AFAI-ISACA · CIGREF · IFACI

GUIDE D'AUDIT DE LA GOUVERNANCE DU SYSTÈME D'INFORMATION DE L'ENTREPRISE NUMÉRIQUE

2° ÉDITION · MISE À JOUR 2019

GUIDE D'AUDIT DE LA GOUVERNANCE DU SI

ÉDITION 2019

Mise à jour du Guide d'audit de la gouvernance du système d'information de l'entreprise numérique

RÉALISÉ EN PARTENARIAT PAR

Cigref · Afai-Isaca · Ifaci

COMITÉ DE PILOTAGE

Henri d'AGRAIN
Délégué général, Cigref

Pascal ANTONINI
Partner, EY
Président de l'AFAI

Régis DELAYAT
Ancien Conseiller du président pour le numérique, SCOR,
Ex-Vice-président Cigref
Administrateur AFAI

Patrick GEAI
Ancien responsable audits informatiques transverses, LA POSTE
Administrateur AFAI

Jean-Louis LEIGNEL
Associé, MAGE Conseil
Administrateur AFAI

Philippe MOCQUARD
Délégué général, IFACI

Yohann VERMEREN
Partner, KPMG
VP du Groupe Professionnel SI de l'IFACI

COORDINATION

Clara MORLIÈRE
Chargée de Mission, Cigref

SOMMAIRE

REMERCIEMENTS P. 2

PRÉFACE P. 3

IMPACTS DE LA TRANSFORMATION NUMÉRIQUE P. 5

ACTUALISATION DU GUIDE P. 8

DESCRIPTIF DES 12 **VECTEURS** P. 10

BIBLIOGRAPHIE P. 107

GLOSSAIRE P. 108

ANNEXES P. 109

CETTE PUBLICATION EST NÉE DE LA VOLONTÉ STRATÉGIQUE DES TROIS ASSOCIATIONS **AFAI, CIGREF ET IFACI** DE PRODUIRE ENSEMBLE UN OUTIL D'AUDIT DE LA GOUVERNANCE DES SYSTÈMES D'INFORMATION, UTILE ET FACILE D'UTILISATION, DESTINÉ À LEURS MEMBRES.

12 VECTEURS

DEPUIS L'ALIGNEMENT STRATÉGIQUE JUSQU'À LA RÉALISATION DES PROJETS MÉTIERS ET À LA COMMUNICATION AUPRÈS DE TOUTE L'ENTREPRISE

1. Stratégie

Intégrer les **enjeux numériques** dans le plan stratégique de l'entreprise

P. 10

2. Innovation

Diffuser la culture numérique et promouvoir les technologies innovantes

P. 18

3. Risques

Prendre en compte les risques numériques dans les enjeux stratégiques et les processus métiers

P. 26

4. Données

Gérer, **valoriser et protéger** les données de l'entreprise

P. 36

5. Architecture

Aligner l'**architecture du SI** avec les enjeux stratégiques

P. 42

6. Portefeuille de projets

Optimiser la **valeur du patrimoine SI** et gérer ses évolutions

P. 50

7. Projets

Maîtriser la **réalisation des projets** et solutions

P. 58

8. Ressources humaines

Organiser et **manager les talents** et les compétences

P. 68

9. Prestataires & Fournisseurs

Piloter les **relations avec les fournisseurs** de solutions et services numériques

P. 76

10. Services

Fournir des **services numériques** conformes aux attentes clients

P. 84

11. Budget & Performance

Piloter le budget et la **performance du SI**

P. 92

12. Marketing & Communication

Valoriser les services et **communiquer sur les enjeux** technologiques

P. 100

REMERCIEMENTS

CONTRIBUTEURS · EXPERTS

Gönül BASODA, Responsable opérationnel SI, HARMONIE MUTUELLE
Sylvain BIZOUARD, Chef de mission Audit, AXA FRANCE
Pierre CALVANESE, Président, IGC GROUP
Isabelle CARRE, Audit interne, AIR FRANCE KLM
Frédéric CHARLES, Directeur Stratégie Digitale & Innovation, SUEZ ENVIRONNEMENT
Marc DEMERLÉ, Chargé de mission, GDPR Corporate IT Referent, ENGIE
Gilles DU CREHU, Risques et Contrôle interne, EDF
Philippe EBERT, Direction des architectures techniques applicatives, DASSAULT AVIATION
Philippe ELBAZ, Responsable activités transverses, GROUPEMENT DES MOUSQUETAIRES
Tanguy FOURNIS, CISA, Chargé de mission, Contrôle interne DSI, SMA Groupe
Sabine GUILLAUME, Directrice des SI, METROPOLE EUROPEENNE DE LILLE
Jean-Pascal GUILLEMET, Associé, ERNST & YOUNG
Bruno HEMMATI, Strategic vendor management director, ORANGE
Philippe HERVIAS, Head of IS Audit, SANOFI
David METIVIER, Directeur Audit Interne IT et Operations, SODEXO
Joel PELCE, Responsable contrôle interne audit risques DSI, GRDF
Olivier PERNAUDET, Contrôleur des armées, MINISTERE DES ARMEES
Marie-Noelle QUIOT, Contrôleuse Générale des Armées, MINISTERE DES ARMEES
Guy-Pierre RODRIGUEZ, Responsable Conformité & Performance DSI, GROUPE ADP
Jean-François SZYMCZAK, Senior Manager, KPMG
Olivier SZNITKIES, Head of audit EMEA, LAFARGEHOLCIM
Gilles TROLEZ, Directeur Audit et Maitrise des risques, CARGLASS
Nicolas VIALLET, SDS/BPERF, MINISTERE DES ARMEES

AFAI-ISACA

WWW.AFAI.FR

L'Association Française de l'Audit et du conseil Informatiques (AFAI), chapitre français de l'ISACA, est l'association de référence des métiers des systèmes d'information.

CIGREF

WWW.CIGREF.FR

Association de grandes entreprises et d'administrations publiques françaises, le Cigref se donne pour mission de développer leur capacité à intégrer et maîtriser le numérique.

IFACI

WWW.IFACI.COM

L'Institut Français de l'Audit et du Contrôle Internes (IFACI) rassemble 5 500 professionnels de l'audit et du contrôle internes et, plus largement, de toutes les fonctions contribuant à la maîtrise des risques.

PRÉFACE

Avec l'intégration du numérique dans les entreprises, les organisations évoluent et se transforment tant sur leurs approches stratégique qu'opérationnelle. Le système d'information est au cœur du métier de l'entreprise, le SI développe et accélère le numérique dans l'entreprise. Il porte l'activité de l'entreprise, et son bon fonctionnement est indispensable.

Face aux mutations de l'entreprise dues à la transformation numérique, la gouvernance du système d'information (SI) est directement impactée et évolue par conséquent afin de s'adapter aux nouveaux modes de fonctionnement et aux opportunités apportées par les technologies.

La gouvernance du SI par l'entreprise est une démarche de pilotage ayant pour objectif d'apporter une contribution optimale à la création de valeur, d'aligner la stratégie numérique avec la stratégie de l'entreprise, d'optimiser l'utilisation des ressources et de maîtriser les risques en fonction de ses enjeux.

Nos trois associations, ayant publié en 2011 le Guide d'audit de la gouvernance des SI, ont souhaité le mettre à jour compte-tenu de l'évolution des entreprises et de leur SI. Une réflexion commune sur les impacts de la transformation numérique sur les entreprises a permis de proposer une actualisation de l'ensemble des vecteurs. Les recommandations données dans ce guide sont de nature stratégique et opérationnelle.

Il est important de préciser que ce guide traitant de la gouvernance du système d'information, il traite de fait également de l'activité de toute l'entreprise. C'est bien l'ensemble des acteurs de l'entreprise qui doit maitriser son système d'information de manière transverse pour assurer la réussite du numérique dans l'entreprise. La direction du système d'information est un des acteurs majeurs de cette gouvernance, sans en être le seul. La convergence, les objectifs communs de toutes les directions et la bonne collaboration sont des prérequis à une gouvernance efficace et adaptée.

Au regard des impacts cités, le comité de pilotage a proposé un nouvel ensemble de douze vecteurs. Certains vecteurs de l'édition 2011 ont été fusionnés et intégrés, et deux nouveaux vecteurs ont été ajoutés. Les deux thèmes ajoutés jouent des rôles primordiaux dans la transformation : la culture de l'innovation, et la gestion des données de l'entreprise. Par leur importance, le choix d'en faire des vecteurs dédiés est apparu comme une évidence.

Cette nouvelle version du Guide d'audit de la gouvernance du SI s'affirme encore comme un outil concret au service des auditeurs, des contrôleurs, des informaticiens, et plus largement de tous les collaborateurs de l'entreprise numérique.

Pascal Antonini, Président, AFAI-ISACA
Bernard Duverneuil, Président, Cigref
Jean-Marie Pivard, Président, IFACI

FACE AUX TRANSFORMATIONS ENGAGÉES DANS LES ENTREPRISES, LES TROIS RÔLES FONDAMENTAUX DE LA DSI RESTENT IDENTIQUES

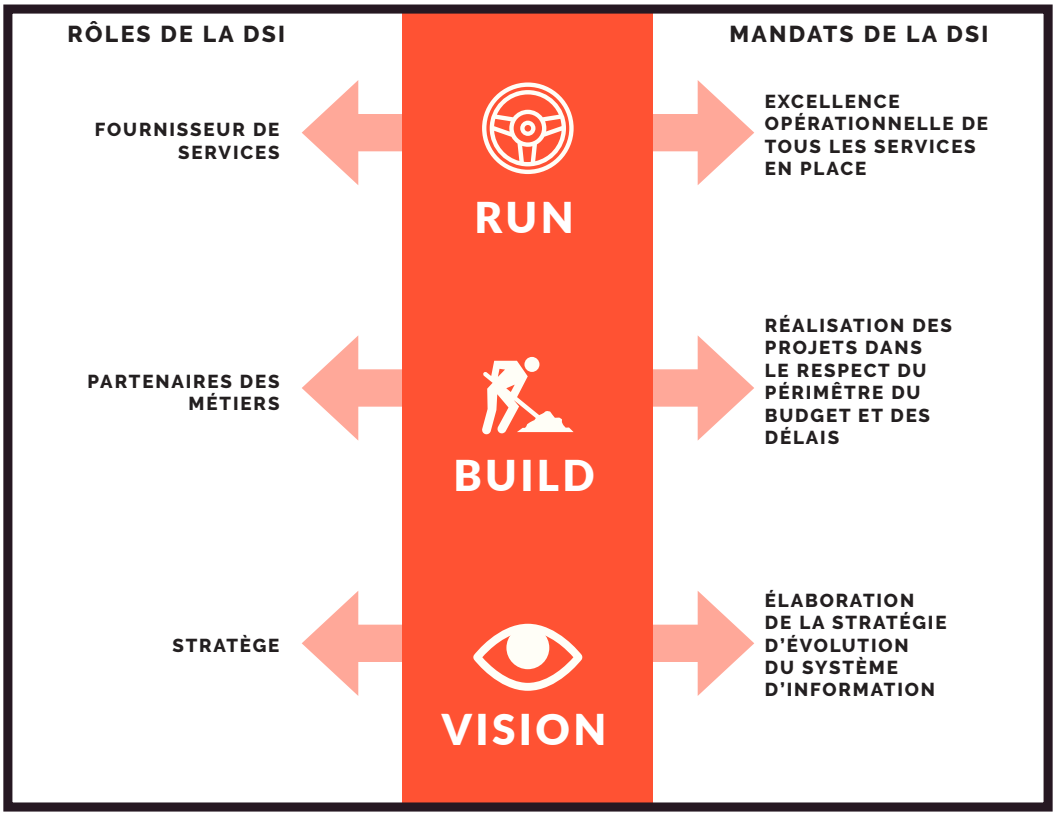
- **FOURNISSEUR DE SERVICES**
  Excellence opérationnelle de tous les services en place (*run*)
- **PARTENAIRE DES MÉTIERS**
  Construction du SI, réalisation des projets dans le respect du périmètre, du budget et des délais (*build*)
- **STRATÈGE**
  Elaboration de la stratégie d'évolution du SI (vision)

IMPACTS DE LA TRANSFORMATION NUMÉRIQUE SUR LES ENTREPRISES ET LEUR SYSTÈME D'INFORMATION

Face aux transformations engagées dans les entreprises, les trois mandats fondamentaux de la DSI restent identiques. Si ces mandats restent les mêmes, le contexte, les contenus, les moyens d'être performant et d'atteindre ces objectifs ont sensiblement évolué avec la transformation numérique de l'entreprise. La double révolution du numérique et de l'information a des effets majeurs sur l'entreprise, sur ses métiers, sur ses femmes et ses hommes, sur son système d'information et par conséquent sur sa gouvernance.

Ces fondamentaux de la DSI restent… mais leur contenu est fortement impacté par la révolution numérique.

RÔLES ET MANDATS DE LA DSI



L'ENTREPRISE, SES MÉTIERS, SES PROCESSUS, SES COLLABORATEURS

DE NOMBREUSES **ÉVOLUTIONS TECHNOLOGIQUES** (INTELLIGENCE ARTIFICIELLE, BLOCKCHAIN, INTERNET DES OBJETS…) ET **CULTURELLES** (USAGES, AGILITÉ, COMPORTEMENTS) **IMPACTENT LES PROCESSUS MÉTIERS** DE L'ENTREPRISE À DES FINS D'AMÉLIORATION DE SON EFFICACITÉ OPÉRATIONNELLE ET DU DÉVELOPPEMENT DE SON ACTIVITÉ.

La recherche de nouveaux *business models* est impérative et systématique. **De nouveaux modèles d'organisation voient le jour**. Certains métiers cherchent à externaliser leurs processus *back/middle*, pour se concentrer sur leur cœur d'activité en utilisant notamment l'automatisation et la robotisation des processus. On observe une dématérialisation et une automatisation totales des interactions avec l'écosystème de l'entreprise.

Il est essentiel pour les entreprises de renforcer leurs services aux clients pour se différencier de la concurrence mondiale. Le développement de multiples services numériques est ainsi nécessaire pour la compétitivité des entreprises et marque l'évolution de l'économie globale en France et dans le monde.

L'entreprise doit traiter la dimension culturelle de la transformation numérique et **amener ses collaborateurs à être acculturés avec le numérique**. De nombreux changements de comportements venant en partie de l'émergence des usages du numérique bouleversent les pratiques en entreprise, comme, par exemple, l'impact des réseaux sociaux. L'entreprise reconstitue ses équipes avec des profils plus jeunes, plus *numériques*, plus mixtes. Ces profils, parfois difficiles à trouver, ont de nouvelles attentes en matière de méthodes de travail (agilité, flexibilité, autonomie) qui ont des conséquences sur leur environnement de travail (mobilité, *flex-office*, travail à distance) et sur l'alignement des outils professionnels et personnels.

Ces changements de conjonctures, de comportements et de modèles pressent les entreprises à instaurer une culture de l'innovation, qui n'est pas forcément naturelle dans les entreprises habituées à engager des dépenses/projets sur la base d'un *business case*. **De nouvelles démarches apprenantes du type *Test & Learn* (MVP, PoC, Labs, *design thinking*…),** le passage du prototype (*Proof of Concept* – PoC) à l'industrialisation, l'introduction de l'agilité à l'échelle de l'entreprise et l'ouverture de l'entreprise à de nouveaux partenaires, concurrents, *startups*, clients ou fournisseurs, à de nouvelles logiques communautaires, sont des exemples de pratiques nouvelles.

LA DONNÉE, PLÉTHORIQUE, INTERNE ET EXTERNE, STRUCTURÉE ET NON-STRUCTURÉE, CONSTITUE UN CHALLENGE

La donnée, pléthorique, interne et externe, structurée et non structurée, constitue un challenge et un actif majeur pour l'entreprise. Il convient de l'exploiter et de la protéger de manière optimale. Les données personnelles représentent un enjeu réputationnel majeur. Leur exploitation est contrôlée et les risques de fuite ou de vol doivent être soigneusement prévenus. **Les risques cyber et technologiques se sont exacerbés** et sont devenus un sujet de Conseil d'administration/Comité exécutif. Face à la complexification et à l'augmentation des failles de sécurité, cyberattaques et fraudes, une forte gouvernance et un pilotage accru de la sécurité sont une obligation pour toutes les entreprises

Le poids des régulateurs est devenu prépondérant, et les règlementations représentent une contrainte lourde et coûteuse pour l'entreprise. Cette contrainte touche tous les métiers mais particulièrement la DSI.

LE SYSTÈME D'INFORMATION, LA DSI

ON CONSTATE LE RENFORCEMENT DE LA GLOBALISATION DU SYSTÈME CENTRAL (*CORE IT*[1]), UNE ÉVOLUTION DANS LES RELATIONS AVEC LES FOURNISSEURS, L'APPARITION DE NOUVEAUX ACTEURS (*STARTUPS*) ET DE NOUVEAUX MODÈLES (*CLOUD*).

La DSI devient un orchestrateur de multiples solutions et technologies, et doit faire face à d'importants challenges sur l'intégration et l'architecture du SI. La DSI devient intégratrice de *clouds* multiples.

L'entreprise se doit d'avoir une grande réactivité aux demandes ou changements et donc d'être agile. **La DSI doit concilier cette double facette** *(Core et Fast*[2]*)* du développement SI pour tirer profit des opportunités d'innovation et maitriser les risques du « *Shadow IT* » & « *Shadow Development* ». Le *Shadow IT* met en danger l'entreprise en termes de sécurité et de conformité, notamment sur le traitement des données personnelles.

Dans le même temps, l'entreprise cherche à toujours optimiser les dépenses courantes du SI pour se donner des moyens d'investir dans le développement. L'évolution des business modèles des fournisseurs vers le *cloud* entraine par ailleurs une transition des dépenses d'investissement vers des dépenses de fonctionnement (CAPEX/OPEX). Les dépenses SI pour les services aux métiers sont susceptibles d'être refacturées sur un mode « *pay-per-use* » permettant aux usagers de contrôler leur consommation.

Dans un contexte de pénurie globale des **talents numériques,** la DSI a besoin de nouveaux profils aux compétences recherchées mais aussi d'une plus grande diversité.

Les exigences de transparence de la DSI sont renforcées (tableau de bord, communication, *service management*, cybersécurité, etc.) avec la nécessité de se conformer aux nouvelles réglementations : Règlement général de protection des données (RGPD), Loi Lemaire et Macron sur le numérique, Directive NIS.

Prenant en compte ces nombreuses évolutions et transformations de l'entreprise, il est important de **s'assurer que la gouvernance du système d'information de l'entreprise numérique permet de traiter l'ensemble de ces enjeux.**

[1&2] Cf. Glossaire p. 108

ACTUALISATION DU GUIDE

L'ambition du guide d'audit est d'obtenir une vision globale de la gouvernance du SI des entreprises à l'ère du numérique. Ce document et l'outil associé (cf. chapitre suivant) constituent une première étape avant un audit du SI plus poussé qui pourrait nécessiter des référentiels plus complets (COBIT). Ce *Guide d'audit de la gouvernance du SI* se veut avant tout pragmatique. Il est le résultat de travaux basés sur le savoir-faire d'une trentaine d'experts du sujet (DSI, auditeurs, informaticiens et consultants).Il est l'outil pour évaluer le niveau de maîtrise des bonnes pratiques dans un objectif d'amélioration continue à la fois pour l'auditeur et pour le praticien. Ce dernier peut l'utiliser pour une auto-évaluation.

COMPOSITION D'ENSEMBLE

Le guide découpe l'analyse de la gouvernance du SI en douze vecteurs, depuis l'alignement stratégique jusqu'à la réalisation des projets métiers et à la communication auprès de toute l'entreprise. Le vocabulaire est commun aux fonctions représentées au sein des trois associations cosignataires, tout en préservant leurs spécificités.

ÉVOLUTION DES VECTEURS

Il a été proposé un **nouvel ensemble de douze vecteurs**. Certains vecteurs de l'édition 2011 ont été fusionnés et intégrés ; deux nouveaux vecteurs ont été ajoutés. Les deux thèmes ajoutés jouent des rôles primordiaux dans la transformation : la culture de l'innovation, et la gestion des données de l'entreprise. Par l'importance de ces sujets, le choix d'en faire des vecteurs dédiés est apparu comme une évidence.

Cf. page suivante : évolution des vecteurs entre l'édition 2011 et l'édition 2019 du guide.

STRUCTURATION

Chaque **vecteur** est introduit par des parties évoquant les **« enjeux et les menaces pour l'entreprise »** qui pourraient résulter d'une mise en œuvre insuffisante des bonnes pratiques associées au vecteur. Chacune des **bonnes pratiques** identifiées s'appuie sur un certain nombre de **critères d'évaluation** permettant d'auditer la qualité de leur mise en œuvre. Pour faciliter cet audit, des « **facteurs de risques associés au vecteur** » ont été identifiés comme étant susceptibles de nuire à l'efficacité des bonnes pratiques, voire à empêcher leur bonne mise en œuvre.

Bien que les vecteurs aient des liens entre eux, chacun est **autoporteur** afin de pouvoir être audité seul.

GOUVERNANCE

La mise à jour de ce guide est basée sur la même méthodologie et la même organisation que celles adoptées pour l'édition 2011, et qui avaient conduit à son succès. Chacun des vecteurs a été revu par les experts des trois associations afin de bien prendre en compte les différents points de vue. Nous tenons à remercier les trois pilotes de ces groupes de travail : Patrick Geai, Jean-Louis Leignel et Yohann Vermeren, ainsi que tous les contributeurs qui se sont impliqués dans la réactualisation de ce guide.

MODALITÉS D'APPRÉCIATION

Une fois le ou les vecteurs choisis, en fonction des objectifs et du périmètre de l'audit que l'on souhaite engager, il s'agit de passer en revue l'ensemble des bonnes pratiques propres à chaque vecteur et évaluer le niveau de maîtrise de chacun des critères concernés.

Les critères d'une pratique expriment parfois une progressivité dans son niveau de maîtrise. Il n'y a cependant pas de pondération à appliquer et chaque critère peut s'évaluer indépendamment des autres critères. Pour évaluer une bonne pratique, il convient donc d'examiner l'ensemble des critères de la bonne pratique concernée. Éventuellement, un critère peut être « non-applicable » au contexte de l'organisation.

La pondération sur les différentes bonnes pratiques ou vecteurs est laissée à l'appréciation de l'auditeur/évaluateur selon le contexte de sa mission dans l'entreprise auditée. Il peut alors porter un jugement sur le niveau de maîtrise globale de chaque bonne pratique, puis donner son évaluation sur l'ensemble du vecteur. Il est bien sûr recommandé de recueillir des preuves (documentation, tableaux de bord, indicateurs, mails, etc.) permettant de conforter l'évaluation du niveau de maîtrise constaté.

L'utilisateur du guide veillera, dans son évaluation finale, à identifier des points de vigilance et proposera éventuellement un audit approfondi.

