COBIT se réunissaient en moyenne deux ou trois fois par an pour travailler sur des recherches particulières ou à des tâches de révision assignées par les principaux responsables de COBIT. De plus certains projets de recherche particuliers ont été assignés à des écoles de commerce/gestion comme l'Antwerp Management School (DAMS) et l'University of Hawaii.

Les résultats de ces efforts de recherche, et le retour d'information apporté par les utilisateurs de COBIT au fil des ans et des difficultés rencontrées à l'occasion du développement de nouveaux produits comme les pratiques de contrôle, ont été intégrés au projet principal de COBIT pour mettre à jour et améliorer les Objectifs de Contrôle, le Guide de Management et le Cadre de Référence COBIT. Deux laboratoires de développement majeurs, comportant chacun plus de 40 experts de la gouvernance des SI, du management et du contrôle (patrons, consultants, universitaires et auditeurs) du monde entier ont été organisés pour passer en revue et mettre profondément à jour les contenus des Objectifs de Contrôle et du Guide de Management. D'autres groupes plus petits ont travaillé pour affiner et finaliser la production importante de ces instances majeures.

La version quasi définitive a été soumise à un processus de révision complet par une équipe d'environ 100 personnes. L'abondante moisson de commentaires a été analysée au cours d'un dernier atelier de révision du Comité de Pilotage COBIT.

Les résultats de ces ateliers ont été mis en forme par le Comité de Pilotage COBIT, par les principaux responsables de COBIT et par l'ITGI pour rédiger les nouveaux documents COBIT qu'on trouve dans ce volume. L'existence de COBIT Online® témoigne du fait que la technologie existe désormais pour tenir plus facilement à jour le contenu essentiel de COBIT, et cette ressource sera utilisée comme référentiel maître du contenu de COBIT. Il sera tenu à jour par les informations apportées par la base utilisateurs ainsi que par des revues du contenu de certains domaines spécifiques. Des publications périodiques (documents papier et électroniques) permettront de se référer hors ligne au contenu de COBIT.

.

Annexe VII

Glossaire

ANNEXE VII – GLOSSAIRE

Les termes anglais figurent entre parenthèses et en italique à la fin de chaque rubrique.

Activité – Principales actions entreprises pour activer le processus COBIT *(Activity)*

Analyse causale – Processus de diagnostic permettant de remonter à l'origine d'un événement et qui peut être utilisé pour apprendre des conséquences, typiquement des erreurs et des problèmes *(Root cause analysis)*

Approbateur – Dans le tableau RACI, fait référence à la personne ou au groupe qui a l'autorité pour approuver ou accepter la réalisation d'une activité *(Accountable)*

Architecture d'entreprise – Description de l'architecture fonctionnelle des composants fondamentaux des systèmes métiers ou un des éléments de ces systèmes (par ex. technologie), des relations entre eux et de la façon dont ils soutiennent les objectifs de l'entreprise *(Enterprise architecture)*

Architecture informatique de l'entreprise – Description de l'architecture technique des composants fondamentaux des systèmes métiers, des relations entre eux et de la façon dont ils soutiennent les objectifs de l'entreprise *(Enterprise architecture for IT)*

Architecture de l'information – Une des composantes de l'architecture des SI (avec l'architecture fonctionnelle et l'architecture technique). Voir Architecture des SI *(Information architecture)*

Architecture des SI – Cadre de référence intégré pour faire évoluer ou tenir à jour les technologies existantes et en acquérir de nouvelles pour atteindre les objectifs stratégiques et les objectifs métiers *(IT architecture)*

Authentification – Action de vérifier l'identité d'un utilisateur et son droit à accéder à l'information numérisée. Elle a pour but de protéger les systèmes contre des tentatives d'intrusion frauduleuses *(Authentication)*

Bonnes pratiques – Activité ou processus qui a fait ses preuves et est appliqué avec succès par de nombreuses entreprises *(Best practice)*

Cadre (référentiel) de contrôle – Ensemble de contrôles fondamentaux destiné à aider les propriétaires de processus métiers à s'acquiter de leur responsabilité de prévenir les pertes financières ou d'information pour l'entreprise *(Control framework)*

Capacité – Le fait de disposer des caractéristiques nécessaires pour fonctionner et/ou accomplir les tâches prévues *(Capability)*