Evolution des vecteurs entre l'édition 2011 et l'édition 2019 du guide

	2011	2019
Vecteur 1	Planification du SI et intégration dans le plan stratégique de l'entreprise	**STRATÉGIE :** Intégrer les enjeux numériques dans le plan stratégique de l'entreprise
Vecteur 2	Urbanisme et architecture d'entreprise au service des enjeux stratégiques	**INNOVATION :** Diffuser la culture numérique et promouvoir les technologies innovantes NEW
Vecteur 3	Gestion du portefeuille de projets orientée création de valeur "Métiers"	**RISQUES :** Prendre en compte les risques numériques dans les enjeux stratégiques et les processus métiers
Vecteur 4	Management des risques SI en fonction de leurs impacts "Métiers"	**DONNÉES :** Gérer, valoriser et protéger les données de l'entreprise NEW
Vecteur 5	Alignement de la fonction informatique par rapport aux processus métiers	**ARCHITECTURE :** Aligner l'architecture du SI avec les enjeux stratégiques
Vecteur 6	Maîtrise de la réalisation des projets en fonction des enjeux métiers	**PORTEFEUILLE DE PROJETS :** Optimiser la valeur du patrimoine SI et gérer ses évolutions
Vecteur 7	Fourniture de services informatiques conformes aux attentes clients	**PROJETS :** Maîtriser la réalisation des projets et solutions
Vecteur 8	Pilotage des services externalisés	**RESSOURCES HUMAINES :** Organiser et manager les talents et les compétences
Vecteur 9	Contrôle de gestion informatique favorisant la transparence	**PRESTATAIRES & FOURNISSEURS :** Piloter les relations avec les fournisseurs de solutions et services numériques
Vecteur 10	Gestion prospective des compétences informatiques	**SERVICES :** Fournir des services numériques conformes aux attentes clients
Vecteur 11	Gestion et mesure de la performance du SI	**BUDGET & PERFORMANCE :** Piloter le budget et la performance du SI
Vecteur 12	Gestion de la communication	**MARKETING & COMMUNICATION :** valoriser les services et communiquer sur les enjeux technologiques

STRATÉGIE

INTÉGRER LES ENJEUX NUMÉRIQUES DANS LE PLAN STRATÉGIQUE DE L'ENTREPRISE

ENJEUX POUR L'ENTREPRISE

1. Enrichir la stratégie de l'entreprise par une vision métier de sa transformation numérique et de son SI futur.
2. Optimiser la contribution du SI à la stratégie de l'entreprise, en identifiant les initiatives informatiques et organisationnelles à favoriser dans les années à venir.
3. Intégrer, dans la stratégie de l'entreprise, des opportunités de nature technologique, qui sont de plus en plus importantes pour les processus métiers.
4. Aligner les évolutions du SI avec les enjeux stratégiques de l'entreprise en impliquant la Direction générale et les métiers.
5. Être au rendez-vous de la transformation numérique qui touche toutes les entreprises.

MENACES POUR L'ENTREPRISE

1. Perdre en compétitivité en passant à côté d'opportunités de nature technologique.
2. Perdre en compétitivité en ayant des difficultés pour intégrer les projets liés à la transformation numérique.
3. Ne pas tirer le meilleur parti des investissements numériques par rapport aux objectifs stratégiques de l'entreprise, en n'anticipant pas suffisamment « en amont » un plan d'actions approprié.

INTÉGRER LES ENJEUX NUMÉRIQUES DANS LE PLAN STRATÉGIQUE DE L'ENTREPRISE

FACTEURS DE RISQUES ASSOCIÉS

1. **Manque de connaissance de la stratégie de l'entreprise.**
2. **Manque d'adaptation et d'efficacité du SI.**
3. **Manque de connaissance de l'impact des nouvelles technologies sur le modèle économique.**
4. **Manque de dialogue entre la fonction SI et la Direction générale.**

BONNES PRATIQUES

1. **ORGANISATION**
   Processus de planification et de transformation.
2. **CONTENU STRATÉGIQUE**
   Intégration des cibles métiers et technologiques.
3. **COMMUNICATION**
   Communiquer pour la compréhension et l'adhésion des métiers.
4. **INDICATEURS**
   Indicateurs financiers et non-financiers définis.
5. **PILOTAGE**
   Pilotage de la mise en œuvre de la stratégie SI.

ORGANISATION

Bonne pratique n°1

La DSI est associée au processus de planification et de transformation de l'entreprise (stratégie, plan à moyen terme et budget).

CRITÈRE 1

La DSI participe à l'élaboration du plan stratégique et du budget de l'entreprise.

- La DSI s'assure que les métiers prennent en compte les possibilités offertes par les nouvelles technologies ainsi que les contraintes du SI existant.
- La DSI participe pleinement à l'élaboration du plan stratégique de l'entreprise (intervention de la DSI dans la prise de décision sur les programmes stratégiques de l'entreprise concernant la faisabilité technique, donnant des ordres de grandeur en termes de délais et de coûts).

CRITÈRE 2

Les résultats de la veille **(CF. VECTEUR 2 INNOVATION)** sont partagés avec les responsables impliqués dans l'élaboration de la stratégie de l'entreprise.

- Ces résultats peuvent être par exemple des restitutions au COMEX des découvertes et observations faites dans des événements technologiques, dans l'optique d'un usage métier.
- Les idées d'innovation incluent, en plus de l'innovation produit/outil, les nouveaux usages, modèles économiques, services, processus, etc.
- Certaines décisions concernant les programmes stratégiques sont impulsées par des ruptures technologiques (ex : Internet des objets, *blockchain*...).
- La DSI s'organise pour être force de proposition dans la démarche de planification de l'entreprise en proposant les innovations technologiques dont l'entreprise pourrait bénéficier.
- Des propositions faites par la DSI relatives à des innovations sont reprises dans le plan stratégique de l'entreprise.

CRITÈRE 3

En collaboration avec les métiers, la DSI a élaboré le volet numérique du plan stratégique de l'entreprise.

- Ce volet numérique est élaboré conjointement avec les métiers dans le cadre du processus de planification à moyen terme de l'entreprise.
- La DSI explicite les étapes techniques majeures (grands paliers d'évolution) qui sont pré-requises par rapport aux différents objectifs du plan stratégique de l'entreprise.
- Les caractéristiques particulières de l'entreprise (nouvelles offres de service, nouveaux marchés, croissance externe ou interne, internationale, acquisition ou recentrage, etc.) sont intégrées pour déterminer les axes majeurs de la stratégie numérique.
- Toutes les entités (Lignes de Services et/ou Géographiques) associent pleinement les responsables SI (centraux ou délocalisés) dans leur processus d'élaboration de la stratégie.

CRITÈRE 4

Le volet numérique est cohérent et intégré au plan stratégique de l'entreprise au même titre que celui des autres fonctions de l'entreprise.

- Le plan stratégique de l'entreprise ayant pour vocation de coordonner les plans des différentes fonctions et d'allouer à chacune d'elles les ressources nécessaires, le volet numérique en fait nécessairement partie.
- Les affectations budgétaires sont cohérentes avec la contribution attendue du SI au plan stratégique de l'entreprise.

CONTENU

Bonne pratique n°2

Le volet numérique du plan stratégique intègre les cibles métiers et technologiques ainsi que la planification des ressources nécessaires à leur atteinte.

CRITÈRE 1

Le volet numérique du plan stratégique de l'entreprise précise les cibles métiers couvertes (processus, cartographie fonctionnelle) et les principaux impacts (organisation, compétences, technologies).

CRITÈRE 2

Le volet numérique inclut des paliers d'évolution au regard des enjeux métiers et des contraintes budgétaires (calendrier et étapes de mise en œuvre).

- Les paliers correspondent à des « états stables » ou étapes majeures de la transformation, sur lesquels l'entreprise peut capitaliser (mise en place de nouveaux services, etc.).
- Ces paliers n'empêchent pas des évolutions rapides liées par exemple au numérique.

CRITÈRE 3

Le volet numérique précise les ressources (métiers et DSI, internes et externes, financières, compétences, technologies, etc.) nécessaires à l'atteinte de la cible.

- Les plans d'action déclinés du volet numérique prévoient la mise en œuvre de ressources (du côté métiers et DSI), qui doivent être intégrées dans le plan stratégique de l'entreprise et validées.

CRITÈRE 4

Le volet numérique définit la stratégie de sourcing lui permettant d'atteindre les objectifs du plan stratégique de l'entreprise (humains, financiers, sécurité, périmètre d'activité, etc.).

- Les ressources nécessaires ayant été définies dans le critère 3 ci-avant, il s'agit ici de préciser si ces ressources proviennent d'un *sourcing* interne (développement de compétences) ou s'il est nécessaire de les acquérir à l'extérieur (achats, partenariats, recrutements, etc.).

CRITÈRE 5

Les investissements découlant du volet numérique du plan stratégique de l'entreprise sont mis en regard des bénéfices que les métiers en attendent.

- Il ne s'agit pas ici d'élaborer un *business case*, mais d'indiquer la finalité et la valeur métier des investissements demandés afin qu'une enveloppe soit inscrite au plan stratégique. Les investissements devront ensuite être autorisés au cas par cas dans le cadre de projets.

CRITÈRE 6

Le volet numérique prend en compte les enjeux éthiques, de responsabilité sociétale et environnementale (RSE), définis par la stratégie de l'entreprise.

- Ethique de conception, éthique des usages et éthique sociétale.
- **CF. PUBLICATION DU CIGREF ET DU SYNTEC NUMÉRIQUE D'UN RÉFÉRENTIEL « ÉTHIQUE ET NUMÉRIQUE ».**

COMMUNICATION — Bonne pratique n°3

Le volet numérique est communiqué, avec le plan stratégique de l'entreprise, pour susciter l'adhésion des métiers et en faciliter leur compréhension.

CRITÈRE 1

La DSI a précisé l'objectif attendu de la communication du volet numérique du plan stratégique de l'entreprise (partage, adhésion, mobilisation, transparence).

- Il est nécessaire d'élaborer un plan de communication pour le volet numérique en complément de celui pour le plan stratégique de l'entreprise.

CRITÈRE 2

La DSI a identifié les cibles pour cette communication (Direction générale, directions métiers, responsables de la DSI, les principaux acteurs impliqués dans le SI, les collaborateurs de l'entreprise, les parties prenantes externes).

- La DSI connait les attentes en matière de système d'information et de numérique des différentes directions et montre en quoi sa stratégie y contribue.
- Elle communique avec les métiers les points sur lesquels elle attend une collaboration étroite pour mener à bien son plan (par exemple : migration / reprises de données, accompagnement du changement, gestion des transitions, etc.).
- Elle a défini pour chacune de ces cibles, ses objectifs de communication et les moyens de mesurer l'atteinte de ces objectifs.

CRITÈRE 3

La DSI a défini les moyens de communication (contenu, forme, média, etc.) permettant d'atteindre les cibles identifiées.

- Les contenus sont adaptés à chaque cible identifiée et aux objectifs poursuivis par la communication.
- Les modalités (rythme, support, instance, audience, communautés d'échanges, indicateurs…) sont précisées.

CRITÈRE 4

La DSI met en œuvre et anime cette communication qui a été définie selon les modalités les plus adaptées.

CRITÈRE 5

La DSI mesure l'efficacité de cette communication (indicateurs, enquêtes, *feedback*, sondages, etc.) au regard de l'objectif initial.

INDICATEURS

Bonne pratique n°4

Des indicateurs financiers et non-financiers permettent à la DSI de rendre compte de l'exécution du volet numérique du plan stratégique à la Direction générale et aux directions métiers.

CRITÈRE 1

La DSI a défini et fait valider les indicateurs de différentes natures permettant de couvrir l'ensemble des enjeux du volet numérique du plan stratégique **(CF. VECTEUR 11 · BUDGET & PERFORMANCE).**

- A titre d'exemples : budgets d'investissements « CAPEX » et de fonctionnement « OPEX », GPEC, grands jalons, *sourcing*, mixité des équipes, bilan carbone de l'IT, etc.
- **CF. PUBLICATION *IT SCORECARD* DE L'AFAI.**

à découvrir sur

Afai.fr

CRITÈRE 2

La DSI mesure chacun de ces indicateurs conformément à un mode opératoire formalisé (objectif, source, fréquence, calcul, etc.)

CRITÈRE 3

La DSI analyse les résultats de ces indicateurs et leur écart par rapport aux objectifs afin de mettre en œuvre les actions préventives ou correctives dans une démarche d'amélioration continue.

CRITÈRE 4

La DSI met à disposition de la Direction générale un tableau de bord synthétisant les résultats de ces indicateurs et actions correctives mises en œuvre.

- La Direction générale suit de façon régulière ces indicateurs, au même titre que ceux des autres fonctions (telles que Finances, RH, etc.).

PILOTAGE — Bonne pratique n°5

Une instance de pilotage stratégique du SI est mise en place, au niveau de la Direction générale, pour valider le volet numérique du plan stratégique, rendre les arbitrages nécessaires et assurer le suivi de sa mise en œuvre.

CRITÈRE 1

Le comité exécutif (COMEX) de l'entreprise assure le pilotage stratégique du numérique.

- Le comité exécutif décide de l'organisation qu'il souhaite pour piloter sa stratégie numérique et met en place les instances nécessaires.
- Le directeur du SI (DSI) participe nécessairement à cette instance.

CRITÈRE 2

Le rôle de cette instance (validation du volet numérique du plan stratégique, arbitrages, suivi de la mise en œuvre) est défini et communiqué.

- L'instance doit être présidée par la Direction générale.

CRITÈRE 3

Cette instance comporte les directeurs métiers, le DSI et un représentant de la Direction générale.

- Le représentant de la Direction générale est le Directeur général ou une personne qu'il a désignée.

CRITÈRE 4

Cette instance se réunit régulièrement, ses décisions sont communiquées et leur application est suivie.

CRITÈRE 5

Cette instance est en articulation avec les instances de pilotage opérationnel organisées avec les directions métiers.

NOTES...

INNOVATION

DIFFUSER LA CULTURE NUMÉRIQUE ET PROMOUVOIR LES TECHNOLOGIES INNOVANTES

ENJEUX POUR L'ENTREPRISE

1. Garantir la capacité d'innovation numérique de l'entreprise au profit du développement de sa compétitivité.
2. Avoir la capacité d'identifier et de décliner les opportunités de nature technologique au sein de l'entreprise.
3. Communiquer autour de l'innovation au sein de l'entreprise et auprès des instances décisionnelles.
4. Créer les conditions les plus favorables au développement d'innovations concrètes : veille technologique, *benchmark, lab, open innovation,* écosystème *startups.*

MENACES POUR L'ENTREPRISE

1. Services ou produits obsolètes par rapport à la concurrence : perte de marché, moindre capacité à augmenter les prix et à financer la R&D.
2. Manque d'avantage concurrentiel et défaut d'image de l'entreprise.
3. Manque d'attractivité RH (recrutement, départs, *turn over*...) et de compétences adéquates pour faire face aux évolutions technologiques.

DIFFUSER LA CULTURE NUMÉRIQUE ET PROMOUVOIR LES TECHNOLOGIES INNOVANTES

FACTEURS DE RISQUES ASSOCIÉS

1. **Absence d'organisation adaptée à l'innovation, et de compétences adéquates.**
2. **Manque de compréhension des opérations et de la stratégie de l'entreprise.**
3. **Manque de compétences en communication et absence d'instance susceptible d'évaluer les opportunités proposées.**

BONNES PRATIQUES

1. **VISION GLOBALE**
   Vision établie et diffusée au sein de l'organisation
2. **ORGANISATION**
   Organisation avec une instance en charge de l'effort d'innovation
3. **VEILLE TECHNOLOGIQUE**
   Veille éclairant les efforts d'innovation et la stratégie
4. **RAPIDITÉ**
   Rapidité pour traiter dans les initiatives d'innovation
5. **COMMUNICATION ET PERFORMANCE**
   Evaluation de son efficacité et amélioration continue

VISION

Bonne pratique n°1

Une vision globale de l'innovation est établie et est diffusée au sein de l'organisation.

CRITÈRE 1

Le COMEX définit et communique sa vision de l'innovation dans l'entreprise, incluant son appétence face aux risques induits.

- La Direction générale doit encourager les employés à se dépasser, à aller au-delà de leur zone de confort.
- Elle doit communiquer que l'entreprise a conscience que l'échec fait partie du processus d'innovation.
- Elle communique également régulièrement sur l'importance de l'innovation sur le succès long terme de l'entreprise.
- La Direction générale établit l'appétence aux risques dans le cadre de l'innovation.

CRITÈRE 2

Le COMEX s'inscrit comme sponsor et est garant de la culture d'innovation.

- L'entreprise met en œuvre des techniques et dispositifs de gestion destinés à créer les conditions les plus favorables au développement d'innovations concrètes.
- L'innovation s'inscrit comme étant le fruit d'un travail effectué de manière transversale : divers départements et équipes y sont impliqués et la DSI est consultée, en tant qu'expert et contributeur, dans les sujets liés à l'innovation.

ORGANISATION

Bonne pratique n°2

Une instance coordonne les efforts d'innovation.

CRITÈRE 1

Une instance en charge de l'effort d'innovation existe, avec des rôles et responsabilités clairement définis.

- Il est nécessaire de définir les rôles et responsabilités en matière d'innovation.
- Le mandat de cette instance est clair et consiste en la promotion et la facilitation de l'innovation. Ce mandat est formellement assigné par et avec le soutien fort de la Direction générale.
- Suggestions de responsabilités pour cette instance :
  - Pilotage du processus d'innovation, alignement avec la stratégie d'entreprise
  - Sélection des projets d'innovation
  - Allocation des ressources
  - Suivi de la performance
- Cette instance peut être constituée d'éléments de la DSI, des métiers mais potentiellement de membres externes.

CRITÈRE 2

L'utilisation d'un PMO facilite l'innovation portée par les technologies émergentes.

- Le PMO aide à créer un endroit sûr et propice à l'idéation et l'expérimentation en intégrant les exercices d'idéation dans le processus de planification du portfolio.
- Le PMO peut également réserver une portion du portfolio à l'innovation.
- Le PMO travaille en collaboration étroite avec toutes les parties prenantes afin d'impliquer les bonnes personnes au bon moment.

CRITÈRE 3

L'instance en charge de l'effort d'innovation organise et suit les idées retenues.

- Un dispositif permet de collecter les idées innovatrices dans l'organisation (les initiatives peuvent prendre la forme de boites à idées, plateformes numériques, concours…).
- L'instance s'assure de la mobilisation des bonnes ressources en fonction de l'objectif de l'innovation.
- Le financement de l'effort d'innovation utilise des fonds séparés des projets standards.
- Une approche *via* des pilotes ayant une échelle limitée est adoptée afin de démontrer le potentiel de l'idée innovatrice.
- Quand une idée a démontré son potentiel en pilote, elle est sélectionnée et rejoint le portfolio de projets standards.

CRITÈRE 4

Une instance d'inspection existe afin de confirmer que les projets innovants sont conduits de façon responsable vis-à-vis de la direction et des *guidelines* technologiques d'entreprise en architecture, sécurité et standards.

- Il s'agit non seulement de confirmer le respect de certaines normes mais également de sensibiliser les équipes.
- Ces « inspecteurs / *coachs* » doivent représenter à la fois la Direction générale, les métiers et la DSI.
- Ceci permet également d'éviter la formation de *Shadow IT.*

CRITÈRE 5

Un espace innovation (par exemple un temps spécialement dédié) est accordé aux collaborateurs de façon exclusive pour les sujets d'innovation.

- Créer les environnements dédiés et propices à l'expression de la créativité et favorisant l'innovation tout en assurant le respect des bonnes pratiques du SI (« bac à sable », Lab d'innovation, salle de coworking…) ainsi que sa sécurité.
- Les collaborateurs ont la possibilité de se consacrer aux activités d'innovation, développement de projets, sur un pourcentage de leur temps de travail ou un temps dédié dans la semaine.
- Des centres d'excellence permettent de centraliser les compétences et l'expérience, de servir de dépôt de bonnes pratiques, d'exécuter des PoCs et pilotes et de former.

CRITÈRE 6

Des actions sont organisées afin d'encourager les travaux en équipes mixtes métiers/filière SI : atelier, travail collaboratif, démarche apprenante (*test and learn*).

- L'entreprise met en œuvre des techniques et dispositifs de gestion destinés à créer les conditions les plus favorables au développement d'innovations concrètes.

VEILLE TECHNOLOGIQUE

Bonne pratique n°3

Organiser la veille (technologique, réglementaire, environnementale, écosystème, etc.) pour éclairer les efforts d'innovation et la stratégie de l'entreprise.

CRITÈRE 1

Les activités de veille et d'innovation sont organisées au niveau de l'entreprise. Elles sont coanimées par la DSI et les métiers en s'appuyant sur une feuille de route partagée, et disposent de ressources suffisantes.

- Cette organisation peut se décliner de différentes façons plus ou moins formelles (par ex. rapprochement DSI et Marketing stratégique pour détecter les innovations qui pourraient différencier l'entreprise par rapport à ses concurrents).
- Sans avoir besoin d'un formalisme lourd, les « règles du jeu » sont claires : objectifs et limites de la veille, positionnement par rapport aux PoCs et aux projets.
- La DSI identifie avec les métiers les risques et opportunités des principales évolutions technologiques.

CRITÈRE 2

La DSI fait partie d'un réseau de veille au niveau de l'entreprise qui inclut d'autres fonctions métiers.

- La DSI participe à la veille globale pour anticiper et intégrer les impacts SI.
- La DSI a sélectionné un certain nombre de technologies qu'elle juge stratégiques en accord avec les métiers et dans lesquelles elle décide d'exercer une activité de veille.

CRITÈRE 3

La DSI a élargi son périmètre de veille à son écosystème, *via* la participation à des réseaux externes à l'entreprise (clubs, organismes…).

- Des experts sont sollicités pour témoigner de leur expérience et partager leurs connaissances dans le cadre de manifestations organisées par des organismes reconnus en France et à l'étranger.
- L'entreprise participe à l'évolution des normes dans les secteurs techniques stratégiques.
- Les informations issues de ces participations sont mises à disposition des collaborateurs de la DSI ainsi que des interlocuteurs métiers identifiés.

CRITÈRE 4

Les activités de veille peuvent déboucher sur des *proof of concept* (PoC) et des démonstrateurs en vue de l'amélioration des processus.

- Des démonstrations technologiques et des actions de communication au sein de l'entreprise et à l'extérieur sont réalisées.
- Certaines entreprises mettent en place des « bacs à sable » pour favoriser l'innovation. Les démonstrateurs et les PoC sont la mise en pratique des travaux de veille et démontrent la faisabilité de l'idée pour améliorer les processus de l'entreprise.

RAPIDITÉ DE L'ORGANISATION — Bonne pratique n°4

L'entreprise est organisée de façon à prendre rapidement en compte, et à traiter dans le temps imparti les initiatives d'innovation.

CRITÈRE 1

L'entreprise est en capacité de mobiliser les ressources (financières, humaines, etc.) afin de compléter les initiatives et projets dans un temps imparti.

- Un suivi du portefeuille d'innovation est réalisé.
- L'avancement des initiatives et l'utilisation des ressources mobilisées sont documentés.

CRITÈRE 2

L'entreprise implémente un processus d'innovation agile.

- Les méthodes agiles permettent à de petites équipes cross-fonctionnelles de travailler en petits incréments afin de construire et tester un produit ou une fonctionnalité sur un *proof of concept*, suivi éventuellement par un pilote sur petite échelle.

CRITÈRE 3

Le processus juridique est anticipé afin de minimiser les temps d'exécution du processus de la contractualisation et de la mobilisation des ressources externes.