CE – Contrat d'Exploitation. Accord interne sur la fourniture de services relatif à la fourniture de services par l'informatique. *(OLA, Operational Level Agreement)*

Charte d'Audit – Document définissant le but, l'autorité et la responsabilité de l'activité d'audit interne approuvée par le CA *(Audit charter)*

Client – Personne ou entité interne ou externe destinataire de services informatiques de l'entreprise *(Customer)*

Comité informatique stratégique – Comité constitué au niveau du CA pour faire en sorte que les administrateurs s'impliquent dans les questions/décisions majeures qui concernent l'informatique. Le comité est principalement responsable de la gestion des portefeuilles d'investissements, de services et d'autres ressources informatiques. Le comité est le propriétaire de ces portefeuilles *(IT strategy committee)*

Consulté – Dans le tableau RACI, fait référence aux personnes dont l'avis sur une activité est recherché (communication montante et descendante) *(Consulted)*

Continuité – Prévention, réduction des interruptions et restauration du service. On peut aussi utiliser dans ce contexte les expressions "plan de reprise d'activité", "plan de restauration après sinistre" et "plan de secours" ; elles s'intéressent toutes à la restauration de la continuité *(Continuity)*

Contrôle d'accès – Processus qui limite et contrôle l'accès aux ressources d'un système informatique ; contrôle logique ou physique conçu pour protéger contre un accès ou une utilisation non autorisés *(Access control)*

Contrôle applicatif – Ensemble de contrôles intégrés à des solutions automatisées (applications) *(Application control)*

Contrôle de détection – Contrôle utilisé pour identifier des événements (indésirables ou pas), des erreurs et d'autres circonstances dont une entreprise pense qu'ils ont un impact matériel sur un processus ou sur un produit final *(Detective control)*

Contrôles généraux informatiques – Contrôles autres que les contrôles applicatifs relatifs à l'environnement informatique de développement, de maintenance et d'exploitation des applications, utilisé par toutes les applications. Les objectifs des contrôles généraux sont de s'assurer d'un développement et d'une implémentation corrects des applications, de l'intégrité des programmes, des données et des traitements. Comme les contrôles applicatifs, les contrôles généraux sont soit manuels soit programmés. Ils intègrent à titre d'exemples l'élaboration et la mise en oeuvre de la stratégie informatique, de la politique de sécurité des SI, de l'organisation des équipes informatiques pour assurer la séparation des tâches, du plan de secours et de reprise d'activité *(General computer control)*

Contrôle interne – Politiques, procédures, pratiques et structures organisationnelles conçues pour fournir une assurance raisonnable que les objectifs métiers seront atteints et que les événements indésirables seront prévenus ou détectés et corrigés *(Internal control)*

Contrôle préventif – Contrôle interne utilisé pour prévenir des événements, des erreurs et d'autres circonstances dont une entreprise pense qu'ils peuvent avoir un impact matériel négatif sur un processus ou sur un produit final *(Preventive control)*

Contrôle programmé – Ensemble de contrôles intégrés aux solutions automatisées (applications) *(Automated application control)*

COSO – Committee of Sponsoring Organisations of the Treadway Commission. Son rapport de 1992 intitulé *Référentiel intégré de contrôle interne* est une norme de gouvernance d'entreprise reconnue internationalement. Voir www.coso.org

Coût total de possession – En informatique comprend : le coût initial des serveurs et logiciels, les mises à jour du materiel et du logiciel, la maintenance, le support technique, la formation, certaines activités assures par les utilisateurs *(TCO - Total Cost of Ownership)*

CS - Contrat ou convention de services – Accord de préférence documenté entre un fournisseur de services et le client/utilisateur qui définit les niveaux convenus pour un service et la façon dont ils sont mesurés *(SLA, Service level agreement)*

Cycle de vie de développement des systèmes – Phases successives du développement ou de l'acquisition d'un système logiciel. Typiquement comprend étude de faisabilité, étude des besoins, définition des besoins, conception détaillée, programmation, tests, mise en place et revue après mise en œuvre. Ne comprend ni la délivrance du service ni les bénéfices attendus de la réalisation des activités *(SDLC, Systems development life cycle)*

DF – Directeur financier, le premier responsable de la gestion des risques financiers d'une entreprise *(CFO)*