CRITÈRE 4

L'innovation est prise en compte dans la gestion des ressources humaines et notamment dans le plan de développement des compétences. **(CF. VECTEUR 8 · RESSOURCES HUMAINES)**

CRITÈRE 5

L'entreprise met en place et organise des partenariats avec son écosystème (établissements d'enseignement supérieur, incubateurs, pôles de compétitivité, associations, clubs…)

- Les partenariats avec son écosystème permettent à l'entreprise de développer l'esprit d'innovation et d'attirer les talents.
- **CF. PUBLICATION DU CIGREF : « OPEN INNOVATION, UNE RÉPONSE AUX CHALLENGES DE L'ENTREPRISE ».**

COMMUNICATION ET PERFORMANCE — Bonne pratique n°5

L'innovation fait l'objet d'une communication clairement définie, d'une évaluation de son efficacité et d'une amélioration continue.

CRITÈRE 1

La communication de l'innovation est structurée selon un plan de communication interne et externe. Les actions sont relayées et les acteurs mis en avant.

- Cette communication est établie entre les différents acteurs, coordonnée par la Direction de la communication de l'entreprise.
- Ce critère est en lien avec le **VECTEUR 12 · MARKETING & COMMUNICATION.**

CRITÈRE 2

Les progrès et résultats du processus d'innovation sont communiqués à l'entreprise.

- L'instance responsable de l'innovation développe et maintient un *scorecard* afin de capturer et communiquer des métriques clés sur l'innovation.

CRITÈRE 3

Des critères d'évaluation de l'efficacité sont définis en lien avec les besoins de performance de l'entreprise.

- Ces indicateurs peuvent être quantifiés (financiers, de ressource etc...) et qualitatifs.

CRITÈRE 4

Une analyse sur la base de ces critères est effectuée pour déterminer l'impact de la nouveauté des projets innovants sur l'organisation, les collaborateurs, les clients/utilisateurs.

CRITÈRE 5

Les différents critères d'évaluation font l'objet d'une revue par la Direction générale.

NOTES...

RISQUES

PRENDRE EN COMPTE LES RISQUES NUMÉRIQUES (TECHNOLOGIQUES ET CYBER) DANS LES ENJEUX STRATÉGIQUES ET LES PROCESSUS MÉTIERS

ENJEUX POUR L'ENTREPRISE

1. Permettre d'inscrire les risques numériques (technologiques et cyber) dans la gestion globale des risques de l'entreprise et sa cartographie métier, et aider à la prise de décisions stratégiques.
2. Réciproquement, intégrer les impacts métiers dans la gestion des risques numériques en tenant compte de la gravité et de la probabilité de ces impacts.
3. Réduire les facteurs de risque inhérents à l'utilisation des technologies numériques porteuses des processus critiques et métiers au regard du fonctionnement continu et de l'exécution de la stratégie de l'entreprise (et des métiers).

MENACES POUR L'ENTREPRISE

1. Manque de fiabilité, de conformité, d'intégrité, de disponibilité et de confidentialité des informations critiques ou sensibles de l'entreprise (données financières, commerciales, personnelles, stratégiques, ou liées au savoir-faire de l'entreprise).
2. Manque de capacité de l'entreprise à faire face aux risques numériques sur les applications majeures, les infrastructures clés et les données critiques.

PRENDRE EN COMPTE LES RISQUES NUMÉRIQUES (TECHNOLOGIQUES ET CYBER) DANS LES ENJEUX STRATÉGIQUES ET LES PROCESSUS MÉTIERS

FACTEURS DE RISQUES ASSOCIÉS

1. **Absence de processus systématiques d'identification et de gestion des risques.**
2. **Manque de communication et d'échange avec les directions métiers et la Direction générale.**

BONNES PRATIQUES

1. **CADRE DE GESTION DES RISQUES NUMÉRIQUES**
   Cadre de gestion des risques numériques dans la gestion globale.
2. **CONTRÔLES EMBARQUÉS DES APPLICATIONS**
   Contrôles embarqués des applications avec les métiers.
3. **ENJEUX MÉTIERS ET STRATÉGIQUES**
   Enjeux métiers et stratégiques des risques.
4. **EVALUATION DES CONTRÔLES SI**
   Evaluation des contrôles SI régulière et en regard des enjeux.
5. **CONTRÔLE DES PROCESSUS SI**
   Contrôles de prévention, de détection et de réaction.
6. **RÉACTIVITÉ FACE AUX INCIDENTS MAJEURS**
   Mise en place de scénarios de traitement efficaces et testés.
7. **REPORTING DES RISQUES**
   Reporting des risques à la DG pour prendre les décisions appropriées.

CADRE DE GESTION DES RISQUES NUMERIQUES — Bonne pratique n°1

L'entreprise pilote la gestion des risques numériques en prenant en compte le cadre global de la gestion des risques de l'entreprise.

CRITÈRE 1

L'entreprise considère la gestion du risque comme une composante essentielle de la gouvernance de l'entreprise et l'intègre dans sa communication.

- Une communication interne et externe des dirigeants est effectuée sur la gestion des risques avec une définition claire des objectifs.
- La gestion des risques est partie intégrante du bilan annuel d'activité de l'entreprise.
- Un programme de sensibilisation et de formation est mis en œuvre.

CRITÈRE 2

Le management a mis en place une politique et une organisation de gestion des risques, couvrant l'ensemble des processus critiques de l'entreprise, intégrée au sein des métiers et de la fonction informatique.

- Il existe des comités *ad hoc* de gestion des risques intégrant les acteurs métiers et des membres du comité exécutif.
- Une filière risque intégrant l'ensemble des métiers est définie dans l'organigramme de l'entreprise. La mission de la filière risque est précisée et communiquée. La filière risque comprend une partie veille sur les risques métiers et SI ainsi que sur les risques émergents. Un correspondant risque est identifié au sein de la DSI. Un document de politique de gestion des risques est partagé au sein de l'entreprise.

CRITÈRE 3

Le niveau d'appétence et de tolérance au risque est défini et partagé avec l'ensemble des acteurs, à chaque niveau où il est pertinent. Les plans d'actions de réduction des risques sont coordonnés par la direction des risques ou à défaut par le comité de direction.

- Les unités de mesure et de fréquence sont définies et communes pour l'ensemble de l'entreprise.
- Le management a défini des seuils de risques résiduels raisonnables pour l'entreprise ainsi que l'impact financier maximal acceptable.
- Ce dispositif permet d'apporter des réponses aux questions : quelles sont les méthodes de transfert et/ou de diminution du risque ?

CRITÈRE 4

La démarche mise en œuvre pour l'identification des principaux risques associe les acteurs métiers et la DSI. Cette dernière évalue notamment les risques sur ses processus (projet, changement, exploitation, incident, sécurité, gestion des données, etc.).

- Un inventaire des risques a été établi avec les métiers et est consolidé. Cet inventaire intègre les risques SI. Une revue en est réalisée annuellement par entretiens. Elle est présentée régulièrement aux instances dirigeantes et de contrôle. L'inventaire peut également s'appuyer sur des référentiels de risques SI reconnus (*Risk IT Framework, COBIT5 for Risk,* ISO 27005).

CRITÈRE 5

L'entreprise dispose d'outils de pilotage et de suivi de gestion des risques servant d'aide aux décisions stratégiques.

- Existence de tableaux de bord relatifs à la gestion des risques technologiques et cyber pour le COMEX et Conseil d'administration (**CF. PUBLICATION CIGREF « CYBERSÉCURITÉ : COMPRENDRE, VISUALISER, DÉCIDER »**).
- Existence de bases des incidents importants, dont l'impact sur l'activité et en termes financiers est mesuré.
- Analyse et reporting de l'évolution probable, en fréquence et en impact, des incidents pris en compte dans la gestion des risques.

CRITÈRE 6

La DSI prend en compte les priorités identifiées dans le plan d'actions de réduction des risques dans le cadre du volet SI du plan stratégique de l'entreprise.

- La composante SI prend en compte généralement la disponibilité, la continuité d'activité, la protection des données contre le vol, la mauvaise sélection de projets, les projets n'atteignant pas leurs objectifs, la non-maîtrise des technologies dont l'entreprise peut avoir besoin pour son développement et sa compétitivité, etc.
- Les risques au regard des critères intégrité et confidentialité doivent également être évalués et revus périodiquement.

CONTRÔLES EMBARQUÉS DES APPLICATIONS — Bonne pratique n°2

La DSI, conjointement avec les métiers, prend en compte les contrôles embarqués dans les applications.

CRITÈRE 1

Les contrôles embarqués dans les applications sont identifiés et documentés.

- Le référentiel de contrôles inclut les contrôles embarqués. Ceux-ci, comme tout contrôle, sont décrits.

CRITÈRE 2

Les contrôles embarqués dans les applications sont testés et effectifs.

CRITÈRE 3

Le métier, en tant que propriétaire des données, reste responsable des données qu'il traite dans ses processus et partage la responsabilité des contrôles, manuels ou automatisés, avec la DSI. (**CF. VECTEUR 4 · DONNEES**)

- Il est nécessaire de vérifier que chacun conserve son niveau de responsabilité sur un traitement manuel ou informatisé. Le métier conserve une part de responsabilité même si le contrôle est automatisé par la DSI.

CRITÈRE 4

Les contrôles embarqués dans les applications sont analysés dès la phase de conception des projets (applicatifs ou d'infrastructure) afin d'optimiser la maîtrise des processus métiers et de renforcer leur contrôle interne (« *Control by design* »).

- Il existe plusieurs natures de contrôles embarqués : contrôle d'accès et séparation des tâches, configuration du système, configuration des états d'exception ou rapports d'événement (IPE, Informations Produites par l'Entité), contrôle d'interface.

ENJEUX MÉTIERS ET STRATÉGIQUES — Bonne pratique n°3

La DSI procède à une identification et une évaluation des risques numériques conjointement avec la Direction générale, la Direction des risques et les directions métiers en prenant en compte les enjeux majeurs pour l'entreprise.

CRITÈRE 1

Le périmètre d'analyse des risques SI s'appuie sur le périmètre des processus métiers définis comme critiques pour l'entreprise.

- Sont généralement pris en compte : les applications supportant des flux financiers majeurs (systèmes comptables, consolidation & reporting) ; les systèmes de facturation (gestion des achats, des commandes et des stocks) ; les applications de gestion des référentiels car considérées comme transverses (clients, contrats, etc.) ; les applications de gestion des accès ; les applications critiques en termes de confidentialité ; les applications considérées comme « cœur de métier ».
- Une vigilance particulière est accordée aux traitements des données personnelles.

CRITÈRE 2

Les ressources informatiques supportant les processus métiers identifiés comme critiques sont inventoriées. Les risques sont évalués, en termes de fréquence et d'impact, et comparés au seuil de tolérance au risque du processus métier supporté.

- Les ressources comprennent les applications, les serveurs, l'infrastructure et les postes clés qui leur sont associés.

CRITÈRE 3

L'entreprise a défini une liste des « données clés » ou « données maitres » avec la DSI et les métiers, et les a identifiées comme telles dans un dictionnaire de données unique. (**CF. VECTEUR 4 · DONNEES**)

- La connaissance des données qualifiées de « sensible » permet à une entreprise d'adapter au mieux ses dispositifs de maîtrise des risques.
- Cela intègre les traitements liés aux données sensibles (mise en place de trace, conservation, revues périodiques des droits d'accès…).
- A titre d'exemple, les données bancaires peuvent être considérées comme des données sensibles et un dispositif spécifique de contrôle doit être mis en place.

CRITÈRE 4

La DSI prend en compte les évolutions d'organisation interne et externe (fusion, nouvelle activité, nouvelle implantation, etc.).

- Dans le cas d'intégration/prise en gestion de SI, il s'agit de redéfinir un cadre de référence technique ou de s'aligner sur celui existant.
- Des réunions périodiques avec les métiers sont mises en place pour prendre en compte les évolutions.

CRITÈRE 5

Les événements survenus ou pouvant survenir (menaces) avec une fréquence et un impact potentiel négatif suffisamment important pour l'entreprise sont identifiés. Les évènements survenus sont historisés.

- Des bases d'incidents sont mises en place pour permettre de tracer et de recenser les incidents majeurs.
- Un dispositif de veille est en place afin d'anticiper les risques émergents (veille sécurité internet, émergence risques métiers, etc.).
- Un SOC (*Security Operation Center)* assure la supervision des systèmes d'information afin d'assurer un suivi en temps réel et de se protéger des cyberattaques.

CRITÈRE 6

A partir des évènements, des scénarios de risques sont identifiés puis regroupés en familles de risques informatiques.

- La non-disponibilité d'une application peut être liée à différents évènements : rupture de communication, incendie du centre de traitement, panne serveur.

CRITÈRE 7

Les risques SI prennent en compte les contraintes réglementaires, juridiques, contractuelles et sociales.

- Les contraintes réglementaires à prendre en compte sont principalement : Règlement Général de Protection des Données (RGPD), transposition de la directive NIS, Archivage fiscal et légal, SOX s'il y a lieu, réglementation sectorielle (Bâle 2, Solvency 3, Santé, Pharmacie, etc.).

ÉVALUATION DES CONTROLES SI

Bonne pratique n°4

L'entreprise réalise une évaluation régulière de l'efficacité des contrôles SI en regard des enjeux stratégiques, financiers, commerciaux, réglementaires, industriels ou d'innovation.

CRITÈRE 1

La pertinence des contrôles clés identifiés, qu'ils soient automatiques ou manuels, doit être évaluée et justifiée.

- Nombre de contrôles clés adapté à l'organisation.
- Intégration des contrôles au sein des processus.

CRITÈRE 2

L'évaluation des risques résiduels s'appuie sur les tests d'efficacité des contrôles clés au sein des processus majeurs de la fonction SI tels que la gestion de la sécurité logique et physique, gestion de l'exploitation, gestion des développements, gestion des changements.

CRITÈRE 3

L'évaluation des contrôles doit être réalisée par des équipes indépendantes des opérations évaluées.

- A cet égard, des certifications établies par des cabinets indépendants se développent notamment sur les risques Cyber (notation du niveau de cyber-résilience) mais aussi autour des notions d'OIV (Opérateur d'Importance Vitale) et OSE (Opérateur de Services Essentiels).

CRITÈRE 4

La DSI fait un suivi de la mise en œuvre et de l'efficacité des contrôles clés.

CRITÈRE 5

L'évaluation documentée comprend les contrôles récurrents de surveillance, définis avec les métiers.

CONTRÔLE DES PROCESSUS SI — Bonne pratique n°5

La DSI met en œuvre les dispositifs de contrôle sur les processus SI afin de réduire les risques notamment cyber, en liaison avec les contraintes des métiers. Ces dispositifs incluent des contrôles de prévention, de détection ainsi que des capacités de réaction adaptées.

CRITÈRE 1

La DSI identifie et met en place un référentiel d'objectifs de contrôle des risques par une approche processus SI (de type COBIT ou autre).

- **COBIT, DIFFUSÉ EN FRANCE PAR L'AFA-ISACA**, est un référentiel reconnu de gouvernance et de management du SI, notamment en termes de contrôles, de création de valeur, et de risques SI par une approche processus (exemples de processus COBIT : Assurer l'optimisation du risque, gérer les programmes et les projets, gérer l'identification et la construction des solutions, gérer les changements etc...).

CRITÈRE 2

La DSI identifie ses contrôles clés qui permettent de prévenir, détecter les risques numériques, réagir en cas d'incidents et reconstruire le SI.

- Il s'agit d'avoir un référentiel des contrôles clés, dont des contrôles généraux informatiques.
- Exemples de contrôles clés : procédure de gestion des accès aux SI, mécanismes de journal des activités sur les SI et revue de ces journaux, procédure de gestion des changements, ...
- Des audits sont réalisés de manière indépendante notamment sur les projets critiques et les enjeux cyber.

CRITÈRE 3

La DSI formalise ses contrôles clés en appliquant le modèle de documentation des contrôles défini par l'entreprise (ex : direction des risques).

- Ces modèles permettent une description et classification standardisées au niveau de l'entreprise.
- Les différents domaines comme l'infrastructure, le réseau, les données, etc.. sont à considérer.
- Cette démarche doit prendre en considération la pertinence des contrôles automatisés par rapport aux contrôles manuels pour optimiser les processus et réduire les risques résiduels.

CRITÈRE 4

La DSI étudie régulièrement les projets susceptibles de réduire les risques informatiques de façon conséquente. Ces projets peuvent être proposés pour intégration au plan informatique avec les autres projets, l'arbitrage étant réalisé avec les métiers.

- Par exemple, un projet de sauvegarde en temps réel de données critiques permet, en favorisant un démarrage très rapide en cas d'incident, de réduire un risque de discontinuité d'activité. C'est aux métiers, à la Direction des risques et à la Direction générale de décider si les coûts supplémentaires envisagés sont acceptables par rapport à l'impact de l'interruption d'activité.

CRITÈRE 5

Lors de la mise en place de contrôles applicatifs (nouveaux ou ajustements), la DSI s'assure que les tests de leur efficacité sont réalisés et communiqués.

- Les tests sont spécifiés, communiqués auprès des parties prenantes, testés et validés.

RÉACTIVITE FACE AUX INCIDENTS MAJEURS

Bonne pratique n°6

L'entreprise est capable de réagir, efficacement et dans des délais impartis, à des incidents majeurs ayant un impact significatif pour le métier.

CRITÈRE 1

Le plan de gestion de crise est formalisé et maintenu en condition opérationnelle. Il doit être associé au plan de continuité d'activité et au plan de reprise d'activité (PCA/PRA).

- Une campagne de revue des plans de crise est réalisée périodiquement
- Il est nécessaire de distinguer les plans de continuité d'activité et de reprise d'activité ainsi que les plans de continuité informatique et de reprise informatique qui ne relèvent pas des mêmes acteurs (Métiers/Direction générale et DSI).
- S'assurer que chacun de ces plans est maintenu en condition opérationnelle.

CRITÈRE 2

Les conditions de déclenchement sont définies et validées en fonction du type d'événements ou d'incidents.

- A titre d'exemple : perte ou vol de données, destruction du SI, intrusion, catastrophe industrielle ou naturelle.

CRITÈRE 3

Les *scenarios* de traitement sont définis, validés et régulièrement testés.

- La structure de réaction et de décision face aux incidents majeurs est régulièrement mise en œuvre.

CRITÈRE 4

Un bilan de gestion des incidents majeurs est réalisé, partagé, communiqué.

- La revue de Direction générale vient confirmer un engagement en faveur du management du risque en attribuant l'autorité et la responsabilité aux niveaux appropriés de l'entreprise et en garantissant que les ressources nécessaires sont allouées au management du risque.

REPORTING DES RISQUES

Bonne pratique n°7

Les parties prenantes du pilotage du risque communiquent à la Direction générale son exposition aux risques pour lui permettre de prendre les décisions appropriées dans les délais adaptés.

CRITÈRE 1

La revue des risques SI est réalisée régulièrement et en liaison avec la revue des risques métiers.

CRITÈRE 2

Les actions de revue des contrôles sont organisées en liaison avec les revues de contrôle interne au sein des processus métiers.

CRITÈRE 3

Les plans de réduction sont établis en liaison avec les évaluations des risques et des enjeux métiers, suivis par la filière risque et pilotés en coordination avec les métiers.

- Mise en place de contrôles complémentaires ou ajustement des contrôles existants (conception/formalisation).
- Partage en amont des objectifs et des modalités de contrôles à mettre en place.

CRITÈRE 4

L'entreprise dispose d'indicateurs de risque, qui permettent de mettre en évidence les événements ou situations dont l'impact négatif peut être significatif pour le métier.

- Ces indicateurs permettent de façon simple d'alerter, de mesurer l'impact, la tendance haussière ou baissière.
- Exemples :
  - **Risque projet :** besoins non validés par le management, non-respect des délais, absence de suivi des risques projets, etc.
  - **Risque de conformité :** non-respect des procédures de validation des livrables, de mise en production, absence de publication des livrables, etc.
  - **Risque sécurité :** taux d'indisponibilité des serveurs, nombre d'incidents majeurs par application/infra, nombre d'actes de malveillance externe (virus, hacking…), nombre de mots de passe faibles, nombre de tests de restauration effectués dans l'année, nombre d'audits externes, nombre de comptes génériques, nombre de comptes cumulant des fonctions incompatibles, etc.
  - **Risque contrôle interne :** niveau de satisfaction des utilisateurs, nombre de mises en production non liées à une demande d'intervention, nombre de changements urgents et non standards (modification des données en production), etc.

CRITÈRE 5

Un reporting à destination des dirigeants est effectué régulièrement, permettant d'effectuer un suivi des principaux risques et des prises de décisions appropriées qui peuvent faire l'objet d'évaluations lors d'interventions de l'audit interne.

NOTES...

DONNÉES

GÉRER, VALORISER ET PROTÉGER LES DONNÉES DE L'ENTREPRISE

ENJEUX POUR L'ENTREPRISE

1. Gouverner les données comme un actif stratégique pour l'entreprise.
2. Tirer profit des données pour développer des nouveaux projets/services.
3. Donner un avantage compétitif à l'entreprise par la différentiation vis-à-vis de la concurrence.
4. Développer la confiance dans l'utilisation des données recueillies (internes et externes).

MENACES POUR L'ENTREPRISE

1. Perte de réputation et d'image.
2. Blocage des systèmes.
3. Perte de maitrise du système.
4. Coûts financiers et/ou baisse du chiffre d'affaires.

GÉRER, VALORISER ET PROTÉGER LES DONNÉES DE L'ENTREPRISE

FACTEURS DE RISQUES ASSOCIÉS

1. **Absence d'organisation et des compétences permettant d'aligner la connaissance des données, la stratégie et les opérations de l'entreprise.**
2. **Insuffisance du dispositif de contrôle interne permettant d'assurer la protection des données (non-altération) et le respect des réglementations.**
3. **Perte et fuite de données (vol, fuite involontaire, intrusion, sabotage...).**

BONNES PRATIQUES

1. **RÉFÉRENTIEL DES DONNÉES**
   Référentiel des données pour les gérer comme actif majeur.
2. **VALORISATION**
   Utilisation des données pour créer de la valeur pour l'entreprise.
3. **SÉCURISATION**
   Sécurisation mise en place pour protéger ses données.
4. **RÉGLEMENTATION**
   Respect de la réglementation relative aux données.
5. **ETHIQUE**
   Ethique sur les actions menées pour un numérique responsable.

RÉFÉRENTIEL DES DONNÉES — Bonne pratique n°1

L'entreprise doit identifier les données et les gérer comme un actif majeur de l'entreprise.

CRITÈRE 1

Il y a une stratégie cohérente de l'utilisation des données.

- Cette stratégie concerne tout type de données : données stratégiques, données commerciales, données industrielles, données personnelles ou données critiques.
- Le sujet d'utilisation des données est inclus dans le volet numérique du plan stratégique de l'entreprise (**CF. VECTEUR 1 · STRATEGIE**).

CRITÈRE 2

L'entreprise fait et maintient un référentiel des données importantes de l'entreprise, précisant les applications qui les utilisent, la politique d'accès, la durée de conservation, le niveau de sécurité requis, etc.

- Un référentiel recense les données représentant un objet (référentiel clients, référentiel organisation, référentiel produits, etc.) ainsi que leurs caractéristiques et les relations entre elles.
- La description des processus métiers intègre bien la cartographie des données.