DG – Directeur général, le rang le plus élevé dans une entreprise *(CEO)*

Dictionnaire de données – Base de données renfermant nom, type, valeurs min. et max., source et autorisation d'accès pour chaque donnée de la base. Elle indique également quel programme applicatif utilise cette donnée de façon à ce que lorsqu'on envisage de manipuler une donnée on puisse générer une liste des programmes concernés. Le dictionnaire de données est soit un système d'information autonome utilisé à des fins de gestion et de documentation, soit un gestionnaire d'exploitation de base de données *(Data dictionary)*

Domaine – Pour COBIT, regroupement d'objectifs de contrôle en étapes logiques dans le cycle de vie des actifs de l'informatique (Planifier et Organiser, Acquérir et Implémenter, Délivrer et Supporter, Surveiller et Evaluer *(Domain)*

DSI ou DI– Directeur des Systèmes d'Information ou Directeur Informatique, le responsable de l'informatique d'une entreprise. Le DSI assure parfois le rôle de Responsable de la Connaissance (Chief Knowledge Officer - CKO) qui distribue la connaissance et pas seulement l'information. Voir également Directeur des Technologies *(CIO)*

DT– Directeur des Technologies, a en charge les aspects techniques de l'entreprise. Le titre de DT est souvent synonyme de DSI *(CTO)*

Élément de configuration – Composant d'une infrastructure ou un élément comme une demande de modification, associé à une infrastructure, qui est (ou doit être) sous le contrôle de la gestion de la configuration. Ces éléments peuvent différer largement en complexité, taille et type, allant d'un système complet (matériel, logiciel et documentation) à un simple module ou à un composant matériel mineur *(Configuration item)*

Entreprise – Groupe de personnes travaillant ensemble dans un but commun, typiquement dans le contexte d'une organisation, d'une société, d'une agence gouvernementale, d'une association ou d'une fondation *(Enterprise)*

FCS – Facteur Clé de Succès, correspond pour le management aux aspects ou aux actions les plus importantes pour réussir à mettre sous contrôle ses processus informatiques *(CSF)*

Fournisseur de services – Entité externe qui fournit des services à l'entreprise *(Service provider)*

Gestion de la configuration – Contrôle des modifications apportées à un ensemble d'éléments de configuration au cours du cycle de vie d'un système *(Configuration management)*

Gestion de la performance – En informatique, capacité à gérer tout type de mesure, y compris celles qui concernent les employés, les équipes, les processus, les opérations et les finances. Ce terme évoque des contrôles en boucle et un suivi régulier des mesures *(Performance management)*

Gouvernance de l'entreprise – Ensemble des responsabilités et pratiques assurées par le conseil d'administration et la direction générale dont le but est de fixer la stratégie, s'assurer que les objectifs sont atteints, que les risques sont gérés correctement et de vérifier que les ressources de l'entreprise sont utilisées à bon escient *(Enterprise governance)*

Guide – Description d'une manière particulière d'accomplir quelque chose ; moins rigide qu'une procédure *(Guideline)*

ICO – Indicateur Clé d'Objectif ; indicateurs qui informent le management a posteriori si un processus informatique a répondu aux exigences metier. Il s'exprime habituellement en termes de critères liés à l'information *(KGI -Key Goal Indicator)*

ICP – Indicateur Clé de Performance ; indicateurs qui déterminent à quel point la performance du processus infomatique lui donne des chances d'atteindre l'objectif. Ce sont des indicateurs essentiels pour savoir si un objectif a des chances d'être atteint ou non, et de bons indicateurs des capacités, des pratiques et des compétences. Ils mesurent les objectifs de l'activité, à savoir les actions que le propriétaire du processus doit entreprendre pour que la performance du processus soit bonne *(KPI - Key Performance Indicator)*

Incident informatique – Tout événement qui ne fait pas partie du fonctionnement normal d'un service et qui cause, ou peut causer, une interruption ou une réduction de la qualité de ce service *(IT Incident,* définition conforme à l'*IT Infrastructure Library, ITIL)*

Inducteurs de performance – Mesures considérées comme les inducteurs des indicateurs a posteriori. Ils peuvent être mesurés avant la manifestation du résultat et correspondent à des indicateurs a priori. Il y a une relation présupposée entre les deux qui suggère qu'une meilleure performance d'un indicateur a priori induit une meilleure performance de l'indicateur a posteriori. On les désigne aussi ICP (Iindicateur Clé de Performance) et on les utilise pour mesurer si les objectifs ont des chances d'être atteints *(Performance drivers)*