CRITÈRE 3

Les données de référence (utilisées par plusieurs applications ou processus métiers) sont identifiées, et les risques de conflit de mise à jour par les différentes applications sont mis en évidence.

- Le dictionnaire de données doit autant que possible indiquer l'application maître des données quand elle existe et/ou identifier les éventuels conflits et doublons avec d'autres applications.
- Le dictionnaire définit chacune des données majeures de l'entreprise (données structurées et non structurées).

CRITÈRE 4

Le dictionnaire de données est partagé et compris par les métiers et la DSI : les propriétaires des données sont identifiés, les données ont une classification de sécurité et de conformité réglementaire.

- Le dictionnaire permet notamment de recenser les données sensibles et critiques pour répondre aux contraintes réglementaires (CNIL/RGPD/Solvabilité 3) et de sécurité.
- Les acteurs de la gestion du dictionnaire ont été définis en rôle et responsabilité.
- Exemples d'acteurs : Délégué à la Protection des Données (ou *Data Protection Officer)*, Directeur des données (ou *Chief Data Officer*), mais aussi DSI, administrateur fonctionnel et technique.

CRITÈRE 5

Une gouvernance existe pour l'utilisation et la mise à jour du référentiel et du dictionnaire de données et inclut bien l'ensemble des parties concernées (métiers, fonctions).

- Une comitologie (ensemble de comités) a été mise en place avec l'ensemble des parties prenantes (référentiels de données et dictionnaires). Avec une fréquence régulière qui s'inscrit dans l'amélioration continue. Les comptes-rendus de ces comités sont tracés.

CRITÈRE 6

Un point de contrôle est réalisé pour vérifier que les référentiels et dictionnaires de données sont bien utilisés dans les nouveaux projets.

- Tout nouveau projet utilise et informe les acteurs de gestion du dictionnaire des données. Exemple : comité projet ou urbanisme.

CRITÈRE 7

L'entreprise adresse et met en place des processus de vérification de la qualité des données.

- Possibles critères de la qualité : Traçabilité / Intégrité / Fraicheur (mise à jour régulièrement) / Exactitude / Dédoublement / Exhaustivité / Cohérence / Disponibilité ...

VALORISATION

Bonne pratique n°2

L'entreprise est capable de réagir, efficacement et dans des délais impartis, à des incidents majeurs ayant un impact significatif pour le métier.

CRITÈRE 1

L'entreprise a mis en place des compétences pour exploiter ses données (Directeur des Données (*Chief Data Officer*), Délégué à la Protection des Données, *Data scientist*, Responsable des Données, Chef de Projets, etc.)

- Les fiches de rôle ou de poste sont disponibles.

CRITÈRE 2

L'entreprise a mis en place des initiatives/outils pour valoriser ses données

- Exemple d'outils : *datalake, big data, analytics, machine learning*, mais aussi *Business Intelligence* et *Customers Relationship Management* etc.
- Ces initiatives/outils concernent les données structurées et non structurées.

CRITÈRE 3

Les différentes directions de l'entreprise ont connaissance de ces initiatives/outils et se les sont appropriées.

CRITÈRE 4

Les outils et les compétences sont utilisés par les métiers pour leur fonctionnement et leurs projets notamment en matière d'innovation.

CRITÈRE 5

L'utilisation de ces initiatives/outils est mesurée périodiquement.

CRITÈRE 6

Les données sont utilisées pour anticiper et pour faire des projections.

- Des modèles prédictifs sont définis en s'appuyant sur les données utilisées

CRITÈRE 7

Les entreprises qui ont l'obligation de mettre à disposition certaines données en open data (conformité loi Lemaire) ont identifié les impacts sur la valorisation de leurs données.

- Vérifier l'existence d'une analyse d'impact formalisée sur le *business* de l'entreprise.

SÉCURISATION — Bonne pratique n°3

L'entreprise a mis en place un dispositif pour protéger ses données.

CRITÈRE 1

En fonction des enjeux, une cartographie des risques est basée sur la criticité des données (confidentialité, intégrité, disponibilité, traçabilité)

- Existence d'une méthodologie de gestion des risques, connue et partagée par l'entreprise.

CRITÈRE 2

Des dispositifs de couverture des risques sont mis en place en fonction de la criticité et de l'évaluation de la menace sur les données (**CF. VECTEUR 3 · RISQUES**)

- Existence d'un plan d'action ou de remédiation.

CRITÈRE 3

L'entreprise sensibilise ses collaborateurs, y compris la Direction générale, à la protection des données et à ses dispositifs de couverture de risques.

- Existence d'un plan de communication.

CRITÈRE 4

La «dimension donnée» est bien intégrée dans les plans de continuité et de retour de l'activité de l'entreprise (PCA et PRA).

CRITÈRE 5

L'entreprise prend en compte les aspects de sécurité lorsqu'elle utilise le cloud (propriété des données, contractualisation, type de cloud, criticité des données, réversibilité, audit, localisation des données, etc.)

- Ces mesures concernent également les sous-traitants.

RÉGLEMENTATION — Bonne pratique n°4

L'entreprise veille à être en conformité avec la réglementation relative aux données qui s'applique à son activité (RGPD, BCBS239, NIS, LPM, Solvency 3, *e-privacy*, etc.)

CRITÈRE 1

L'entreprise a identifié et gère ses obligations règlementaires.

- Il s'agit de vérifier la pérennité et la gestion dans le temps des obligations règlementaires (volet juridique, contractuel, gestion des sous-traitants, consentement des personnes, implémentation technique, gestion de crise, points de contrôle, programme de sensibilisation, gestion de la protection des données personnelles, portail de gestion des demandes, etc.)

CRITÈRE 2

L'entreprise a mis en place un dispositif pour répondre à de nouvelles obligations règlementaires.

- Mise en place d'une gestion de projet pour instaurer un cadre de gouvernance de toute nouvelle règlementation. L'entreprise s'appuie si possible sur la cartographie des processus de l'entreprise.

CRITÈRE 3

L'entreprise a mis en place un dispositif de contrôle de sa conformité à la règlementation.

- L'entreprise établit les plans de contrôle (contrôle interne et gestion des risques) et sait identifier les impacts des obligations règlementaires sur ses processus.
- Le dispositif contrôle les données existantes mais également les données entrantes (notamment les données clients).

ÉTHIQUE — Bonne pratique n°5

Au-delà du cadre réglementaire, l'entreprise capitalise sur les actions menées pour un numérique responsable.

CRITÈRE 1

L'entreprise prend des engagements auprès de son écosystème (clients, collaborateurs, fournisseurs, partenaires) à travers une charte d'utilisation des données.

- Les services juridiques, IT et métiers participent à la rédaction de la charte. La Direction générale valide et est garante de son applicabilité.

CRITÈRE 2

L'entreprise sensibilise/forme ses collaborateurs, y compris la Direction générale, à cette charte d'utilisation des données.

- La Direction de la communication peut être sollicitée pour la diffusion de la charte.

CRITÈRE 3

L'entreprise contrôle la bonne mise en œuvre de la charte au sein de l'entreprise.

- Vérifier l'existence des supports de communication et l'accessibilité de la charte. L'appropriation de la charte peut être contrôlée par exemple par des questionnaires ou des résultats de formation.
- L'entreprise peut nommer un référent pour le déploiement de cette charte (par exemple dans le rôle du Délégué à la Protection des Données ou du Responsable Ethique).

CRITÈRE 4

Dans la gestion de ses données et de son matériel, l'entreprise prend en compte le coût environnemental (mesure) et cherche à diminuer son empreinte environnementale.

- A titre d'exemple : Actions concrètes d'économie d'énergie dans les *Datacenters*, optimisation des impressions, achat et recyclage de matériel, sensibilisation du personnel, etc.

CRITÈRE 5

L'utilisation de ces initiatives/outils est mesurée périodiquement.

- L'entreprise vérifie l'existence d'un plan de communication orienté RSE (responsabilité sociétale et environnementale), s'étalonne, voire se fait certifier.

ARCHITECTURE

ALIGNER L'ARCHITECTURE DU SI AVEC LES ENJEUX STRATÉGIQUES

ENJEUX POUR L'ENTREPRISE

1. Concrétiser, au niveau des processus métiers, le volet SI du plan stratégique pour favoriser l'implication du management et maximiser les chances d'atteindre les objectifs visés.
2. Définir la trajectoire et les principales étapes pour atteindre la cible SI du plan stratégique en prenant en compte notamment les ressources et investissements requis pour chacune d'elles.
3. Fournir un cadre d'architecture au portefeuille de projets pour s'assurer qu'ils contribuent à l'atteinte de la cible SI.
4. Réduire les coûts du SI et accroître son adaptabilité en le rationalisant, en le simplifiant, en favorisant la réutilisation de fonctionnalités et en tirant parti des opportunités de services externalisés.

MENACES POUR L'ENTREPRISE

1. Ne pas atteindre la cible stratégique par mauvaise identification et planification des moyens (financiers, organisationnels, compétences, etc.).
2. Ne pas tirer parti des innovations, des offres de produits et services et des opportunités technologiques.
3. Induire des surcoûts et brider la capacité d'évolution du SI par manque de rationalisation et augmentation de sa complexité.
4. Exposer l'entreprise à des incidents de sécurité et des non-conformités (CNIL, RGPD, traçabilité, etc.).
5. Perdre le contrôle du SI (exemple « *Shadow IT* » généralisé, utilisation anarchique des offres *cloud* et SaaS, etc.).

ALIGNER L'ARCHITECTURE DU SI AVEC LES ENJEUX STRATÉGIQUES

FACTEURS DE RISQUES ASSOCIÉS

1. **Absence de connaissance de la stratégie de l'entreprise.**
2. **Manque de communication et de coordination entre métiers et SI.**
3. **Manque de compétences adéquates à la DSI et dans les métiers.**
4. **Manque d'organisation et de méthodologie nécessaire pour la gestion du SI.**

BONNES PRATIQUES

1. **CARTOGRAPHIE**
   Cartographie des applications, données, flux et infrastructures.
2. ***ROADMAP* SI**
   Feuille de route / schéma directeur déclinant la stratégie numérique de l'entreprise.
3. ***CORE* ET *FAST IT***
   Core et *Fast IT* cohabitent avec l'intégration de multiples *clouds*.
4. **COMMUNICATION VERS LES MÉTIERS**
   Communication vers les métiers pour partager les enjeux et impacts.
5. **RÈGLES ET PRINCIPES**
   Règles et principes d'architecture avec des modalités d'application.
6. **GOUVERNANCE DE L'ARCHITECTURE**
   Basée sur un cadre de référence et prise en compte des évolutions.

CARTOGRAPHIE

Bonne pratique n°1

Recenser les applications, les infrastructures, les données et les flux de données entre applications. Mettre en relation cette cartographie SI avec les processus métiers de l'entreprise et la faire évoluer à l'occasion des projets.

CRITÈRE 1

La DSI établit et maintient des cartographies applicatives (catalogue d'applications et services), techniques (infrastructures et composants techniques) et de données couvrant l'ensemble du SI. Elles sont mises à jour notamment à l'occasion des projets.

- Les cartographies n'ont d'intérêt que si elles sont utilisées de façon opérationnelle. Pour ce faire, il est indispensable qu'elles soient exactes (et donc entretenues), qu'elles contiennent des informations pertinentes (en particulier les liens entre les différents composants (VOIR CRITÈRE 2)), que leur formalisme soit accessible au plus grand nombre, tout comme les outils utilisés pour les gérer.
- Des moyens permettant de juger de la qualité de la cartographie doivent être mis en place en parallèle de l'établissement des cartographies.
- Des indicateurs (« de vivacité ») sont en place pour mesurer l'utilisation effective de la cartographie ainsi que la pertinence et l'exactitude des données.
- En particulier, l'utilisation des cartographies pour l'analyse d'impact d'une évolution du SI (projet applicatif ou d'infrastructure) devrait être systématique.

CRITÈRE 2

Les cartographies mettent en évidence les liens entre les différents composants recensés : rattachement des données (**CF. VECTEUR 4 · DONNÉES**) aux applications, flux entre applications, rattachement des applications aux composants techniques utilisés, lien entre composants techniques. Elles font aussi le lien avec les processus métiers.

- La description des flux doit préciser le protocole/solution technique, les principales données échangées et le sens des échanges.
- La description des liens entre les différents composants recensés doit être régulièrement actualisée pour garder son intérêt. Pour ce faire, on évitera les visions statiques de type *Powerpoint* difficiles à maintenir et on privilégiera les visions dynamiques. Par exemple, un modèle dynamique avec centralisation des informations de description des applications et de leurs dépendances dans une même base de données de composants de multiples natures (conçue à partir d'un méta modèle) permettrait une vision adaptée selon les métiers au sein de la DSI (conception, exploitation, support etc.).
- La description des processus métiers intègre bien la cartographie des données et des traitements.
- Les cartographies applicatives et techniques font le lien avec le référentiel de données (**CF. VECTEUR 4 · DONNÉES**).
- Les cartographies décrivent impérativement les fins de maintenance/support des composants d'architecture matérielle et logicielle.

CRITÈRE 3

Les cartographies sont mises en cohérence avec les processus métiers au travers d'outils qui permettent facilement de faire le lien entre les utilisateurs, les processus et les composants du SI, et de classifier ces derniers selon leur criticité pour les métiers.

- Certains outils proposent une approche basée sur la cartographie des processus auxquels on rattache dans un second temps les composants du SI.
- La description des processus doit être aussi indépendante que possible de l'organisation (description des 'rôles' plutôt que des 'utilisateurs').

CRITÈRE 4

Un processus d'élaboration, de maintenance et de communication des cartographies impliquant l'ensemble des parties prenantes, est formalisé et mis en place.

- Les cartographies peuvent être gérées *via* des outils spécialisés pour en faciliter l'utilisation et la maintenance, et faire le lien avec d'autres référentiels (ex : processus)

CRITÈRE 5

L'organisation en charge de l'élaboration, de la maintenance et de la communication des différentes cartographies est définie.

- En principe, la responsabilité de la gestion des cartographies est dévolue à l'équipe en charge de l'architecture du SI qui s'assure au travers de leur mise à jour de l'alignement ou de la convergence du SI avec le référentiel d'architecture.

ROADMAP SI — Bonne pratique n°2

Le volet numérique du plan stratégique de l'entreprise se décline dans une feuille de route ou schéma directeur SI, qui s'appuie sur la cartographie, le schéma d'urbanisation et l'organisation des données.

CRITÈRE 1

La *roadmap* SI décrit l'organisation cible à 3-5 ans des différentes fonctions du SI et les liens entre elles pour atteindre les objectifs du volet numérique du plan stratégique de l'entreprise. Elle est connu des responsables SI et des métiers.

- Le schéma d'urbanisation décrit de façon synthétique (en général sous la forme d'un « fond de carte ») le positionnement cible des principaux composants du SI, selon une structure et un niveau de granularité cohérents avec ceux du dictionnaire de données et de la cartographie des processus.

CRITÈRE 2

Les cartographies décrivent le positionnement actuel et cible de chaque composant des cartographies par rapport au schéma d'urbanisation.

- Il est notamment précisé si les composants en écart doivent être adaptés, remplacés ou simplement décommissionnés.

CRITÈRE 3

La *roadmap* SI détaille les projets d'alignement du SI avec le plan stratégique de l'entreprise en précisant les feuilles de route des composants en écart.

- L'impact des écarts sur l'atteinte des objectifs stratégiques est évalué afin de justifier les investissements nécessaires pour atteindre la cible SI.

CRITÈRE 4

La *roadmap* SI est mise à jour au moins annuellement pour tenir compte des évolutions technologiques, stratégiques et règlementaires.

- Les changements doivent être limités et justifiés dans une perspective moyen/long terme

FAST IT — Bonne pratique n°3

La roadmap SI prévoit une architecture permettant de faire cohabiter *Core* et *Fast IT* et d'intégrer de multiples clouds.

CRITÈRE 1

La *roadmap* SI délimite les périmètres cibles et les interactions entre le *Core IT* et les différentes applications *Fast IT*.

- Le *Fast IT* ne répondant pas aux mêmes contraintes ni aux mêmes objectifs que le *Core IT*, il est important de délimiter la frontière entre les deux pour pouvoir les piloter de manière distincte lorsque c'est nécessaire.

CRITÈRE 2

La *roadmap* SI prévoit l'intégration dans le SI de composants externes de type *cloud* (SaaS, PaaS, IaaS, ...) par exemple au moyen de plateformes internes.

- L'utilisation d'une plateforme d'échanges de type *EIP* (*Enterprise Integration Platform*) permet de maîtriser tous les types de flux échangés entre le SI interne et les solutions *cloud*, aussi bien du point de vue de la performance/qualité de service (découplage de charge notamment) que de la sécurité (authentification renforcée, chiffrement des flux), et de la maintenabilité (point de passage unique normalisé facilitant la réversibilité, CF. CRITÈRE 3).

CRITÈRE 3

Les principes de réversibilité des composants externes de type cloud et des règles d'architecture associées sont définis.

- Le *cloud* introduit par construction une dépendance potentiellement forte à un fournisseur externe qu'il faut limiter dès la contractualisation et le design de l'intégration du cloud avec le SI interne (CF. CRITÈRE 2).
- Des moyens sont mis en place pour détecter et éviter les offres *clouds* structurellement captives (e.g. offres propriétaires en mode SaaS gérant des référentiels de l'entreprise).

CRITÈRE 4

Les dépendances dans la chaine de support et d'exploitation récurrente (y compris la maintenance) sont prises en compte aux niveaux technique et contractuel. Les dépendances techniques éventuelles sont prises en compte également.

- Il faut éviter de coupler des opérations techniques entre différents *clouds* car cela est dans la pratique ingérable.

COMMUNICATION VERS LE MÉTIER

Bonne pratique n°4

Faire comprendre et partager les enjeux d'architecture avec un vocabulaire simple et des schémas explicatifs. Impliquer et responsabiliser les métiers pour les aider dans leurs choix d'investissements en identifiant les impacts sur leurs processus métiers.

CRITÈRE 1

Les principes et règles d'architecture décrivent les impacts métiers sous-jacents : bénéfices et risques associés (performance, robustesse, impact sur l'efficacité opérationnelle, coût d'usage du SI, *time-to-market,* etc.).

CRITÈRE 2

L'analyse de la conformité des solutions informatiques existantes et des projets avec le référentiel d'architecture est partagée avec les métiers en explicitant les impacts des écarts.

CRITÈRE 3

Les objectifs d'architecture SI sont intégrés dans la communication du volet SI du plan stratégique aux métiers.

- Les objectifs d'architecture doivent être mis en regard des enjeux stratégiques métiers.

CRITÈRE 4

Les métiers sont sensibilisés aux enjeux de l'architecture à travers des communautés animées régulièrement : explication des contraintes, des risques et facteurs clés de succès dans la mise en œuvre des différentes technologies, impacts (à court et long terme) de la non-application des principes et règles.

- Communiquer avec pédagogie sur les enjeux d'architecture au travers de cas d'usages concrets liés aux enjeux métier et porteurs d'innovation.
- Partager avec les métiers les retours d'expérience des projets en mettant en exergue les risques, les atouts et les limites des technologies utilisées ou des principes d'architecture appliqués.

RÈGLES ET PRINCIPES

Bonne pratique n°5

Les règles et principes d'architecture sont édictés avec des modalités d'application adaptées aux enjeux et risques. Ils permettent la réutilisation systématique de composants et fonctions préalablement développés. Ils constituent un référentiel sur lequel s'appuient les équipes de projets.

CRITÈRE 1

La DSI a établi un référentiel de principes, normes, standards techniques, procédures et règles de mise en œuvre et d'utilisation, associés à des services, tirant parti des innovations technologiques et tenant compte des contraintes du patrimoine SI existant.

- Le référentiel, également désigné comme « cadre de référence technique », est mis à jour au travers des projets (notamment lorsqu'il n'est pas applicable ou est incomplet) et de la veille technologique (définition du cadre d'application d'une nouvelle technologie, mise à jour liée à l'obsolescence d'une technologie).

CRITÈRE 2

Des règles d'architecture prévoient des espaces de liberté pour favoriser le *time-to-market* et l'innovation tout en limitant les risques de perte de maîtrise du SI (sécurité, résilience, maintenabilité, conformité, etc.).

- Plus que des règles en tant que telles, il s'agit de laisser la possibilité de déroger aux règles en vigueur dans des contextes particuliers (selon des critères précis).

CRITÈRE 3

Des fonctions préalablement développées ont été identifiées comme étant réutilisables. Elles sont dument répertoriées afin que les nouveaux projets puissent facilement les intégrer dans leurs développements.

- Une bonne pratique consiste à créer et maintenir un dictionnaire des services réutilisables et mettre en place une gouvernance des services permettant de déterminer dès leur conception les exigences de réutilisabilité des services.

CRITÈRE 4

Ce référentiel est connu, accepté et appliqué par l'ensemble des parties prenantes (les différentes composantes de la DSI et les métiers impliqués dans les projets).

- Le référentiel doit être maintenu à jour et accessible facilement (Intranet + moteur de recherche) par toutes les parties prenantes des projets.

CRITÈRE 5

Ce référentiel est régulièrement mis à jour et ses évolutions communiquées à l'ensemble des parties prenantes, y compris les impacts des évolutions sur le patrimoine SI.

- Les évolutions du référentiel prennent en compte leur impact sur le SI existant. L'utilisation des cartographies (**CF. BONNE PRATIQUE 1 · CARTOGRAPHIE**) doit permettre de mesurer cet impact et de cibler l'effort d'adaptation ou de migration du parc applicatif sur le futur standard.

CRITÈRE 6

L'application et l'évolution du référentiel d'architecture sont supervisées et contrôlées par le management de la DSI. La conformité au référentiel d'architecture est un indicateur du tableau de bord du SI.

CRITÈRE 7

Une politique générale validée par le management de la DSI régit l'évolution du référentiel et son application : description du cycle de vie, fonctionnement des instances de décision, livrables et procédures de contrôle qualité associés.

- Idéalement, le processus de mise à jour du référentiel doit être défini et intégré à la gouvernance de l'architecture et des projets pour faciliter sa mise en œuvre.

GOUVERNANCE DE L'ARCHITECTURE — Bonne pratique n°6

Une organisation est mise en place pour assurer l'application du cadre de référence et piloter son évolution pour répondre aux besoins des projets et prendre en compte les évolutions technologiques.

CRITÈRE 1

La gouvernance du SI permet de contrôler l'application des règles et principes à toutes les étapes du cycle de vie des solutions informatiques.

- Ce contrôle s'effectue dès la définition de la solution (alignement avec le schéma d'urbanisme du SI), aux différentes étapes des projets de mise en place initiale (respect du cadre de référence), pendant la maintenance (gestion de l'obsolescence), jusqu'au décommissionnement des solutions.
- Le suivi, aux différentes étapes du cycle de vie, permet également de valider ou infirmer le référentiel par l'expérience, et de le faire évoluer si nécessaire.

CRITÈRE 2

Une organisation et une gouvernance sont en place pour instruire et approuver les évolutions du référentiel d'architecture, en prenant notamment en compte les retours d'expérience et les nouveaux besoins des projets ainsi que les évolutions technologiques.