Informé – Dans le tableau RACI, fait référence aux personnes qui sont tenues au courant du progrès d'une activité (communication descendante) *(Informed)*

ISO 17799 – Norme internationale de définition des contrôles de confidentialité, intégrité et disponibilité de l'information

ISO 27001 – *Management de la sécurité de l'information - Guide d'utilisation* ; remplace la norme BS7799-2. Fournit les bases de l'audit externe de certification et est harmonisée avec les autres normes de gestion telles que ISO/IEC 9001 : 2000 et ISO 14001

ISO 9001 : 2000 – Code de bonnes pratiques pour la gestion de la qualité ISO 9001:2000 spécifie les exigences d'un système de gestion de la qualité pour toute organisation qui a besoin de démontrer sa capacité à fournir régulièrement des produits ou des services conformes à des objectifs particulier de qualité

ITIL – IT Infrastructure Library, de l'UK Office of Government Commerce (OGC). Ensemble de guides de management et de principes de fonctionnement des services informatiques.

Maturité – Au niveau métier, indique le degré de fiabilité ou de dépendance d'un processus auquel le métier peut se fier pour atteindre les objectifs souhaités *(Maturity)*

Mesure ou indicateur – Norme d'évaluation et de communication d'un résultat obtenu par rapport à résultat attendu. Les mesures ou indicateurs sont en règle générale quantitatives et s'expriment en nombre, devise (unité monétaire), pourcentage, etc. mais peuvent aussi s'exprimer de façon qualitative comme par exemple un niveau de satisfaction client. Rendre compte et surveiller les mesures ou indicateurs aide l'entreprise à jauger la mise en œuvre réelle de sa stratégie *(Measure)*

Mesures de résultats – Mesures des conséquences d'actions prises souvent désignées par indicateurs a posteriori. Elles s'intéressent souvent aux résultats obtenus à l'issue d'une période de temps déterminé et caractérise une performance historique. On les désigne également ICO (Indicateur Clé d'Objectif) et on les utilise pour indiquer si les objectifs ont été atteints. Elles ne peuvent être mesurées qu'après le résultat et pour cette raison sont appelées indicateurs a posteriori *(Outcome measures)*

Métrique – Instrument de mesure spécifique d'évaluation quantitative et périodique de la performance. Une métrique complète précise l'unité utilisée, la fréquence, la cible à atteindre, la procédure de mesure et la procédure d'interprétation du résultat *(Metric)*

Modèle de Maturité de la Capacité (MMC) – Le Modèle de maturité de la capacité des logiciels, du *Software Engineering Institute (SEI)*, est un modèle utilisé par de nombreuses organisations pour identifier les meilleures pratiques utiles pour évaluer et améliorer la maturité de leurs processus de développement de logiciels *(CMM)*

Objectif de contrôle – Exposé du résultat désiré ou du but à atteindre par la mise en œuvre de procédures de contrôle pour un processus donné *(Control Objective)*

Organisation – Façon dont une entreprise est structurée *(Organisation)*

Performance – En informatique, mise en place effective ou exécution d'un processus *(Performance)*

Plan d'infrastructure technologique – Plan pour les technologies, les ressources humaines et les installations qui permet le traitement et l'utilisation des applications actuelles et à venir *(Technology infrastructure plan)*

Plan stratégique informatique – Plan à long terme, c.-à-d. 3 à 5 ans, dans lequel les directions métiers et informatique coopèrent pour décrire comment les ressources informatique contribueront aux objectifs stratégiques de l'entreprise *(IT strategic plan)*

Plan tactique informatique – Plan à moyen terme, c.-à-d. 6 à 18 mois, qui convertit les orientations du plan stratégique informatique en initiatives requises et en exigences en ressources, et qui précise comment les ressources et les bénéfices seront surveillés et gérés *(IT tactical plan)*

PMBOK – Project Management Body of Knowledge, standard de gestion de projets développé par le Project Management Institute (PMI)

PMO – Chef du bureau projet, responsable de la mise en œuvre de dispositions définies pour aider à la gestion des projets et faire progresser la gestion de projet *(Project management officer)*