- Les moyens sont propres à l'organisation de chaque entreprise.
- Il est tout à fait indispensable de s'assurer que l'évolution du référentiel et son application correspondent à un optimum global transverse qui intègre de multiples facteurs : coût d'application du standard, support des fournisseurs sur les technologies utilisées (au moins pour les applications critiques), capacité à déployer et utiliser les prérequis techniques nécessaires aux projets, intérêt des apports technologiques apportés par le nouveau standard…

CRITÈRE 3

Des critères compréhensibles et acceptés par toutes les parties prenantes (métiers et IT) sont définis pour adapter le niveau d'accompagnement et de contrôle de chaque projet par l'architecture.

- Les objectifs d'architecture doivent être formalisés à partir des objectifs métiers du projet. Ils sont suivis au même titre que les objectifs métiers pendant toute la durée du projet.

CRITÈRE 4

Le processus de pilotage du portefeuille de projets contrôle l'application continue du cadre de référence de l'architecture.

- Un indicateur d'alignement des projets avec le cadre de référence est défini et suivi au niveau du portefeuille de projets (CF. CRITÈRE 6). Des objectifs associés sont définis et suivis (niveau minimum d'alignement des projets, niveau global d'alignement du SI à atteindre…).

CRITÈRE 5

Un processus de gestion de l'obsolescence du SI permet de s'assurer que tous les composants du SI respectent les règles de gestion de l'obsolescence définis par l'architecture. Il définit également les plans de remédiation à mettre en œuvre en cas d'écart.

- La gestion de l'obsolescence est un enjeu important pour la pérennité et la maîtrise des coûts du SI, mais difficile à « vendre » aux métiers.
- La mise en place d'un processus, d'une gouvernance et de moyens dédiés au sein de la DSI est souvent nécessaire pour garantir l'application du cadre de référence relatif à l'obsolescence.

CRITÈRE 6

Le tableau de bord de pilotage du SI intègre des indicateurs relatifs à l'architecture du SI (mesure de l'alignement avec le cadre de référence et du niveau d'obsolescence notamment). Ces indicateurs sont revus par le management de la DSI et des plans d'actions sont définis pour corriger les écarts.

- Des objectifs d'alignement du SI avec le cadre de référence de l'architecture sont définis et suivis.

PORTEFEUILLE DE PROJETS

OPTIMISER LA VALEUR DU PATRIMOINE SI ET GÉRER SES ÉVOLUTIONS

ENJEUX POUR L'ENTREPRISE

1. Couvrir de façon équilibrée, et en tenant compte des enjeux des métiers et des objectifs stratégiques de l'entreprise, l'ensemble de ses besoins en termes d'évolution du SI.
2. Garantir le caractère réaliste du portefeuille en fonction d'une estimation d'ensemble des ressources à mobiliser, des changements à conduire et des compétences nouvelles à développer.
3. Trouver un équilibre optimal entre création de valeur, risques et ressources.
4. Affecter les ressources de l'entreprise aux projets les plus contributifs à la création de valeur.
5. Concrétiser les objectifs de création de Valeur en obtenant un niveau d'engagement suffisant de la part des dirigeants tout au long des étapes du projet (lancement, réalisation, déploiement).

MENACES POUR L'ENTREPRISE

1. Passer à côté des projets stratégiques pour l'entreprise.
2. Gaspiller les ressources de l'entreprise sur des projets peu contributifs, ou mal cadrés, voire concurrents.
3. Accroître le coût du SI par manque de maîtrise des coûts récurrents des nouvelles applications.
4. Ne pas atteindre les bénéfices escomptés des projets par manque d'implication suffisante des responsables métiers et de la Direction générale

FACTEURS DE RISQUES ASSOCIÉS

1. Absence de *roadmap IT* formalisée et validée par la Direction générale et les métiers.
2. Absence de méthodologie pour l'élaboration de *business cases* adaptés à la typologie des projets.
3. Absence de méthodologie pour la gestion des priorités de lancement des projets.
4. Lancement de projets, autres que *fast IT*, sans *business case*.
5. Manque d'organisation et de définition des responsabilités en termes de pilotage du portefeuille de projets pendant toute leur durée de vie.

BONNES PRATIQUES

1. **RÉFÉRENTIEL DES PROJETS**
   Référentiel des projets unique pour la gestion globale.
2. ***BUSINESS CASE***
   Business case pour chaque projet fait avec les métiers et la DSI.
3. **INNOVATION**
   Innovation intégrée dans le portefeuille de projets.
4. **GESTION DES PRIORITÉS DE LANCEMENT**
   Gestion des priorités de lancement basée sur les *business cases*.
5. **SUIVI ET RECADRAGE DES PROJETS LANCÉS**
   Basé sur le reporting fiable et exhaustif.
6. **BILAN DE PROJET**
   Bilan de projet pour tirer les enseignements nécessaires.

RÉFÉRENTIEL DE PROJETS

Bonne pratique n°1

Tous les projets sont répertoriés dans un référentiel unique pouvant être structuré en programme afin de faciliter une gestion globale des projets.

CRITÈRE 1

Il existe un référentiel unique concernant l'ensemble des projets.

- Afin de pouvoir les comparer, les projets sont présentés dans un cadre normalisé au sein de l'entreprise.
- Les idées de projets et initiatives liées à l'innovation sont intégrées au portefeuille, dans une catégorie spécifique, même si le projet n'est pas encore formalisé.

CRITÈRE 2

Tous les projets sont répertoriés dans ce référentiel depuis les idées de projets jusqu'aux projets lancés en cours de réalisation.

- Le *business case* est le livrable d'un processus de validation progressive des projets depuis leur idée initiale jusqu'à la décision de lancement.
- Le processus comprend généralement les étapes de validation suivantes : déclaration d'intention ou d'opportunité, cadrage fonctionnel métier avant-projet, prototypage (si besoin), *business case*, *scoring*, décision de lancement.
- Tous les projets sont déclarés dans le référentiel, y compris les projets en cours.

CRITÈRE 3

Afin de faciliter les prises de décision, le référentiel est structuré pour classifier les projets selon leur typologie.

- La segmentation du portefeuille de projets peut s'appuyer sur la typologie suivante :
  - Programmes, lorsque cela est pertinent, les projets sont affectés à des programmes,
  - Projet de type réglementaire et de mise en conformité,
  - Projet d'innovation (en général technologique),
  - Projet de soutien au développement de l'activité,
  - Projet visant à l'amélioration des performances (qualité, réduction des délais, standardisation des processus),
  - Projet de réduction de coût,
  - Projet d'optimisation des systèmes ou d'infrastructure,
  - Projet de maintien en condition opérationnelle,
  - Projet de décommissionnement,
  - Etc.
- Un autre axe de segmentation classe les projets en fonction de leur stade d'avancement :
  - Déclaration d'intention approuvée,
  - Cadrage fonctionnel métier validé,
  - Avant-projet validé,
  - *Business case* validé,
  - Projets lancés (par phase du projet : **CF. VECTEUR 7 · PROJETS**).
- Pour vérifier l'alignement des projets avec la stratégie de l'entreprise, il est impératif d'indiquer pour chaque projet à quel volet du plan stratégique il se rapporte.
- Les dépendances entre projets doivent être identifiées et décrites.

CRITÈRE 4

Le référentiel des projets est géré par une organisation dont c'est la mission principale.

- La gestion formelle du portefeuille est généralement assurée par un « Project Management Office » (PMO), qui prépare les décisions du COMEX.
- Les projets sont évalués à la fois en fonction de leur contribution à la création de valeur et des risques/difficultés de mise en œuvre inhérents.
- Cette évaluation peut être introduite dans la structuration du référentiel pour classer les projets depuis « valeur forte/risques faibles » jusqu'à « valeur faible/risques forts ».

BUSINESS CASE — Bonne pratique n°2

Les métiers élaborent un business case avec l'aide de la DSI, pour chaque projet métier ayant un volet SI significatif.

CRITÈRE 1

Le business case présente les bénéfices attendus par l'entreprise en termes d'amélioration des processus et de création de valeur.

- Ces *business case* explicitent les bénéfices métiers attendus et les conditions nécessaires à leur obtention :
  - Quoi ? (Objectifs du projet)
  - Pourquoi ? (Opportunité et bénéfices attendus)
  - Qui ? (Moyens humains et compétences nécessaires)
  - Combien ? (Coûts et ROI)
  - Quand ? (Objectif de développement, rapidité d'exécution, perspective court/long terme).
- Les bénéfices du projet sont définis avec des critères qualitatifs et/ou quantitatifs.
- Les impacts pour les métiers (organisation, processus, niveau de compétences à mettre en place) sont clairement évalués.

CRITÈRE 2

Le *business case* évalue la rentabilité des projets en prenant en compte les gains espérés et les coûts prévisionnels globaux.

- Lorsque le volet SI est important, les coûts (projet et récurrent) sont estimés sur la base de prototypes, si nécessaire.
- L'élaboration d'un plan de charge permet d'affiner la vision temporelle du *business case*.
- Les coûts récurrents doivent être estimés sur une période de 3 à 5 ans (voire en fonction de la durée de vie estimée de l'application).

CRITÈRE 3

Le *business case* inclut une analyse des risques (non-atteinte des bénéfices escomptés, dérapage des coûts et des délais, risques à ne pas faire, etc.)

- Identifier les conditions de réussite du projet (notamment privilégier les prototypes lorsque les enjeux le justifient) (**CF. VECTEUR 7 · PROJETS**)
- Identifier les interdépendances entre projet, qui constituent un facteur de risque souvent sous-estimé. Il convient donc d'en mesurer l'impact sur les *business case*.
- Envisager des solutions alternatives (ex : refonte du processus métier) ou un fonctionnement en solution dégradée.

CRITÈRE 4

Le leadership de l'élaboration des *business case* est assuré par les métiers en collaboration avec la DSI.

- Pour les projets purement techniques et d'infrastructure, le *business case* peut être établi par la DSI et validé par le COMEX.
- Trop souvent, l'élaboration de *business case* est limitée aux seuls projets dont les coûts sont les plus importants sans suffisamment prendre en compte leurs enjeux.

CRITÈRE 5

L'entité métier commanditaire du projet est responsabilisée à la fois sur l'atteinte des bénéfices attendus et sur une gestion optimale des risques.

- Les *business case* comportent l'identification des responsables métiers (y compris sponsors) qui auront en charge la concrétisation des bénéfices métiers. Pour cela, ils sont associés au déroulement du projet pendant toute sa durée de vie.
- Les responsables métiers concernés prennent, avec le chef de projet métier toutes dispositions (en termes de personnel, information, formation, organisation, etc.) nécessaires à la concrétisation des bénéfices attendus.

CRITÈRE 6

La DSI vérifie la cohérence du business case avec la roadmap SI.

- Cette vérification de cohérence est indispensable pour :
  - Maîtriser les évolutions du SI (exemple « *Shadow IT* » généralisé, utilisation anarchique des offres *cloud* et *SaaS*…)
  - Garantir la sécurité du SI (incidents de sécurité, cyberattaques, etc.) et sa conformité (CNIL, RGPD, traçabilité, etc.)
  - Rationaliser les évolutions du SI et maîtriser les technologies nécessaires pour ces évolutions
  - Maîtriser la dette technique (obsolescence matérielle et logicielle) (**CF. VECTEUR 5 · ARCHITECTURE**).

INNOVATION — Bonne pratique n°3

Le portefeuille de projets intègre les projets d'industrialisation des initiatives d'innovation (PoC, MVP, Labs et autres travaux de R&D) (CF. VECTEUR 2 · INNOVATION).

CRITÈRE 1

La DSI recense les initiatives qui ont vocation à être industrialisées auprès des acteurs de l'innovation.

- Ces acteurs de l'innovation peuvent être dans la DSI (cellule et communauté d'innovation), dans les directions métiers, dans la Direction innovation, etc.
- La DSI travaille avec les porteurs de ces initiatives, parfois appelés « champions numériques ».
- La DSI doit être impliquée en amont de la décision d'industrialisation pour en assurer la faisabilité (choix d'architecture, sécurité, etc.).

CRITÈRE 2

La gouvernance du portefeuille est adaptée pour gérer ces initiatives d'innovation en fonction de leurs spécificités (notamment leur rapidité - *Fast IT*).

- Ces initiatives sont passées en revue régulièrement pour décider de les poursuivre, de les réorienter ou de les arrêter.
- La méthode d'analyse s'inspire des méthodes de développement du numérique.
- Le processus de décision est rapide.
- Lorsqu'un projet est jugé porteur, des moyens de développement rapide lui sont alloués et il rejoint le portefeuille de projets de type « *Core IT* ».

GESTION DES PRIORITÉS DE LANCEMENT — Bonne pratique n°4

Un processus de gestion des priorités de lancement (inter-projets) basé sur les *business case* est mis en place et implique les directions métiers au niveau du Comité de direction pour les projets clés.

CRITÈRE 1

Pour prioriser leur lancement, les projets du portefeuille sont évalués en fonction des bénéfices escomptés pour l'entreprise, des risques inhérents, et du cadre budgétaire prédéfini appréciés dans la durée.

- Un canevas de décision et d'arbitrage est défini, partagé et préétabli.
- L'évaluation des bénéfices et des risques se fait sur la base du *business case*.
- Les dépendances avec des projets existants ou sur le point d'être lancés sont identifiées et leurs impacts analysés.

CRITÈRE 2

Les décisions de lancement des projets sont prises par le COMEX.

- L'autorisation de lancement des projets tient compte des contraintes opérationnelles : ressources humaines disponibles, capacité à faire, ressources financières.
- Les résultats des évaluations, et leur conséquence en termes de hiérarchisation, sont formalisés et communiqués aux équipes concernées.
- Un processus d'escalade vers la Direction générale est mis en place pour un arbitrage final si nécessaire.

CRITÈRE 3

Les décisions de lancements des projets s'adaptent en fonction des enjeux stratégiques de l'entreprise et de son environnement concurrentiel (time-to-market).

- Dans ce cas, une approche de projet « *time-driven project* » ou agile peut être mis en œuvre (**CF. VECTEUR 7 · PROJETS / BONNE PRATIQUE 3 / CRITÈRE 3**).

SUIVI ET RECADRAGE DES PROJETS LANCÉS — Bonne pratique n°5

Un processus de management de projets, impliquant les directions métiers, permet de suivre, de recadrer (revoir la priorité voire éventuellement arrêter) les projets en cours, sur la base d'un reporting fiable et exhaustif, le cas échéant en actualisant les *business case*.

CRITÈRE 1

L'état d'avancement des projets est suivi régulièrement, de façon synthétique, par le PMO, qui rend compte au COMEX.

- Les chefs de projets mettent à jour l'avancement des projets (qualité, coûts, délais, risques, reste-à-faire, etc.) dans l'outil dédié au suivi des projets pour permettre l'élaboration de synthèses
- Ces informations sont validées conjointement avec le métier dans un comité projet.
- Ce vecteur est en lien très étroit avec le **VECTEUR 7 • PROJETS**, qui décrit le suivi des projets en cours et le reporting à faire remonter aux instances de pilotage (y compris COMEX).

CRITÈRE 2

Sur la base de ce suivi, le COMEX prend des décisions d'allocation de ressources, de re-priorisation et d'actualisation du *business case* si nécessaire.

- Cette allocation de ressources peut se faire entre différents projets.

CRITÈRE 3

Un outil de gestion du portefeuille de projets articulé avec le suivi opérationnel des projets facilite le pilotage de l'ensemble du portefeuille.

- L'outil de gestion de portefeuille agit comme un outil de consolidation des éléments utilisés dans la gestion opérationnelle des projets.
- Il intègre les éléments clés de pilotage, tels que : allocation des ressources, interdépendances avec les autres projets, indicateurs unifiés, ….
- Cet outil est mis à la disposition des directions métiers.

BILAN DE PROJET MÉTIER

Bonne pratique n°6

La Direction générale fait effectuer des bilans de projet métier, lorsque celui-ci a atteint un fonctionnement nominal, pour tirer les enseignements nécessaires à l'optimisation du processus de prise de décisions concernant les projets.

CRITÈRE 1

Pour les projets fortement contributifs à la création de valeur et/ou couteux, les bénéfices métiers atteints sont analysés pour vérifier qu'ils sont en ligne avec le *business case* initial.

CRITÈRE 2

Ces analyses doivent intégrer toutes les parties prenantes (équipe projet, utilisateurs finaux, clients, etc.).

- Le recours à une tierce partie (interne ou externe) pour avoir une vision indépendante peut être utile.

CRITÈRE 3

Les analyses sont formalisées, ainsi que les retours d'expérience concernant le déroulement du projet. Des plans d'actions d'amélioration du processus de gestion du portefeuille de projets, ainsi que de lancement ou de réalisation de projets, sont mis en place pour sécuriser la concrétisation des bénéfices attendus.

- Les bilans de projet métiers viennent alimenter une base de connaissances partagée mise à disposition de l'ensemble des directions métiers et des acteurs de la DSI. Afin d'exploiter plus facilement les données recueillies lors de bilans de projet, l'utilisation d'un modèle unique est recommandée.

CRITÈRE 4

La Direction générale s'assure que les responsables métiers concernés prennent toutes dispositions correctives (en termes de personnel, information, formation, organisation, etc., voire lancement d'un autre projet).

- La Direction générale suit la bonne mise en œuvre des actions correctives décidées.

PROJETS

MAITRISER LA RÉALISATION DES PROJETS ET SOLUTIONS

ENJEUX POUR L'ENTREPRISE

1. S'inscrire en adéquation avec le portefeuille de projets défini par l'entreprise, ce qui doit garantir l'alignement avec les besoins métiers et le plan stratégique de l'entreprise.
2. Concevoir le projet comme un projet métier avec un volet numérique (et non l'inverse), en définissant bien l'implication, les rôles, les responsabilités par les directions métiers et DSI dans le pilotage et dans la conduite du projet en intégrant les processus métiers et les besoins de compétences métiers à faire évoluer (conduite du changement).
3. Mettre en place les conditions du bon déroulement du projet par rapport aux objectifs du business case (étude d'opportunité), notamment en termes de coûts, délais, fonctionnalités développées, bénéfices attendus et appropriation par les utilisateurs.
4. Assurer la bonne cohabitation de diverses méthodes de projet (par ex. « agile » *vs* celle plus classique du « cycle en V »). Cette démarche doit intégrer les critères de décision d'utilisation d'une méthode par rapport à d'autres.

MENACES POUR L'ENTREPRISE

1. Manque d'optimisation des ressources de l'entreprise.
2. Incapacité à générer les bénéfices métiers attendus.
3. Perte de compétitivité par un dysfonctionnement de l'entreprise.

MAITRISER LA RÉALISATION DES PROJETS ET SOLUTIONS

FACTEURS DE RISQUES ASSOCIÉS

1. Non-respect de la stratégie du SI et du portefeuille projet.
2. Absence de définition des rôles et responsabilités (SI et métier).
3. Absence de méthodologie de gestion de projet.
4. Maitrise insuffisante des différentes méthodologies de gestion de projet.

BONNES PRATIQUES

1. **OBJECTIFS MÉTIERS DES PROJETS**
   Objectifs métiers des projets explicites, cohérents et partagés.
2. **GOUVERNANCE DES PROJETS**
   Gouvernance des projets claire, légitime et reconnue.
3. **MÉTHODE DES PROJETS**
   Méthode des projets liée aux objectifs escomptés.
4. **CONFORMITÉ DU PROJET**
   Conformité du projet et sécurité intégrée dès la phase de conception.
5. **PILOTAGE DES JALONS**
   Pour le suivi des dérives des objectifs.
6. **RECETTES TECHNIQUES ET FONCTIONNELLES**
   Recettes techniques et fonctionnelles avant mise en production.
7. **BILAN DE PROJET SI**
   Bilan de projet SI réalisé et partagé.

OBJECTIFS MÉTIERS DES PROJETS

Bonne pratique n°1

Les objectifs stratégiques métiers du projet sont explicites, cohérents entre eux et partagés.

CRITÈRE 1

Les enjeux ou objectifs clés des métiers, à atteindre lors du déroulement du projet, sont clairement identifiés au lancement du projet puis actualisés.

CRITÈRE 2

Les objectifs stratégiques (financiers, opérationnels, techniques, etc.) sont explicités par le management aux différentes parties prenantes.

CRITÈRE 3

Ces objectifs sont cohérents entre eux.

CRITÈRE 4

Ces objectifs sont compris et partagés par tous les acteurs du projet.

CRITÈRE 5

Ces objectifs sont hiérarchisés et une procédure d'arbitrage est en place pour résoudre les conflits entre des objectifs qui deviendraient incompatibles ou même contradictoires.

GOUVERNANCE DES PROJETS

Bonne pratique n°2

Le mode de gouvernance du projet est clair, partagé, légitime et reconnu.

CRITÈRE 1

L'entité leader est unique et légitime.

- L'entité leader est la direction, le service, le département utilisateur final de la solution. Il s'agit dans la plupart des cas d'une entité métiers (à l'exception des projets techniques).
- Dans le cas d'un projet transversal, l'entité leader est l'entité la plus concernée ou la plus légitime, voire la plus motrice.

CRITÈRE 2

Le sponsor est désigné et connu de tous. Sa disponibilité réelle lui permet de tenir son rôle.

- Le sponsor a le rôle de celui d'un facilitateur pour prendre les décisions importantes et pour garantir la cohérence d'ensemble.

CRITÈRE 3

Un comité de pilotage stratégique (présidé par le sponsor et animé par le chef de projet / *Scrum Master*) ainsi qu'un comité de projet opérationnel sont constitués et effectifs.

- Chacun des deux comités effectifs est constitué de participants représentatifs des différentes activités et sujets traités (métiers, informatique, conduite du changement, etc.). Ils se tiennent à fréquence régulière et adaptées aux sujets traités. Ils permettent de prendre des décisions et d'orienter le projet. Un compte rendu de décisions est systématiquement et rapidement rédigé à l'issue de chaque comité.
- Le comité de pilotage produit un reporting à destination d'un comité constitué de représentants de la Direction générale, de la DSI et des métiers sous un format standardisé, lui permettant d'exercer son rôle de gestion consolidée du portefeuille de projets (**CF. VECTEUR 6 · PORTEFEUILLE DE PROJETS**).

CRITÈRE 4

Le mode de pilotage du projet est complètement défini. Il intègre les comités complémentaires au comité de pilotage et au comité du projet. Ces comités additionnels sont connus (objectifs, fréquence, tableaux de bord et indicateurs, etc.).

- Exemples de comités complémentaires : comité métiers, comité d'arbitrage fonctionnel, suivi de lot ou de chantier, comité d'intégration dans le SI, comité de recette des développements réalisés, etc.
- En cas de difficultés rencontrées sur des projets critiques, l'entreprise peut faire appel à des audits indépendants.

CRITÈRE 5

Les enjeux et les risques, opérationnels, financiers et humains, du projet sont identifiés et connus de tous. La criticité de ces risques doit être régulièrement évaluée, suivie et communiquée à toutes les parties prenantes.

- Les coûts du projet sont identifiés et quantifiés. Ces coûts prennent en compte l'ensemble des coûts imputables au projet.
- Le volet « accompagnement » est prévu en amont dans le projet et est dimensionné correctement afin de surmonter les résistances au changement.
- Une cartographie des risques est entretenue et communiquée à des échéances régulières.