Politique – En général, document qui décrit un principe général ou des actions à entreprendre sur lesquelles on s'est accordé. Le but d'une politique est d'influencer et de guider la prise de décision actuelle et future pour qu'elle soit conforme à la philosophie, aux objectifs et aux plans stratégiques établis par les équipes décisionnaires de l'entreprise. Outre leur contenu, les politiques doivent exposer les conséquences d'actions qui ne s'y conforment pas, les moyens pour traites les anomalies, et la façon dont la conformité sera vérifiée et mesurée *(Policy)*

Portefeuille – Groupe de programmes, de projets, de services ou d'actifs sélectionnés, gérés et surveillés pour optimiser le bénéfice pour les métiers *(Portfolio)*

Pratique de contrôle – Mécanisme de contrôle clé qui aide à atteindre les objectifs de contrôle grâce à l'utilisation responsable des ressources, à la bonne gestion des risques et à l'alignement des SI sur les métiers *(Control practice)*

Pratiques clés de management – Pratiques de gestion nécessaires à la bonne exécution des processus des métiers *(Key management practices)*

PRINCE2 –Projects in a Controlled Environment, développé par l'OGC. Méthode de gestion de projets qui s'intéresse à la gestion, au contrôle et à l'organisation d'un projet

Problème – En informatique, cause à la base d'un ou plusieurs incidents *(Problem)*

Procédure – Document décrivant et précisant les étapes à suivre pour réaliser une activité. Les procédures font partie des processus *(Procedure)*

Processus – En général, ensemble de procédures influencées par les politiques et par les standards de l'entreprise ; il prend ses données (entrées) à différentes sources, y compris à d'autres processus, il traite les entrées et produit pour ses clients des sorties, qui peuvent être d'autres processus. Les processus ont de claires raisons "métiers" d'exister, ils sont dotés de propriétaires responsables en dernier ressort, de rôles et de responsabilités pour leur exécution, et de moyens pour mesurer leur performance *(Process)*

Processus métier – Voir processus *(Business process)*.

Programme – Regroupement structuré de projets interdépendants qui comporte l'ensemble des activités requises (à la fois nécessaires et suffisantes) pour atteindre un résultat métier clairement spécifié et qui impliquent les métiers, certains processus, certaines personnes, et certains moyens informatiques et organisationnels *(Programme)*

Programme applicatif, application – Programme qui traite les données métiers au travers d'activités telles que la saisie ou l'entrée de données, la mise à jour ou la requête. Il se distingue des programmes système comme le système d'exploitation ou le programme de contrôle du réseau et des programmes utilitaires comme copier ou trier *(Application program)*

Projet – Ensemble d'activités structurées axées sur la fourniture à l'entreprise d'une capacité définie (nécessaire mais pas suffisante pour atteindre un résultat métier donné) et dotées d'un planning et d'un budget convenus *(Project)*.

Propriétaires de données – Personnes, en général responsables ou chefs de services, qui ont la responsabilité de l'intégrité, de l'exactitude et de l'utilisation des données informatisées *(Data owners)*

SGQ – Système de Gestion de la Qualité. Système qui précise les politiques et les procédures nécessaires pour améliorer et contrôler les divers processus qui conduiront finalement à une amélioration de la performance des métiers. *(Quality Management System)*

Référentiel – Voir Cadre (référentiel) de contrôle *(Framework)*

Résilience ou Résistance aux pannes – Dans l'entreprise, capacité d'un système ou d'un réseau à se rétablir automatiquement après toute perturbation, en général avec le minimum d'effets identifiables *(Resilience)*

Responsable – Dans le tableau RACI, fait référence à la personne qui doit s'assurer que les activités sont réalisées correctement *(Responsible)*

Risque – Dans l'entreprise, potentialité d'une menace donnée à exploiter les points faibles d'un actif ou d'un groupe d'actifs pour provoquer des pertes et/ou des dommages à ces actifs. Il se mesure en général par une combinaison de conséquences et de probabilités d'occurrence *(Risk)*

Schéma de classification des données – Schéma général de classement des données de l'entreprise selon des facteurs comme la criticité, la sensibilité et la propriété *(Data classification scheme)*