CONDUITE DES PROJETS — Bonne pratique n°3

La méthode de conduite des projets est évaluée en amont en cohérence avec les autres projets et l'atteinte des objectifs escomptés. Elle doit inclure les enjeux liés à la conduite du changement.

CRITÈRE 1

Une évaluation de différentes méthodes de conduite de projet reconnues au niveau de la DSI (méthodes « cycle en V » ou « agile ») est menée lors du processus de conception du projet.

- La transformation numérique requiert un modèle de gestion de cycle de vie pour les applications du SI séparant les applications cœur, celles assurant une différentiation et celles permettant l'innovation. En fonction de leur niveau, de la complexité/criticité des projets, de la taille de l'équipe projet, le processus de conduite du projet choisi devra être plus ou moins continu.
- Dans certains cas (*Fast IT*), les projets peuvent être pilotés par les délais (« *time-driven projects* »), les arbitrages sont par conséquent faits sur le contenu fonctionnel de ces projets.

CRITÈRE 2

Le choix de la méthode de gestion de projet doit prendre en compte la synchronisation nécessaire avec les autres projets en cours et la capacité de la DSI d'y faire face, en plus des éléments propres au projet (coût, délai, compétence des équipes).

- La dualité des processus (historiques ou continus) nécessite que la DSI soit en mesure d'assurer une gouvernance unifiée.

CRITÈRE 3

Le chef de projet / *Scrum Master* est unique et il a un profil de compétences orienté métier. Il dispose d'une autorité réelle sur une équipe et un budget dédié.

- Il est possible de mettre en place des binômes de chefs de projets utilisateur/DSI.

CRITÈRE 4

Les acteurs du projet sont mobilisés de façon adaptée en fonction des typologies de projets (méthodes « cycle en V » ou « agile »).

- Dans certains cas (en projet agile notamment), la technique DevOps permet de rapprocher les équipes de développement et les équipes de production ce qui soutient des cycles de développements plus courts, une augmentation de fréquence de déploiement et une livraison continue.

CONFORMITÉ DU PROJET

Bonne pratique n°4

En plus de l'implication *sine qua non* des utiisateurs finaux, la sécurité, la conformité et le contrôle interne doivent être intégrés dès la phase de conception des SI.

CRITÈRE 1

La conformité est prise en compte dès la phase de conception du projet.

- Au-delà de l'intérêt propre pour éviter des surcoûts liés à une prise en compte tardive, le « *security & privacy by design* » est une contrainte réglementaire liée au Règlement Général de Protection des Données (RGPD) et d'autres éventuelles réglementations à appliquer.

CRITÈRE 2

Le contrôle interne est intégré dès la phase de conception du projet.

- Afin de limiter les difficultés de suivi de la conformité (réglementaire et sécuritaire) du projet, il est nécessaire d'intégrer les contraintes liées au contrôle interne au plus tôt.

CRITÈRE 3

La capacité à pouvoir assurer la sécurité du projet inséré dans le SI doit être anticipée.

- Afin de pouvoir s'assurer de la cohérence sécuritaire du SI, et de la capacité du centre opérationnel de sécurité (*Security Operational Center – SOC*) à y répondre, le respect des normes de cohérence technique du SI doivent être pris en compte dès la conception.

PILOTAGE DES JALONS

Bonne pratique n°5

Des jalons réguliers sont prévus pour le suivi des dérives des objectifs, coûts, délais, faisabilité technique, exigences des métiers par rapport aux objectifs initiaux.

CRITÈRE 1

Des indicateurs pertinents sont définis pour permettre de suivre l'avancement du projet et d'anticiper la survenance des difficultés. Ces indicateurs sont mesurés régulièrement.

- Les indicateurs permettent d'assurer le suivi des charges, du planning et de la production (en unité d'œuvre). Ils peuvent, par exemple, mesurer le taux réel d'allocation et de consommation des ressources, le nombre ou le pourcentage d'exigences ajoutées ou modifiées qui peuvent être l'illustration d'une dérive par rapport aux objectifs initiaux. Une partie de ces indicateurs doivent permettre de suivre la préservation des enjeux métiers dans le déroulé du projet.
- En projet agile, le cycle de développement étant plus court, adaptatif et itératif, des indicateurs appropriés doivent être définis, au niveau des *Sprint*/Itérations, *Epic* (Épopée) ou autres.

CRITÈRE 2

Ces indicateurs sont partagés et servent de critères de pilotage et de décision dans les comités mis en place.

CRITÈRE 3

Les procédures de remontée des alertes et d'arbitrage sont définies.

- Si les procédures de remontée des alertes ont été activées, elles ont donné lieu à une décision effective.
- En projet agile, les alertes peuvent être données beaucoup plus rapidement qu'en cycle en V classique.

CRITÈRE 4

L'instance de suivi la plus opérationnelle examine régulièrement les indicateurs de dérive et décide des arbitrages ou, si nécessaire, remonte les alertes jusqu'au comité de pilotage qui tranche en dernier recours.

- En projet agile, il se peut que seule une structure opérationnelle réunissant les parties prenantes existe.

CRITÈRE 5

Le comité de pilotage valide le passage des jalons.

- Les jalons sont fréquemment positionnés pour valider des options structurantes du projet sur lesquelles il sera difficile de revenir en arrière sans conséquence importante. Les passages de jalons sont trop souvent assumés par la fonction SI qui endosse alors une responsabilité dévolue au métier.
- En projet agile, la structure opérationnelle peut valider le choix et la priorisation des *User Stories* du *Backlog* à inclure dans le prochain Sprint.

RECETTES TECHNIQUES ET FONCTIONNELLES — Bonne pratique n°6

Le projet fait l'objet de recettes techniques et fonctionnelles avant mise en production.

CRITÈRE 1

Des tests techniques et fonctionnels unitaires sont réalisés par la DSI.

- Les tests de non régression fonctionnelle peuvent également être menés par la DSI sous réserve d'une validation finale par un panel d'utilisateurs.
- En projet agile et DevOps, des nouvelles techniques de test adaptées sont déployées (tels que des *Test Driven Development, Acceptance Test-Driven Development* ou *Behavior-Driven Development*).

CRITÈRE 2

La phase de recette métiers est planifiée et effectivement réalisée.

- La phase de recette métiers est incontournable quelle que soit la méthodologie de gestion de projet adoptée.
- En projet agile, si le *Product Owner* (PO) est sachant et disponible une validation continue peut être effectuée, sinon une validation par lot est effectuée essentiellement sous forme de démo avec les métiers à la fin d'un *Sprint*.

CRITÈRE 3

La validation de la recette fait l'objet d'une approbation formelle.

- Cette validation est réalisée sur la base d'un bilan détaillé des résultats de chaque recette, y compris les cas restant en anomalie, jugés non bloquants. Le compte rendu du comité de tests produit un procès-verbal (PV) de recette signé et documenté (liste des anomalies restantes et justification de leur caractère non bloquant).
- En projet agile, la matérialisation de cette approbation peut alors n'être qu'un email des métiers confirmant l'adéquation du logiciel avec les *Users Stories* de ce *Sprint*.

CRITÈRE 4

Le feu vert est émis par le comité de pilotage sur la base de critères de GO/NO GO explicites et partagés.

- Les critères de GO/NO GO doivent couvrir l'ensemble des dimensions permettant de décider d'un démarrage : le résultat de la recette est un critère incontournable de GO/NO GO au même titre que la formation, la documentation et l'accompagnement au démarrage (cellule d'accompagnement, support, etc.). Les critères de GO/NO GO ainsi que leur seuil d'acceptabilité doivent être définis en amont de la prise de décision.
- En projet agile, les *Sprints* ne durant que quelques semaines, cette étape n'est pas nécessairement applicable.

BILAN DE PROJET SI

Bonne pratique n°7

Un bilan de fin de projet SI est réalisé et partagé.

CRITÈRE 1

Un bilan de projet est prévu et effectivement réalisé avec toutes les parties prenantes une fois que la phase de démarrage / rodage est terminée.

CRITÈRE 2

Ce bilan doit permettre de vérifier qu'il ne reste aucune tâche résiduelle (donc de coût supplémentaire) : désinstallations, décommissionnements, formations, etc.

CRITÈRE 3

Le bilan permet à tous les acteurs du projet de partager la même vision des coûts du projet, délais, respects des fonctionnalités annoncées.

CRITÈRE 4

Le bilan doit également permettre aux acteurs d'établir et de partager une compréhension commune des enseignements à tirer du projet.

- Exemples d'enseignements : difficultés rencontrées et erreurs à ne pas reproduire, acquis méthodologiques et autres, bonnes pratiques, etc.

NOTES...

RESSOURCES HUMAINES

ORGANISER ET MANAGER LES TALENTS ET LES COMPÉTENCES

ENJEUX POUR L'ENTREPRISE

1. Anticiper les besoins de l'entreprise en investissant sur les compétences qui permettront de réaliser les projets de demain.
2. Maintenir la motivation et l'employabilité des collaborateurs en valorisant leurs compétences.
3. Rendre attractifs les métiers SI et numériques de l'entreprise pour attirer de nouveaux talents.
4. Faire collaborer des personnes de générations et de compétences différentes pour garantir le fonctionnement et l'évolution du SI.

MENACES POUR L'ENTREPRISE

1. Démotiver le personnel de la filière SI et perdre des compétences du fait d'un *turnover* non maitrisé.
2. Ne pas pouvoir recruter les ressources dont l'entreprise a besoin.
3. Un vieillissement non maitrisé de la moyenne d'âge de la filière SI.
4. Une perte de compétitivité de l'entreprise.

ORGANISER ET MANAGER LES TALENTS ET LES COMPÉTENCES

FACTEURS DE RISQUES ASSOCIÉS

1. Inadéquation entre les objectifs et les projets de l'entreprise d'une part et l'évolution des ressources d'autre part.
2. Manque de connaissance et de pilotage des compétences des ressources.
3. Manque de connaissance des technologies et des modes d'organisation attractifs.
4. Absence d'arbitrage entre l'intérêt technologique (ce qui est attractif) et la pertinence pour l'entreprise, manque de communication autour des projets et modes d'organisation attractifs.
5. Manque d'accompagnement au changement des modes de fonctionnement et des différentes générations.

BONNES PRATIQUES

1. **OBJECTIFS DES RH**
   Objectifs des RH anticipant les futurs besoins de la DSI.
2. **RÉFÉRENTIEL**
   Référentiel des compétences formalisé.
3. **GESTION PRÉVISIONNELLE DES COMPÉTENCES**
   Gestion prévisionnelle des compétences en adéquation.
4. **ÉVALUATION**
   Réalisation de l'évaluation des compétences.
5. **RECRUTEMENT**
   Plan de recrutement pour répondre aux besoins SI.
6. **DÉVELOPPEMENT DES COMPÉTENCES**
   Offre de formation SI et numérique.

OBJECTIFS

Bonne pratique n°1

La gestion des ressources humaines SI doit permettre d'anticiper sur les futurs besoins de la DSI, développer les compétences internes et manager les talents.

CRITÈRE 1

Aligné sur la stratégie SI et en relation avec les règles RH de l'entreprise, un plan RH de la DSI est défini pour identifier les futurs besoins, le calendrier de disponibilité des ressources et les moyens mis en œuvre pour les acquérir (partenariat écoles, salons, approche directe, etc).

CRITÈRE 2

Une démarche de gestion des compétences SI est formalisée pour garantir le déploiement du plan RH de la DSI, l'évolution des compétences et son adéquation avec les besoins et pour contribuer à l'évolution du volet numérique du plan stratégique de l'entreprise.

CRITÈRE 3

Des bilans sur l'adéquation des ressources SI ainsi que l'élaboration de mesures correctives de la trajectoire sont régulièrement réalisés et présentés aux directions de la DSI et de la DRH.

CRITÈRE 4

En liaison avec sa démarche d'innovation, l'entreprise réalise une veille sur les compétences futures et l'anticipation de ses besoins.

- A titre d'exemple : *DevOps, Internet of Things*, Intelligence artificielle, *Data Science, Blockchain*, etc.

CRITÈRE 5

Une démarche en faveur de la féminisation des métiers du numérique a été engagée.

- Par exemple, les démarches **« FEMMES@NUMÉRIQUE »** (collectif d'associations, fondation d'entreprises et soutien de l'Etat) et **« SHE LEADS TECH »** (AFAI-ISACA).

RÉFÉRENTIEL

Bonne pratique n°2

Un référentiel des compétences requises est formalisé.

CRITÈRE 1

Un référentiel des emplois métiers SI et numériques est établi en cohérence avec les référentiels de la profession et est partagé avec les parties prenantes. L'identification des passerelles potentielles entre les catégories d'emplois est décrite.

- S'assurer que les métiers du numérique sont bien intégrés dans la démarche. Le référentiel des emplois métiers SI et numériques couvre également des emplois hors de la DSI.
- **CF. PUBLICATION DU CIGREF « NOMENCLATURE RH DES MÉTIERS DU NUMÉRIQUE »**

CRITÈRE 2

Des fiches de postes sont formalisées et rattachées à des emplois du référentiel. Lors du recrutement, ces fiches de postes sont diffusées et connues de l'ensemble des collaborateurs de la DSI.

- Chaque collaborateur doit avoir une fiche de poste qui repose sur le référentiel des métiers numériques.

CRITÈRE 3

Il existe une cartographie des métiers SI et numériques, comprenant les compétences nécessaires. Les postes critiques et/ou clés sont identifiés.

- La cartographie doit décrire fidèlement la situation existante.

CRITÈRE 4

Le référentiel est régulièrement maintenu en adéquation avec les bonnes pratiques de la place, les évolutions technologiques et la stratégie de l'entreprise.

GESTION PRÉVISIONNELLE DES COMPÉTENCES — Bonne pratique n°3

(GPEC/*Strategic workforce planning*). Un plan d'adéquation des compétences aux besoins actuels et futurs de l'entreprise est formalisé et mis en place.

CRITÈRE 1

Une analyse des écarts par rapport aux besoins exprimés est réalisée.

- En relation avec les volets RH et numérique du plan stratégique de l'entreprise (CF. BONNE PRATIQUE 1).
- Les besoins découlent du plan stratégique de l'entreprise.

CRITÈRE 2

La démarche compétences permet de détecter les compétences clés et les (hauts) potentiels incluant les emplois du numérique. La démarche compétences permet d'alimenter les plans de succession.

- Les résultats doivent être tracés, suivis et faire l'objet de plans d'action si besoin.

CRITÈRE 3

Un plan de résorption des écarts est réalisé, formalisé et mis en œuvre (formation, recrutement, partenariats fournisseurs et startups). La synthèse est présentée au comité de direction de la DSI.

- Le plan d'actions est comparé et ajusté avec les bonnes pratiques de la place.

CRITÈRE 4

La démarche de gestion des compétences alimente le prochain plan stratégique de l'entreprise.

- Ce critère est en lien avec le **VECTEUR 9 · PRESTATAIRES & FOURNISSEURS.**

CRITÈRE 5

Un plan de recrutement est défini et partagé avec la Direction des ressources humaines (DRH).

- Ce critère est en lien avec le **VECTEUR 9 · PRESTATAIRES & FOURNISSEURS**.

ÉVALUATION

Bonne pratique n°4

L'évaluation des compétences est réalisée.

CRITÈRE 1

Sur la base du référentiel des compétences, il existe un processus d'évaluation des compétences présentes dans la DSI.

- Le processus est fait une fois par an au minimum (par exemple lors de l'entretien annuel).

CRITÈRE 2

La DSI utilise les outils d'évaluation RH de l'entreprise dans le respect des contraintes réglementaires (sécurité, RGPD, etc.).

CRITÈRE 3

Le processus d'évaluation est suivi, fait l'objet d'indicateurs et, si besoin, d'un plan d'action.

- Vérifier que l'ensemble des collaborateurs a fait l'objet d'une évaluation au moins une fois dans l'année.

CRITÈRE 4

Un processus de capitalisation a été mis en place. La pertinence des indicateurs utilisés est analysée.

- Les résultats de cette analyse sont utilisés pour améliorer les processus d'évaluation des compétences de l'année N+1.

RECRUTEMENTS

Bonne pratique n°5

Un plan de recrutement est défini et mis en œuvre pour répondre aux besoins en ressources de la DSI.

CRITÈRE 1

En relation avec le *sourcing* fournisseur (**CF. VECTEUR 9 · PRESTATAIRES & FOURNISSEURS**) et les compétences actuelles de la DSI, un plan de recrutement est défini pour tenir compte des besoins actuels et futurs de la DSI.

CRITÈRE 2

Chaque poste à pourvoir est présenté de manière à le rendre attractif (description de l'entreprise et sa stratégie, activités à l'international, domaine de responsabilité du poste, etc).

CRITÈRE 3

Les postes à pourvoir sont systématiquement publiés en interne et les postulants sont reçus par les recruteurs. Un retour leur est systématiquement transmis.

CRITÈRE 4

Différents médias sont utilisés pour pourvoir les postes ouverts en externe (réseaux sociaux, cooptation, relations écoles et universités, relations écosystèmes, chasseurs de tête, etc.)

CRITÈRE 5

Des revues de comblement de postes sont régulièrement réalisées avec les directions SI et RH. Cela doit notamment permettre d'anticiper les délais de comblement de poste.

DÉVELOPPEMENT DES COMPÉTENCES — Bonne pratique n°6

Une offre de formation SI et numérique permet d'assurer l'adéquation des compétences aux besoins et de contribuer à garder les compétences en interne (attractivité de la DSI).

CRITÈRE 1

Une offre de formation est publiée et rendue visible à l'ensemble des collaborateurs.

- L'offre de formation doit être actualisée régulièrement (exemple : utilisation de MOOC, partenariats avec des écoles, etc.).

CRITÈRE 2

Le partage de compétences internes et la capitalisation des savoir-faire sont organisés.

- Approche *knowledge management*, réseaux sociaux d'entreprise, communautés thématiques, etc...

CRITÈRE 3

Le management doit veiller à ce que le plan de formation soit en adéquation avec les activités et les objectifs des collaborateurs.

- Les collaborateurs doivent pouvoir bénéficier de formations en lien avec leurs missions actuelles et futures.

CRITÈRE 4

L'efficacité de l'offre de formation est mesurée et formalisée.

- Formalisation de l'efficacité de l'offre de formation au niveau de la DSI. Evolution de l'offre de formation si besoin.

CRITÈRE 5

Les managers font un point régulier avec leurs collaborateurs sur leur montée en compétences.

- Réalisé dans le cadre de l'évaluation annuelle au minimum. Les managers font un point régulier avec leurs collaborateurs sur leur montée en compétences.

CRITÈRE 6

Un bilan annuel des formations est présenté à la DSI et à la DRH puis publié.

- Présentation aux partenaires sociaux.

PRESTATAIRES & FOURNISSEURS

PILOTER LES RELATIONS AVEC LES FOURNISSEURS DES SOLUTIONS ET SERVICES NUMÉRIQUES DE L'ENTREPRISE

ENJEUX POUR L'ENTREPRISE

1. Disposer d'un processus efficace et des éléments nécessaires pour décider du « faire ou faire faire » (« *make or buy* »)
2. Garantir une bonne gouvernance dans les phases de choix, de lancement, de suivi au quotidien et de clôture d'une activité externalisée.
3. Gérer efficacement la relation client/ fournisseur en associant toutes les parties prenantes (métiers, DSI, sous-traitants).
4. Acquérir les solutions adéquates pour accélerer le Time-to market des projets de l'entreprise, en tenant compte des ressources internes (RH, finance,...)

MENACES POUR L'ENTREPRISE

1. Perte de contrôle et dépendance vis-à-vis de certains fournisseurs.
2. Fuite d'informations à la concurrence.
3. Risques juridiques et financiers liés au pilotage des contrats d'externalisation.
4. Impacts sociaux dans l'entreprise liés à une mauvaise gestion des actions de l'externalisation.
5. Dégradation de l'image de l'entreprise.

PILOTER LES RELATIONS AVEC LES FOURNISSEURS DES SOLUTIONS ET SERVICES NUMÉRIQUES

FACTEURS DE RISQUES ASSOCIÉS

1. **Ne pas disposer des critères partagés permettant d'identifier et sélectionner les opportunités de « faire ou ne pas faire ».**
2. **Méconnaissance de l'écosystème des fournisseurs de solutions et de services numériques, manque de méthodologie dans le pilotage de la relation client/fournisseur.**

BONNES PRATIQUES

1. **STRATÉGIE ET GOUVERNANCE**
   Stratégie et gouvernance des services externalisés définies
2. **ETUDE**
   Etude d'opportunité et de faisabilité
3. **DÉMARCHE**
   Démarche incluant une transition et une conduite du changement
4. **GESTION**
   Gestion organisée et au quotidien des services
5. **CLÔTURE ET RÉVERSIBILITÉ**
   Définies en fonction des enjeux métiers
6. **RELATION FOURNISSEURS**
   Relation fournisseurs organisée et suivie

STRATÉGIE ET GOUVERNANCE — Bonne pratique n°1

Une stratégie de services externalisés et sa gouvernance associée ont été définies.

CRITÈRE 1

La stratégie d'externalisation SI inclut la politique « faire ou faire faire » (« *make or buy* »). La DSI évalue, avec les métiers, l'opportunité d'externaliser chacune des activités SI en fonction de la criticité des activités concernées, qui doit être validée au niveau hiérarchique approprié.

- Une telle évaluation :
  - Comprend la cartographie des activités de l'entreprise et les activités SI correspondantes (y compris *shadow IT*),
  - Conduit à passer au crible les critères suivants : alignement sur la stratégie métier, alignement sur la stratégie SI, maturité du marché et offres des prestataires, nécessités opérationnelles, nombre et qualité des compétences internes,
  - Impose des contraintes de confidentialité, de sécurité, réglementaires,
  - Prend en compte les risques sociaux, industriels et de dépendance vis-à-vis des prestataires, juridiques, financiers et d'image.

CRITÈRE 2

Un dispositif de management des services externalisés a été mis en place. Il inclut un volet de management des risques.

- Mise en place de l'organisation et des processus de services externalisés pour répondre aux besoins des métiers.
- L'exposition au risque et les mesures prises doivent être connues des métiers.
- Les risques suivants sont fréquemment étudiés : fiabilité/intégrité du tiers, confidentialité et protection des données, cybersécurité, conformité réglementaire, responsabilité sociétale de l'entreprise (RSE), éthique et développement durable, qualité et sûreté.

CRITÈRE 3

Une gestion des ressources humaines associée a été mise en place.

- Identifier les ressources clés (y compris nouvelles compétences) à maintenir au sein de l'organisation (exemples : *contract manager*, chef de projet expert dans le pilotage de la sous-traitance, architecte capable d'évaluer les propositions des sous-traitants). Vérifier que les rôles et responsabilités associés aux services externalisés ont été attribués. S'assurer que la gestion des emplois et compétences est bien en place (**CF. VECTEUR 8 · RESSOURCES HUMAINES**).

CRITÈRE 4

Des indicateurs ont été définis et mis en place pour mesurer la valeur apportée aux métiers lors d'une externalisation de services.

- Exemples de valeur apportée : gains financiers, vélocité, réduction des risques, etc...

CRITÈRE 5

La gestion du savoir a été organisée.

- Capitaliser et développer les connaissances relatives à la gestion des services externalisés pour :
  - piloter les contrats,
  - auditer les prestations achetées,
  - exercer la réversibilité des prestations (**Cf. bonne pratique 5**).

ÉTUDE

Bonne pratique n°2

Pour chacune des prestations candidates à l'externalisation, il y a eu une étude d'opportunité/faisabilité.

CRITÈRE 1

Concernant la prestation à externaliser, il existe des études de marché et d'identification de prestataires potentiels.

- Y compris des *benchmarks*.

CRITÈRE 2

Il existe une analyse des forces / faiblesses de l'existant.

- Analyse de la documentation, du niveau de compétence, de l'obsolescence du système, de la dette technique, etc.

CRITÈRE 3

Il existe un *business case* relatif à l'externalisation d'une activité.

- Objet, gains / coûts tangibles et intangibles : les incidences quantifiables et non quantifiables financièrement pour l'intégration, l'interopérabilité, la réversibilité des offres ainsi que les coûts supplémentaires liés au niveau de sécurisation à atteindre doivent être pris en compte.
- Le plan d'affaires doit également faire apparaître les gains générés au sein des métiers : éléments de comparaison pertinents (interne / externe) et estimation du ROI.

CRITÈRE 4

Il existe une analyse de risques concernant l'activité à externaliser.

- Les risques sont cartographiés (y compris ceux liés à la cybersécurité). Un plan d'atténuation des risques existe, mis en œuvre et est maintenu.
- Pour les offres cloud, les risques sont à différencier selon le degré de sensibilité des données concernées et selon qu'il s'agit de *cloud* public, de *cloud* privé externe, ou de *cloud* hybride. (**CF. VECTEUR 4 · DONNÉES**).

CRITÈRE 5

La décision d'externaliser une activité métier est prise par le métier en associant systématiquement la DSI. La décision d'externaliser une activité propre à la DSI est prise par la DSI en y associant les métiers.

- Sur la base du *business case* et de l'analyse de risques.

DÉMARCHE

Bonne pratique n°3

Pour chacune des activités SI à externaliser, une démarche incluant une transition et une conduite du changement est mise en place.

CRITÈRE 1

Pour l'activité à externaliser, les services concernés ont été clairement définis dans un cahier des charges (expression de besoin et exigences de résultat).

- Une validation formelle du cahier des charges a été effectuée par la direction métier et la DSI.

CRITÈRE 2

Une procédure, incluant des critères d'évaluation des fournisseurs, est construite parallèlement à l'élaboration du cahier des charges.

- Les critères d'évaluation doivent prendre en compte les différents risques de dépendance, de perte de contrôle, etc.

CRITÈRE 3

Le plan de transfert du service à un fournisseur a été défini et inclut les éventuels impacts RH (transferts du personnel au prestataire).

- A réaliser le plus tôt possible, avant le lancement de l'appel d'offres.

CRITÈRE 4

Un processus pour le transfert de connaissances et des données au prestataire a été défini.

- Le transfert de connaissances est formalisé (base documentaire, bonnes pratiques, etc.).
- Il est notamment indiqué dans le contrat que le fournisseur ne pourra utiliser les données de l'entreprise que dans le cadre de l'exécution du contrat.

CRITÈRE 5

Il existe dans le contrat d'externalisation une définition des engagements de sécurité à respecter par le fournisseur (notamment la rédaction d'un plan d'assurance sécurité par le fournisseur et validé par le client).

- Exemple : dans le cadre du recours au *cloud* et à l'utilisation des données de l'entreprise.

CRITÈRE 6

Il existe dans le contrat d'externalisation les éléments permettant de mesurer la qualité de la prestation fournie.

- Ces éléments contractuels recouvrent des aspects tels que la définition d'un *service level agreement (SLA)*, l'identification des obligations de moyens et de résultats, un *reporting* ainsi que les clauses d'audit.

CRITÈRE 7

L'élaboration du contrat et la capacité de le modifier durant son exécution sont le fruit de la collaboration entre toutes les parties prenantes (métier, DSI et fonctions achats et juridique).

- Un contrôle est effectué pour vérifier que toutes les parties prenantes ont été associées à l'élaboration du contrat. Le contrat doit rendre possible l'évolution de la prestation après accord des parties (clause de revoyure).

GESTION

Bonne pratique n°4

La gestion des services au quotidien est organisée.

CRITÈRE 1

Des points formalisés de gestion du service externalisé sont faits régulièrement avec le prestataire.

- Suite à une analyse des forces, faiblesses, risques et opportunités du contrat :
  - Des points de contrôle ont été définis (exemple : habilitation du personnel du prestataire) ;
  - Un dispositif de pilotage adapté est mis en place pour permettre une exécution au plus proche des termes du contrat (jalons contractuels, facturations, etc.) ainsi qu'un reporting associé.
- Il y a des comptes rendus systématiques après chaque point de gestion des services.

CRITÈRE 2

Des plans de résorption des écarts sont identifiés et mis en œuvre. Les contrôles suivis des incidents et des problèmes sont organisés avec le prestataire.

- Tout événement ou écart contractuel pouvant avoir un impact sur le planning, le montant du contrat (ou les coûts du projet) doivent faire l'objet d'une communication au niveau adapté pour permettre une prise de décision.

CRITÈRE 3

Il y a une revue périodique (au moins annuelle) du contrat avec toutes les parties prenantes (métiers, DSI, Direction achats). Un processus d'évolution des prestations a été défini, connu et partagé avec le prestataire.

- Les évolutions des prestations doivent s'inscrire dans le cadre du contrat.

CRITÈRE 4

Le dispositif prévoit un mode de prévention et de traitement des conflits potentiels grâce à :

- Un processus défini et connu, par les parties, pour le traitement des conflits ;
- Un glossaire pour accorder les différences de vocabulaire ;
- Un processus défini et connu pour réduire l'impact lié aux différences culturelles.

- C'est un réel besoin avec tous les prestataires et il est indispensable en cas d'*offshore*.

CRITÈRE 5

L'analyse de la valeur du service est effectuée à une fréquence appropriée (par rapport aux objectifs initiaux et à la durée du contrat). La décision de reconduire les services externalisés est instruite et prise avec le métier.

- Bilan des services externalisés.
- Réalisation des économies attendues (comparaison avec le plan d'affaires et le retour sur investissement initial).

CLÔTURE ET RÉVERSIBILITÉ — Bonne pratique n°5

La clôture du service et la gestion de la réversibilité ont été définies en fonction des enjeux métiers.

CRITÈRE 1

Une clause décrivant les modalités détaillées de clôture du service et de réversibilité ont été définies dans le contrat.

- Dès l'initialisation du projet, l'opérabilité de la réversibilité doit être étudiée, démontrée et définie dans les clauses contractuelles. La capacité à gérer une réversibilité d'un partenaire vers un autre fournisseur ou vers l'interne doit être vérifiée et préservée.
- Il faut mettre à jour les éléments permettant l'opération de réversibilité (à faire annuellement avec le prestataire).
- Une réversibilité intégrant la restitution des données propriété de l'entreprise et leur effacement en fin de contrat doit être prévue.

CRITÈRE 2

Le transfert des ressources du prestataire a été anticipé en fonction des évolutions du périmètre de la prestation.

- Voir les impacts RH dans le cadre d'une ré-internalisation.

CRITÈRE 3

Le Plan de Continuité des Activités (PCA) doit inclure les interdépendances de la prestation avec l'environnement SI de l'entreprise (interfaces, autres applications concernées, etc.)

- Un Plan de Continuité des Activités a été défini pour pallier les éventuelles défaillances lors de la phase de réversibilité.

CRITÈRE 4

Le processus de transfert de connaissances et des données a été défini.

- Dans le cadre du contrat, le plan de réversibilité fourni par le prestataire externe inclut :
  - La description des formations nécessaires pour que l'entreprise ou le repreneur puissent exploiter les données restituées (y compris la documentation),
  - L'assurance de la destruction des données une fois le transfert effectué.

CRITÈRE 5

Les modalités de clôture et de réversibilité sont revues régulièrement.

- Il faut notamment traiter de la récupération des données, de la documentation (procédures opérationnelles actualisése) et du matériel le cas échéant.
- Une fois par an, la DSI vérifie que le plan de réversibilité (incluant un mécanisme de récupération des données) est à jour. Des tests de réversibilité et des audits de réversibilité sont programmés et effectués périodiquement (périodicité définie dans le contrat).

RELATIONS FOURNISSEURS — Bonne pratique n°6

La gestion des fournisseurs de matériels et de logiciels est organisée et suivie.

CRITÈRE 1

La Direction des achats et la Direction juridique sont associées aux moments clés de l'acquisition de matériels et logiciels.

- Elles sont associées lors des différentes étapes, notamment : choix d'un fournisseur, contractualisation, revue avec le fournisseur, clôture du contrat, etc.

CRITÈRE 2

Dans le cadre des projets, les choix des fournisseurs de matériels et logiciels suivent les recommandations en matière d'urbanisme et d'architecture technique de l'entreprise (**CF. VECTEUR 5 · ARCHITECTURE**)

- Dans le cadre d'achat de matériels et logiciels, des points de validation technique doivent être mis en œuvre afin de s'assurer de leur cohérence avec l'existant.

CRITÈRE 3

Il existe une gestion du parc matériel.

- C'est a minima :
  - La gestion des configurations est régulièrement mise à jour,
  - L'inventaire du parc est réalisé une fois par an minimum,
  - La maintenance matérielle est optimisée,
  - Les sorties du parc matériel sont tracées.

CRITÈRE 4

Il existe une gestion des actifs logiciels.

- Des ressources sont allouées à cette fonction (*Software asset management*).
- C'est a minima :
  - L'inventaire du parc logiciel est tenu à jour et optimisé afin de veiller à ce que le nombre de licences acquises corresponde à l'utilisation (les écarts sont régularisés et la maintenance logicielle est optimisée),
  - Les sorties du parc logiciel sont tracées,
  - Il est nécessaire de gérer les licences afin de limiter le risque juridique.
- En 2018, le Cigref a publié le **« SOFTWARE ASSET AND CLOUD MANAGEMENT »**.

CRITÈRE 5

La gestion des versions (*versioning*) et l'anticipation de l'obsolescence des matériels et logiciels sont organisées.

- Un processus de montée de version existe et les fournisseurs sont associés lorsque l'opération est jugée critique.

SERVICES

FOURNIR DES SERVICES NUMÉRIQUES CONFORMES AUX ATTENTES CLIENTS

ENJEUX POUR L'ENTREPRISE

1. Connaitre les besoins des métiers et leur évolution.
2. Garantir un niveau de service conforme aux besoins des métiers prenant en compte les contraintes budgétaires.
3. Proposer un catalogue de services répondant à l'évolution des besoins des clients ou des utilisateurs.

MENACES POUR L'ENTREPRISE

1. Non-alignement des services rendus par rapport aux besoins des métiers et des collaborateurs.
2. Allocation inadaptée de ressources (sur ou sous allocation) entrainant à une perte de compétitivité des fonctions opérationnelles mal servies.
3. Dégrader le fonctionnement des processus métiers notamment en termes de disponibilité, d'intégrité et de confidentialité.

FOURNIR DES SERVICES NUMÉRIQUES CONFORMES AUX ATTENTES CLIENTS

FACTEURS DE RISQUES ASSOCIÉS

1. **Manque de communication avec les métiers et le COMEX se traduisant par une méconnaissance de leurs besoins.**
2. **Manque de compréhension et de réactivité au regard de l'évolution des besoins des métiers.**
3. **Absence de processus structuré et de méthodologie permettant de délivrer avec le niveau d'efficacité attendu.**

BONNES PRATIQUES

1. **CATALOGUE DE SERVICES CLIENT SI**
   Catalogue de services client SI proposé et clair.
2. **DEMANDE CLIENT**
   Gestion de la demande client mise en place sur les services existants.
3. **CONTRATS DE SERVICE**
   Contrats de service mis en place et gérés.
4. **AMÉLIORATION CONTINUE DES SERVICES**
   Amélioration continue de la qualité de services perçue par les utilisateurs.
5. **ACTIVITÉ DE PRODUCTION**
   Activité de production pilotée à l'aide de tableaux de bord.

CATALOGUE

Bonne pratique n°1

La DSI a mis en place un catalogue de services client.

CRITÈRE 1

Le catalogue de services a été établi avec les clients.

- La DSI co-construit le catalogue de services avec ses clients.

CRITÈRE 2

Le catalogue présente les services et les unités d'œuvre (UO) pour les quantifier.

- Cette description doit être intelligible et concertée avec le client.

CRITÈRE 3

Le catalogue de services fait l'objet d'une actualisation régulière.

- Cette actualisation doit être effectuée en collaboration ou concertation avec le client.

CRITÈRE 4

Les éléments constituant la structure de coût de chaque service sont connus, suivis et leur évolution est régulièrement communiquée aux clients.

- Ce critère fait le lien avec le **VECTEUR 11 · BUDGET & PERFORMANCE**.
- La qualité de cette communication est un élément clé dans une relation contractuelle interne.

CRITÈRE 5

La DSI est capable de relier les services délivrés et les processus métiers auxquels ils se rattachent.

- Il s'agit ici de co-constuire une cartographie - éventuellement simplifiée - des processus et services associés avec le client.

DEMANDE CLIENT

Bonne pratique n°2

La DSI a mis en place un processus de gestion de la demande client sur les services existants (*run*).

CRITÈRE 1

La DSI rencontre régulièrement ses clients pour identifier et actualiser leurs besoins et attentes.

- La fréquence minimale de ces rencontres est au moins deux fois par an.

CRITÈRE 2

Les métiers ont une vision claire des services qui leur sont délivrés.

- Les métiers vérifient que les services délivrés correspondent bien au SLA (*service level agreement*) et ont une vision des services rendus de bout en bout.

CRITÈRE 3

Les métiers ont une vision documentée du coût de chaque service.

- La sensibilisation des métiers clients aux coûts de service leur permet de mieux comprendre la valeur ajoutée du service.

CRITÈRE 4

La DSI réalise des benchmarks lui permettant de comparer son offre de services à celle d'autres entreprises du même secteur d'activité et de taille comparable, voire même à l'offre de prestataires externes.

- Ce critère fait le lien avec le **VECTEUR 11 · BUDGET & PERFORMANCE**.
- Dans les faits, il s'agit de questionner la capacité de la DSI à maîtriser ses coûts et à les auto-évaluer.
- Le Cigref a publié la mise à jour du rapport **« MODÈLE D'ANALYSE ET DE BENCHMARKING DES COÛTS INFORMATIQUES »** en août 2018.

CONTRAT — Bonne pratique n°3

La DSI a mis en place des contrats de service.

CRITÈRE 1

Les services délivrés à une fonction de l'entreprise ou à un processus particulier, sont regroupés dans un contrat de service entre la DSI et l'entité concernée.

- La DSI a notamment défini avec les utilisateurs dans ses contrats de services la durée d'interruption acceptable et le processus de décision de passage en mode dégradé, en cas d'interruption prolongée. On doit s'assurer que le contrat de service est en cohérence avec la gestion de crise et les plans de continuité d'activités (PCA) et de reprise d'activités (PRA).
- Ce critère est en lien avec le **CRITÈRE 3 DE LA BONNE PRATIQUE 5 DE CE VECTEUR.**

CRITÈRE 2

Les contrats de service sont rédigés avec les métiers et font formellement apparaitre les accords respectifs. Leur formulation est intelligible par les deux parties.

- Il s'agit de formaliser un accord de collaboration où chacun connait les enjeux de l'autre et accepte ses contraintes.

CRITÈRE 3

Le contrat fait figurer l'objectif et les attentes du client ainsi que les devoirs et obligations de chaque partie prenante.

- La prise en compte des aspects règlementaires est à intégrer également.

CRITÈRE 4

Le contrat est régulièrement actualisé, tant en termes de type de services que de structure de coûts.

CRITÈRE 5

Des indicateurs de suivi sont définis et font l'objet d'un *reporting* et d'échanges réguliers et formalisés avec les métiers.

- Le tableau de bord lié au contrat permet d'assurer une communication permanente avec le client. Sa fréquence est adaptée au service et doit être régulière pour être un véritable outil de pilotage conjoint.

AMÉLIORATION

Bonne pratique n°4

La DSI a mis en place un processus d'amélioration continue basé sur la qualité perçue par l'utilisateur.

CRITÈRE 1

La DSI a mis en place des outils de mesure du bon fonctionnement et de la performance de ses services, avec un processus de collecte des réclamations et incidents relatifs aux services délivrés aux clients.

- La collecte des réclamations est le point de départ du processus d'amélioration continue.

CRITÈRE 2

Les réclamations/incidents remontés et les écarts constatés par rapport aux engagements, font l'objet d'analyses régulières et de dispositifs de résolution réduisant leurs occurrences futures.

CRITÈRE 3

Un tableau de bord de suivi de la qualité de services est établi à partir des indicateurs mentionnés au contrat de service (performance, résolutions d'incidents…).

- Les indicateurs sont communiqués à travers des tableaux de bord diffusés aux acteurs responsables de la DSI et aux clients concernés.

CRITÈRE 4

La DSI ou un tiers réalise régulièrement des enquêtes de satisfaction auprès de ses clients (ex : NPS, *net promoter score*)

- De préférence, ces enquêtes doivent être réalisées par un tiers.
- Les tableaux de bord et enquêtes sont à partager avec les instances clients.

CRITÈRE 5

Les indicateurs de qualité mesurée et les enquêtes de satisfaction participent à l'évolution des contrats de services.

- Les points d'amélioration issus de l'enquête de satisfaction sont à discuter avec le métier de manière à adapter les contrats de service.

CRITÈRE 6

La DSI valorise la mise en œuvre d'approches innovantes dans la délivrance de ses services et intègre les avantages procurés par les innovations les plus significatives.

- L'innovation est intégrée dans le processus d'amélioration continue. Des challenges innovation ou hackathons peuvent être co-initiés de manière à améliorer les services ou créer de nouveaux services. Les clients peuvent être sollicités pour tester des idées innovantes.

PRODUCTION

Bonne pratique n°5

La DSI pilote ses activités de production et de support à l'aide d'un tableau de bord.

CRITÈRE 1

La DSI a mis en place des ressources et des outils pour gérer et superviser la production, les changements, les configurations, les incidents et les problèmes, les données, les environnements, etc.

- La DSI a décrit son organisation et cartographié ses processus internes dans ces domaines. Elle doit pouvoir justifier du pilotage de ses activités au travers de tableaux de bord ou indicateurs ou instances de pilotage. Par ailleurs, elle s'assure de se conformer aux certifications obligatoires de son secteur.

CRITÈRE 2

La DSI maîtrise les travaux programmés et les interruptions prévisibles de services.

- La DSI est capable d'analyser l'impact des dégradations de performance ou des interruptions de services sur les activités de ses clients. Les travaux programmés sont convenus avec le métier.

CRITÈRE 3

La DSI communique efficacement avec ses clients en cas d'incident.

- La DSI a une connaissance actualisée des organisations et réseaux d'utilisateurs potentiellement impactés par l'incident. Les moyens de communication doivent être adaptés au type d'incident.

NOTES...

BUDGET & PERFORMANCE

PILOTER LE BUDGET ET LA PERFORMANCE DU SI

ENJEUX POUR L'ENTREPRISE

1. Aligner les objectifs de performance du SI sur les objectifs de l'entreprise.
2. Assurer l'atteinte des objectifs de performance du SI en gérant la meilleure allocation des ressources au meilleur coût.
3. Maîtriser le budget du SI (fonctionnement récurrent et projets).
4. Associer les différentes parties prenantes (COMEX, métiers, DSI) à la gestion du SI grâce à un processus de communication sur la performance du SI.

MENACES POUR L'ENTREPRISE

1. Prendre de mauvaises décisions par manque de maîtrise de l'ensemble des éléments de coûts.
2. Ne pas maîtriser les facteurs de « dérapage » des projets.
3. Générer une incompréhension entre la Direction générale, la Direction financière, les directions métiers et la DSI sur l'évolution du budget SI et des coûts des prestations fournies par la DSI à ses clients, ce qui peut se traduire par une perte de confiance préjudiciable à l'atteinte des objectifs de l'entreprise.

PILOTER LE BUDGET ET LA PERFORMANCE DU SI

FACTEURS DE RISQUES ASSOCIÉS

1. **Méconnaissance des objectifs de l'entreprise et des attentes des métiers.**
2. **Manque de compréhension sur la contribution du SI aux objectifs de l'entreprise.**
3. **Absence de *roadmap IT* et de gestion du portefeuille de projets.**
4. **Absence de processus structuré de suivi de la performance et du budget du SI.**
5. **Manque de culture économique et de compétences en contrôle de gestion du SI.**

BONNES PRATIQUES

1. **OBJECTIFS DE PERFORMANCE SI**
   Objectifs de performance SI alignés avec ceux de l'entreprise.
2. **INDICATEURS**
   Indicateurs sur la mesure de la performance et l'atteinte des objectifs.
3. **BUDGET**
   Budget géré avec un processus d'arbitrage de la DG.
4. **COÛTS COMPLETS DES SERVICES**
   Coûts complets des services calculés pour co-responsabiliser les métiers.
5. **PROJETS**
   Projets suivis selon les coûts, délais et fonctionnalités.

OBJECTIFS DE PERFORMANCE

Bonne pratique n°1

Le pilotage de la DSI s'appuie sur l'ensemble des objectifs de performance du SI alignés avec ceux de l'entreprise.

CRITÈRE 1

La DSI a défini ses objectifs prioritaires en mettant en évidence leur contribution à ceux de l'entreprise (**CF. VECTEUR 1 · STRATÉGIE**) et en structurant selon les six volets de l'***IT SCORECARD*** définis par l'AFAI :

1 - Contribution à la création de valeur métier

2 - Maîtrise des risques liés au SI

3 - Prise en compte des attentes des clients du SI

4 - Performance des processus informatiques (*build, run*, évolutions)

5 - Maîtrise des coûts des services fournis par l'informatique à ses clients

6 - Gestion des compétences informatiques et préparation du futur

CRITÈRE 2

Les objectifs de la DSI sont communiqués à toutes les parties prenantes (collaborateurs DSI, clients internes ou externes, comité de direction des autres directions, COMEX, partenaires, etc.).

- Les objectifs doivent être SMART (Simples, Mesurables, Atteignables, Réalistes et avec une Temporalité).
- Les objectifs sont documentés pour être compris par toutes les parties prenantes.
- Certains objectifs peuvent être issus des exigences de certifications externes (ISO 9001, ISO 2700x, etc.).

CRITÈRE 3

Les objectifs sont revus au moins annuellement à partir des mesures observées, de leur niveau d'atteinte et de la stratégie de l'entreprise.

INDICATEURS — Bonne pratique n°2

Des indicateurs de mesure de la performance du SI et le niveau d'atteinte des objectifs de la DSI sont définis, suivis et partagés régulièrement avec les parties prenantes.

CRITÈRE 1

Des indicateurs de mesure de la performance (quantitatifs et qualitatifs) sont formalisés dans des tableaux de bord. Ils permettent de mesurer le niveau d'atteinte des objectifs de la DSI (Cf. bonne pratique 1).

- L'**IT SCORECARD** publié par l'AFAI peut être utilisé pour trouver des exemples d'indicateurs.
- Ces indicateurs sont formellement définis. Pour les aspects quantitatifs, les données servant à la mesure de l'indicateur doivent être extraites, si possible, de façon automatisée du SI existant.