Séparation des tâches – Contrôle interne de base qui prévient et détecte les erreurs et les irrégularités de séparation des individus en attribuant à des personnes différentes la responsabilité d'initier et d'enregistrer les traitements et celle de veiller sur les actifs. Communément pratiquée dans les grandes DSI afin que personne ne puisse introduire un code malveillant ou frauduleux sans détection *(Segregation/separation of duties)*

Service d'assistance (client) – Le seul point de contact entre l'informatique et les utilisateurs de services informatiques *(Service desk)*

Standard ou Norme – Pratique métier ou produit informatique qui constitue une pratique acceptée confirmée par l'entreprise ou par l'équipe de direction des SI. Les standards ou normes peuvent être mis en place pour soutenir une politique ou un processus, ou comme réponse à un besoin opérationnel. Comme les politiques, les standards ou normes doivent comporter une description de la manière dont on détectera la non conformité. *(Standard)*

SI ou Informatique – Système d'information, Informatique voire Technologies de l'information. Intègre le matériel, le logiciel, les réseaux et toute les autres installations nécessaires à l'entrée, au stockage, au traitement, à la transmission et à la sortie des données sous toutes leurs formes *(IT)*

Tableau de bord – Outil qui permet de représenter les attentes d'une entreprise à chaque niveau et de vérifier en permanence la situation de la performance par rapport à la cible visée *(Dashboard)*

Tableau de bord des investissements informatiques – Outil de mesure des attentes de l'entreprise et de surveillance continue des résultats par rapport aux objectifs des dépenses et des retours sur investissements des projets à composantes informatiques en termes de valeur pour les métiers *(IT investment dashboard)*

Tableau de bord équilibré – Méthode pour mesurer les actions d'une entreprise en rapport avec sa vision et ses stratégies en donnant au management un aperçu rapide et complet de la performance de son activité professionnelle. C'est un outil de gestion qui cherche à mesurer l'activité de l'entreprise selon les perspectives suivantes : financière, client, métier et acquisition de connaissances. (Robert S. Kaplan and David Norton, 1992) *(Balanced scorecard)*

Tableau RACI – identifie qui est Responsable, Approuve, est Consulté et/ou Informé au sein de l'entreprise *(RACI chart)*

Tests comparatifs – Processus utilisé en management, particulièrement en management stratégique, au cours duquel les entreprises évaluent divers aspects de leurs processus métiers par rapport aux meilleures pratiques constatées en général dans leur propre branche *(Benchmarking)*

Utilisateur informatique – Personne qui utilise l'informatique pour réaliser ou atteindre un objectif métier *(IT User)*

Page volontairement laissée blanche

ANNEXE VIII

COBIT ET PRODUITS DE LA FAMILLE COBIT

ANNEXE VIII – COBIT ET PRODUITS DE LA FAMILLE COBIT

Le référentiel COBIT dans sa version 4 et suivantes comprend :

- Le cadre de référence - explique comment COBIT structure les objectifs de la gouvernance des SI, les objectifs de contrôle et les bonnes pratiques, par domaine informatique et par processus, et les relie aux exigences métiers
- La description des processus - comprend 34 processus informatiques couvrant toutes les domaines de responsabilité de l'informatique de A à Z
- Les objectifs de contrôle - décrivent sous forme de bonnes pratiques génériques les objectifs de gestion des processus informatiques
- Le guide de management - propose des outils pour aider à répartir les responsabilités, mesurer la performance, tester par comparaison la capacité et à trouver des réponses aux insuffisances dans ce domaine
- Les modèles de maturité - apportent différents profils de processus par la description de différents états possibles actuels et futurs.

Depuis sa création, le contenu de base de COBIT n'a cessé d'évoluer au fil des ans et le nombre de produits dérivés de COBIT n'a cessé d'augmenter. Les publications dérivées de COBIT sont aujourd'hui les suivantes :

- *Conseils aux dirigeants d'entreprises pour la gouvernance des SI, 2e édition* - ce document aide les dirigeants à comprendre l'importance de la gouvernance des SI, quels sont ses enjeux et quel est leur rôle dans sa mise en œuvre
- COBIT Online - permet de personnaliser COBIT afin de l'adapter à son entreprise, d'enregistrer et de modifier les versions à volonté. Les services en ligne comprennent la réalisation d'études en temps réel, une foire aux questions, des tests comparatifs et un forum permettant de poser des questions et de partager des expériences
- *Pratiques de contrôle COBIT : Recommandations pour atteindre les objectifs de contrôle et réussir la gouvernance des SI, 2ème édition* - recommandations pour limiter les risques et accroître la valeur grâce à la mise en oeuvre d'objectifs de contrôle et indications pour les mettre en place. Il est vivement recommandé d'utiliser les Pratiques de contrôle COBIT avec le *Guide de mise en place de la gouvernance informatique : Utilisation de COBIT et Val IT, 2ème Édition*
- *Guide d'Assurance informatique : Utilisation de COBIT* - fournit des conseils sur la façon d'utiliser COBIT pour favoriser différentes activités d'assurance ainsi que des propositions de procédures d'évaluation pour tous les processus informatiques et les objectifs de contrôle de COBIT. Il remplace le *Guide d'Audit* pour l'audit ou l'auto-évaluation des objectifs de contrôle de de COBIT 4.1
- *Objectifs de contrôle informatiques pour Sarbanes-Oxley : rôle de l'informatique dans la conception et la mise en place du contrôle interne des rapports financiers, 2ème Édition* - fournit un guide pour assurer la conformité à la loi de l'environnement informatique en s'appuyant sur les objectifs de contrôle COBIT
- *Guide de mise en place de la gouvernance informatique : Utilisation de COBIT et Val IT, 2ème Édition* - fournit une feuille de route générique pour mettre en place la gouvernance des SI en utilisant les ressources de COBIT et Val IT ainsi qu'un ensemble d'outils associés
- COBIT *Quickstart, 2ème Édition* - fournit une base de contrôle pour les PMI-PME et peut servir d'étape préliminaire pour une grande entreprise
- COBIT *Base pour la sécurité, 2ème Édition* - se focalise sur les étapes fondamentales de mise en œuvre de la sécurité des SI de l'entreprise
- COBIT Mappings actuellement disponibles à l'adresse suivante : www.isaca.org/downloads :
  - Aligning COBIT, ITIL and ISO 17799 for Business Benefit
  - COBIT Mapping: Overview of International IT Guidance, 2nd Edition
  - COBIT Mapping: Mapping de ISO/IEC 17799:2000 avec COBIT, 2nd Edition
  - COBIT Mapping: Mapping de PMBOK avec COBIT 4.0
  - COBIT Mapping: Mapping de SEI's CMM for Software avec COBIT 4.0
  - COBIT Mapping: Mapping de ITIL avec COBIT 4.0
  - COBIT Mapping: Mapping de PRINCE2 avec COBIT 4.0
- *Gouvernance de la sécurité des SI : recommandations aux dirigeants d'entreprise, 2ème Édition* - présente la sécurité des SI en termes métiers et renferme des outils et des techniques pour aider à découvrir les problèmes de sécurité

VAL IT est le terme général retenu pour présenter les publications ainsi que les produits et activités à venir se référant au référentiel VAL IT.

Les publications actuelles de la famille VAL IT sont :

- *Valeur dans l'enterprise : gouvenance des investissements informatiques - le cadre de référence VAL IT* explique comment une entreprise peut tirer la meilleure valeur possible de ses investissements informatiques. Il est basé sur COBIT et est structuré en :
  - Trois processus - gouvernance de la valeur, gestion de portefeuille et gestion de l'investissement
  - Des pratiques clés de management des SI - les principes de gestion fondamentaux qui facilitent l'atteinte d'un but ou du résultat souhaité d'une activité particulière. Ils appuient les processus de VAL IT et jouent à peu près le même rôle que les objectifs de contrôle de COBIT.
- *Valeur dans l'enterprise : gouvenance des investissements informatiques - l'analyse de rentabilisation*, se focalise sur un élément clé du processus de gestion de l'investissement
- *Valeur dans l'enterprise : gouvenance des investissements informatiques - l'étude de cas ING*, décrit comment une grande entreprise du secteur financier gère un portefeuille d'investissements informatiques dans le contexte VAL IT

Visiter les sites www.isaca.org/cobit ou www.isaca.org/valit pour avoir connaissance des informations les plus à jour et les plus complètes sur COBIT et VAL IT, les produits dérivés, les études de cas, les programmes de formation, les lettres d'information et toute autre information particulière sur ces référentiels. En France consulter le site de l'AFAI : www.afai.fr

Page volontairement laissée blanche