CRITÈRE 2

Des objectifs d'amélioration sont associés aux indicateurs de mesure de la performance.

- Les engagements de service négociés avec les métiers sont mesurés par ces indicateurs.

CRITÈRE 3

Des moyens de mesure et de contrôle de l'atteinte des objectifs (définition d'indicateurs, mesures régulières) sont en place au niveau de la DSI.

- La DSI analyse les résultats de ces indicateurs et leur écart par rapport aux objectifs afin de mettre en œuvre les actions correctives éventuelles.

CRITÈRE 4

Les indicateurs de mesure de la performance sont revus et mis à jour, si nécessaire (changements de stratégie ou d'objectifs de l'entreprise ou de la DSI) afin de permettre des améliorations de la mesure de la performance.

- Les règles de gestion des indicateurs doivent résulter de règles de gestion communes et partagées.

CRITÈRE 5

Les indicateurs de performance sont consolidés dans des tableaux de bord qui sont partagés régulièrement avec les parties prenantes et la Direction générale dans un format adapté en faisant apparaitre la contribution de chacun.

- Dans un but de transparence et d'amélioration de la communication, la DSI publie et partage périodiquement avec les parties prenantes et la Direction générale des tableaux de bord restituant de façon synthétique les niveaux et les tendances de ces indicateurs.
- La publication doit être faite « au fil de l'eau » pour donner une vision la plus à jour possible de la performance.
- Ces tableaux de bord peuvent être également partagés avec les collaborateurs de la DSI à des fins de management.

BUDGET

Bonne pratique n°3

La DSI met en œuvre un processus de gestion budgétaire permettant de gérer les arbitrages avec la Direction générale et les directions métiers relatifs aux projets, aux évolutions et au fonctionnement récurrent.

CRITÈRE 1

Un budget consolidant l'ensemble des coûts de la filière SI existe.

- Ce budget consolide non seulement les coûts placés sous la responsabilité de la DSI, mais aussi ceux d'entités ou correspondants informatiques rattachés à des directions opérationnelles ou fonctionnelles.

CRITÈRE 2

Le budget de la filière SI est construit sur la base de natures de dépenses adaptées à l'informatique, et de centres de responsabilité.

- Le **MODÈLE D'ANALYSE ET DE BENCHMARKING DES COÛTS INFORMATIQUES** du Cigref indique la liste des natures de dépenses à prendre en compte (y compris amortissements, locaux, ...).
- Les centres affectés à des responsables du SI doivent regrouper l'ensemble des dépenses dont ils ont l'initiative.
- Des frais répartis (structure, locaux, ...) peuvent également figurer dans les centres de responsabilité afin d'obtenir un coût complet des activités des centres, mais ils doivent être bien différenciés des dépenses directes.

CRITÈRE 3

Le budget de la filière SI permet d'identifier les ressources allouées aux projets (transformation), à la maintenance évolutive et aux autres coûts récurrents, en particulier la production informatique.

- Cette distinction en 3 parties au moins est essentielle car chacune se pilote selon un mode différent :
  - Pour les projets, il s'agit d'un investissement qui doit être « rentable » pour l'entreprise.
  - Quant au récurrent, on est plus proche d'une « usine », (placée sous la responsabilité hiérarchique ou fonctionnelle de la DSI) de production de services dont les coûts doivent être optimisés.
  - Les évolutions, quant à elles, doivent être encadrées par un budget négocié par domaine applicatif.

CRITÈRE 4

Le processus d'élaboration budgétaire de la DSI est formalisé. Les rôles et responsabilités du processus budgétaire sont formellement attribués (élaboration, suivi des écarts, mises à jour, ...). Il existe un processus d'arbitrage clairement défini.

- Pour faire fonctionner ce processus, la mise en place d'un contrôle de gestion de l'informatique est recommandée.
- Ce contrôle de gestion contribuera à l'élaboration du budget et à ses révisions, suit les réalisations par centres et natures de dépenses en les comparant à la fois au Budget et aux réalisations des années précédentes.
- Pour pouvoir anticiper d'éventuels dérapages, le suivi des dépenses se fera aussi « à l'engagement ».

COÛTS DES SERVICES

Bonne pratique n°4

La DSI calcule le coût complet des prestations du catalogue de services fournis à ses clients en le décomposant en coûts unitaires et volumes pour co-responsabiliser les métiers sur les coûts SI.

CRITÈRE 1

Un catalogue de services clients a été défini en relation avec les clients de la DSI et couvre la totalité des prestations fournies.

- Ce catalogue est orienté clients (lisible et compréhensible par le métier).
- Il comprend la mise à disposition des postes de travail, des applications, ainsi que la réalisation des évolutions et des projets.
- Il peut comprendre également des prestations telles que conseil, expertise …
- Il se situe à un niveau auquel il est possible de prendre des engagements de type *SLA*.

CRITÈRE 2

La DSI a identifié l'ensemble de ses activités.

- Le **MODÈLE D'ANALYSE ET DE BENCHMARKING DES COÛTS INFORMATIQUES** fournit une liste type d'activités qu'on retrouve peu ou prou dans toutes les DSI.

CRITÈRE 3

Le coût unitaire des services fournis aux clients de l'informatique est calculé avec une méthode reconnue de type *Activity Based Costing* (ABC), qui doit permettre d'expliquer clairement ses évolutions et de les piloter.

- Le calcul de coûts unitaires justifiables, par application de la méthode ABC, doit permettre de :
  - Se poser, avec les clients de la DSI, des questions du type : coût des exigences en matière de *SLA*, décommissionnement éventuel de certaines applications sur la base d'un coût par utilisateur,
  - Facturer aux clients de la DSI le coût des services,
  - Faciliter la réalisation de *benchmarking*,
  - Mettre en évidence la productivité de la DSI (évolution du coût unitaire par inducteur des services fournis)
- Pour cela, il faut que les managers de la DSI comprennent leur contribution au coût complet des services fournis afin de pouvoir les piloter en agissant sur les leviers d'action dont ils ont la responsabilité.

PROJETS — Bonne pratique n°5

Pour les aspects coûts, délais et fonctionnalités livrées, la DSI a mis en place, pour chaque projet, un suivi des activités sous son contrôle impactant le *business case*.

CRITÈRE 1

Le suivi économique des projets est articulé avec la gestion opérationnelle des projets.

- Idéalement, le suivi opérationnel et le suivi économique s'appuient sur un outil de suivi partagé ou « *a minima* » sur un référentiel partagé.

CRITÈRE 2

Une consolidation du suivi des coûts, délais et fonctionnalités livrées est articulée avec la gestion du portefeuille de projets (**CF. VECTEUR 6 · PORTEFEUILLE DE PROJETS**).

CRITÈRE 3

Un tableau de bord de suivi des projets existe et est partagé avec les directions métiers concernées.

CRITÈRE 4

Les écarts entre réalisation et prévision sont remontés aux instances de pilotage et pour les projets stratégiques au COMEX.

CRITÈRE 5

Le *business case* fait l'objet d'une mise à jour si les écarts constatés la justifient.

NOTES...

MARKETING & COMMUNICATION

VALORISER LES SERVICES ET COMMUNIQUER SUR LES ENJEUX TECHNOLOGIQUES ET EN SITUATION DE CRISE

ENJEUX POUR L'ENTREPRISE

1. Faire évoluer l'image de la DSI, comme étant un acteur stratégique à forte valeur ajoutée.
2. Donner de la transparence sur la performance du SI afin de favoriser la connaissance des enjeux et chantiers de la DSI pour les métiers.
3. Faciliter l'adhésion des collaborateurs dans les plans de transformation numérique.
4. Anticiper et être en mesure de communiquer en situation de crise.

MENACES POUR L'ENTREPRISE

1. Manque de transparence et perte d'information pouvant favoriser le *Shadow IT* et dégrader l'image de la DSI auprès des clients internes.
2. Effet négatif de la « boite noire » ou « tour d'ivoire » vis-à-vis des utilisateurs finaux.
3. Manque d'attractivité pour les talents à rejoindre la DSI et l'entreprise.

VALORISER LES SERVICES ET COMMUNIQUER SUR LES ENJEUX TECHNOLOGIQUES ET EN SITUATION DE CRISE

FACTEURS DE RISQUES ASSOCIÉS

1. **Méconnaissance de la stratégie de l'entreprise, et non-alignement de la stratégie du SI avec celle de l'entreprise.**
2. **Absence de processus de communication avec les métiers.**
3. **Sous-estimation de l'impact culturel des projets de transformation.**
4. **Absence de processus de communication et de méthodologie de gestion des crises.**

BONNES PRATIQUES

1. **FONCTION MARKETING DE LA DSI**
   Fonction marketing de la DSI organisée et orientée clients du SI.
2. **PLAN DE COMMUNICATION**
   Plan de communication formalisé et partagé.
3. **COMMUNICATION INTERNE DE LA DSI**
   Communication interne de la DSI.
4. **COMMUNICATION INTERNE À L'ENTREPRISE**
   Communication interne à l'entreprise.
5. **COMMUNICATION EN SITUATION DE CRISE**
   Communication en situation de crise anticipée

FONCTION MARKETING DE LA DSI

Bonne pratique n°1

La DSI organise le marketing de ses services auprès de ses clients.

CRITÈRE 1

La fonction marketing de la DSI existe et met en place une stratégie de communication structurée.

- Des « clubs utilisateurs » et des événements autour des projets/services de la DSI sont organisés et animés.
- Les projets SI sont accompagnés dans la conduite du changement et dans leur communication opérationnelle vers les utilisateurs.

CRITÈRE 2

La fonction marketing de la DSI construit une relation avec les clients de la DSI.

- Elle est responsable de la relation avec les clients de la DSI.
- Elle a une connaissance précise des besoins des utilisateurs des services de la DSI.
- Elle mesure régulièrement et améliore la satisfaction des clients et des utilisateurs du SI (enquêtes utilisateurs, enquête à chaud support, etc.)
- Elle développe la connaissance clients et utilisateurs (bases de connaissances clients et utilisateurs, segmentations, profilage, etc.).

CRITÈRE 3

La fonction marketing de la DSI définit, valorise, rationalise et commercialise/publie l'offre de services de la DSI.

- L'offre de services et le catalogue de services de la DSI sont valorisés auprès des utilisateurs. (**CF. VECTEUR 10 · SERVICES**).

CRITÈRE 4

La fonction marketing de la DSI gère la satisfaction des clients et utilisateurs.

- La qualité de service et l'expérience client sont valorisées auprès des clients et utilisateurs (satisfaction, respect des SLAs, communication incidents, etc).
- Le développement de projets *SLAs*, la définition et le suivi des engagements de services et la publication de la « météo des services » (*monitoring*) peuvent être mis en place.

CRITÈRE 5

Des indicateurs de performance du marketing de la DSI sont définis.

- Exemples : indice de satisfaction client, nombre d'événements clients et utilisateurs organisés, taux d'adhésion aux nouveaux services.

PLAN DE COMMUNICATION

Bonne pratique n°2

La DSI communique selon un plan de communication formalisé, structuré et partagé.

CRITÈRE 1

Le plan de communication du SI est un aspect important de la stratégie de la DSI.

- La DSI doit intégrer les problématiques liées au sujet de la communication du SI comme un élément obligatoire et l'inscrire à son agenda.
- Ce critère est en lien avec le **VECTEUR 1 · STRATÉGIE**.

CRITÈRE 2

Une communication dédiée au SI est définie et matérialisée au sein d'un plan de communication de la DSI. Les tableaux de bord montrant la performance du SI sont utilisés comme outil de communication et leur contenu est adapté en fonction de la population cible.

- Le plan de communication SI est partagé avec la Direction de la communication de l'entreprise.

CRITÈRE 3

Le plan de communication est validé par le *top management,* diffusé et fait l'objet d'une actualisation une fois par an.

- Une réunion annuelle est organisée en présence du *top management* durant laquelle le plan de communication est validé et mis à jour lorsque nécessaire.

CRITÈRE 4

Le plan de communication identifie et segmente toutes les populations avec qui la DSI communique.

- Par exemple : collaborateurs, chefs de projets, acteurs de la DSI, autres acteurs de l'entreprise incluant la Direction générale, utilisateurs finaux, etc.

CRITÈRE 5

Le plan de communication de la DSI est aligné avec la stratégie de communication globale et stratégique de l'entreprise et notamment prend en compte les notions d'innovation et de risque cyber.

- La communication du SI ne doit pas entrer en conflit avec la stratégie de communication globale de l'entreprise et doit être cohérente afin de ne pas être contre-productive.

CRITÈRE 6

La communication de crise tient une part privilégiée dans le plan de communication et est proportionnée aux risques.

- Les situations de crise donnent lieu à une communication particulière et exceptionnelle qui doit être étudiée avec les équipes de communication de crise de l'entreprise, et recevoir un accompagnement dédié.
- Les scénarios doivent être anticipés et faire l'objet d'exercices réguliers mobilisant la totalité des acteurs de la DSI.

CRITÈRE 7

Des actions sont mises en place régulièrement afin de mesurer l'impact et l'efficacité de la communication et ces résultats sont utilisés dans la mise à jour du plan de communication.

- Des retours d'expérience permettent d'améliorer la communication.

COMMUNICATION INTERNE À LA DSI — Bonne pratique n°3

La communication au sein de la DSI est organisée et régulière.

CRITÈRE 1

Des actions de communication en interne à la DSI ont été définies.

- Sensibilisation des collaborateurs internes à la DSI *via* des canaux de communication internes classiques, *newsletters*, e-mails, intranet, réseau social d'entreprise (RSE), sur des sujets sur lesquels ils doivent être à jour : régulation etc.

CRITÈRE 2

La communication prend la forme d'une diffusion de l'information aux correspondants des différentes fonctions du SI. Elle doit être proactive et qualitative.

- La communication se veut extra-transactionnelle et va au-delà de la communication des chiffres liés à la résolution d'incidents par exemple.
- La communication est proactive car elle ne doit pas seulement avoir lieu en temps d'interruption de service ou de crise.

CRITÈRE 3

Différents canaux de communication sont identifiés et utilisés en fonction de la typologie de communication et de la population cible, en privilégiant les canaux de communication interne habituels de l'entreprise.

- Exemples : E-mails, SMS, affichages, *flyers*, vidéos, intranet, RSE, etc.

CRITÈRE 4

La communication prend la forme d'un engagement des différentes fonctions du SI en utilisant des formats présentiels, qui permettent une communication orale et individuelle.

- Exemples : échanges, face à face, présentations, ateliers, *roadshow* du management de la DSI, etc.

CRITÈRE 5

Les responsables des différentes fonctions du SI sont associés à la conception, à la réalisation et à la diffusion de la communication. La communication interne de la fonction SI intègre les objectifs stratégiques des clients internes.

CRITÈRE 6

L'impact de la communication vers les différentes fonctions du SI est périodiquement analysé et amélioré.

- Des moyens, tels que des enquêtes de satisfaction, peuvent être utilisés.

COMMUNICATION INTERNE À L'ENTREPRISE — Bonne pratique n°4

La communication de la DSI vers les autres acteurs de l'entreprise est réalisée de manière organisée et régulière.

CRITÈRE 1

Des actions de communication vers les acteurs externes à la DSI ont été définies.

- Les acteurs externes à la DSI sont les métiers, la Direction générale, etc.

CRITÈRE 2

La communication prend la forme d'une diffusion de l'information aux directions de l'entreprise. Elle doit être proactive et qualitative.

- La communication prend la forme de partage des usages, des pratiques sur la sécurité et la cybersécurité notamment en ce qui concerne les réseaux sociaux, une aide à l'appréhension des nouvelles technologies et des nouvelles législations (Ex : GDPR).
- La communication se veut extra-transactionnelle et va au-delà de la communication des chiffres liés à la résolution d'incidents par exemple.
- La communication est proactive car elle ne doit pas seulement avoir lieu en temps d'interruption de service ou de crise.

CRITÈRE 3

Différents canaux sont identifiés et utilisés en fonction de la typologie de communication et de la population cible.

- Exemples : emails, *newsletter*, écrans TV, etc.

CRITÈRE 4

La communication prend la forme d'un engagement des différentes fonctions du SI sensibilisées à leur rôle d'ambassadeur et de garant de l'image de la DSI envers les autres parties prenantes, en utilisant des moyens qui permettent une communication orale et individuelle.

- Exemples : conférences présentielles, face à face, présentations, ateliers, *roadshow* du management de la DSI, etc.

CRITÈRE 5

Les différents correspondants du SI sont associés à la conception, à la réalisation et à la diffusion de la communication. La communication intègre les objectifs stratégiques des parties prenantes.

CRITÈRE 6

L'impact de la communication du SI est périodiquement analysé et amélioré.

- Des moyens tels que des enquêtes de satisfaction peuvent être utilisés.
- La prise en compte de l'innovation et du risque cyber peut déclencher une mise à jour de cette communication

CRITÈRE 7

La DSI communique sur sa contribution à la politique RSE de l'entreprise (mixité, handicap, environnement, énergie, etc.)

SITUATION DE CRISE — Bonne pratique n°5

Une communication en cas de crise SI est formalisée et partagée en amont afin d'anticiper.

CRITÈRE 1

Une communication de crise liée au SI s'appuie sur une procédure associée. La communication de crise doit prendre en compte l'importance et la célérité des attaques cyber.

- Par crise, il est entendu toute situation exceptionnelle pouvant représenter un réel risque au bon fonctionnement du SI ou de l'entreprise.
- Compte tenu de la vitesse de l'impact potentiel en cas de cyberattaque il convient d'avoir mené une réflexion sur la vitesse de réaction.
- La diffusion des incidents hors de l'entreprise est réalisée selon les règles établies.
- Ce critère et cette bonne pratique sont en lien avec le **VECTEUR 3 · RISQUES**.

CRITÈRE 2

Les risques majeurs pouvant amener à une situation de crise sont identifiés et font l'objet d'une coordination cohérente de la communication de crise entre les différents acteurs (SI, fonctionnels, opérationnels, dirigeants).

- Exemples : interruption des services internet, intrusion dans le SI, phishing, etc.

CRITÈRE 3

La communication de crise est validée et diffusée aux acteurs et/ou aux entités de l'entreprise.

CRITÈRE 4

Des outils et/ou des ressources, assurant une communication valable en temps de crise entre acteurs, ont été définis.

- Afin de rendre la communication la plus efficiente possible, des outils et ressources adaptés sont identifiés.

CRITÈRE 5

Des exercices de communication de crise sont régulièrement effectués.

- Des situations de crise peuvent être simulées afin de tester la maturité de l'organisation à communiquer en situation de crise.

CRITÈRE 6

Un retour d'expérience est pratiqué pour tirer les enseignements et améliorer la réaction.

- Un des objectifs : pratiquer l'amélioration continue sur la procédure de gestion de crise.

BIBLIOGRAPHIE

POUR ALLER PLUS LOIN...

Référentiels

- COBIT2019 / AFAI-ISACA
- COBIT5 for risk / AFAI-ISACA
- COBIT5 for security/ AFAI-ISACA
- Risk IT Framework / AFAI-ISACA
- ITIL Version 3 / ITIL Foundation
- GTAGs – Global Technology Audit Guides / IIA

Gouvernance / Stratégie

- Agile at scale / Cigref – 2018
- Ethique et numérique / Cigref - 2018
- Open Innovation, réponse aux challenges de l'entreprise / Cigref - 2018
- Entreprise, les clés d'une application réussie du GDPR / AFAI-ISACA, Cigref, TECH IN France - 2017
- Gouvernance du numérique / Cigref - 2014
- Le pilotage du SI par l'entreprise - Nouveaux tableaux de bord de l'IT Scorecard / AFAI-ISACA- 2011

Risques

- Cyber-risques : Enjeux,approches et gouvernance / IFACI – 2018
- Cybersécurité, Visualiser,comprendre et decider / Cigref - 2018
- Enquête « Risk in focus » / IFACI – 2018
- L'entreprise face à ses enjeux et risques numériques / AFAI-ISACA, Cigref, Crowe Horwath, IFACI - 2015

Système d'information

- Contribution du SI à la valeur de l'entreprise : démarche, cas concrets / AFAI-ISACA.
- Modèle d'analyse et de benchmarking des coûts informatiques / Cigref – 2018
- Software Asset& Cloud Management / Cigref – 2018
- Valorisation des données dans les grandes entreprises / Cigref – 2016
- Cloud Computing et protection des données dans le cloud / AFAI-ISACA, Cigref - 2013

ACRONYMES

- **ABC :** Activity-Based Costing
- **COMEX :** Comité exécutif
- **DSI :** Direction des systèmes d'information
- **MVP :** Minimum Viable Product
- **PMO** : Project Management Office
- **PoC :** Proof of Concept
- **SI :** Système d'information
- **SOC :** Security Operational Center

GLOSSAIRE

- **Business Case (étude d'opportunité ou plan d'affaire en français) :** document ayant pour objectif de justifier un investissement en temps ou en argent dans un nouveau projet. Il doit expliquer quel processus, activité, ou produit de l'entreprise est concerné et expliquer en détail les objectifs du projet (Source : thebusinessplanshop).

- **Core IT :** système d'information hérité de toutes les évolutions qui ont eu lieu jusqu'à aujourd'hui, également appelé le SI existant ou le legacy.

- **Cyber-risque :** Il existe 4 types de risques cyber aux conséquences diverses, affectant directement ou indirectement les particuliers, les administrations et les entreprises : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage (Source : Gouvernement.fr)

- **Cybersécurité (selon l'ANSSI) :** État recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la conformité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles (Source : ANSSI).

- **DevOps :** mélange des tâches qu'effectuent les équipes d'une entreprise chargées du développement des applications (Dev) et de l'exploitation des systèmes (Ops, pour opérations) (Source : LeMagIT)

- **Digital :** terme anglais pour désigner le numérique ; équivalent sémantique française dans le vocabulaire commun des entreprises.

- **Fast IT :** informatique agile utilisant des technologies innovantes, exploitant la donnée (produite, stockée, partagée, analysée) pour répondre à de nouveaux usages, cultures et organisations (social, collaboratif, connecté…)

- **Informatique :** science du traitement rationnel, notamment par machines automatiques, de l'information considérée comme le support des connaissances humaines et des communications dans les domaines techniques, économique et social.

- **Méthode agile :** méthode de gestion de projet basée sur des cycles de développement très courts (appelés 'sprint') dont l'objectif principal demeure l'amélioration continue. On délivre rapidement une première version du livrable (Produit Minimum Viable ou Minimum Viable Product) attendu qui sera stabilisé et peaufiné avec les cycles de développement itératifs.

- **Numérique :** ensemble des technologies informatiques au-delà du système d'information de l'entreprise qui opère avec lui et qui l'enrichit/augmente.

- **Roadmap SI :** celle-ci est la déclinaison opérationnelle du volet numérique du plan stratégique de l'entreprise.

- **Système d'information (SI) :** ensemble de ressources (personnel, logiciels, processus, données, matériels, équipements informatiques et de télécommunication…) permettant la collecte, le stockage, la structuration, la modélisation, la gestion, la manipulation, l'analyse, le transport, l'échange et la diffusion des informations (textes, images, sons, vidéo…) au sein d'une organisation.

OUTIL D'ÉVALUATION

À TÉLÉCHARGER LIBREMENT EN FLASHANT LE QR CODE

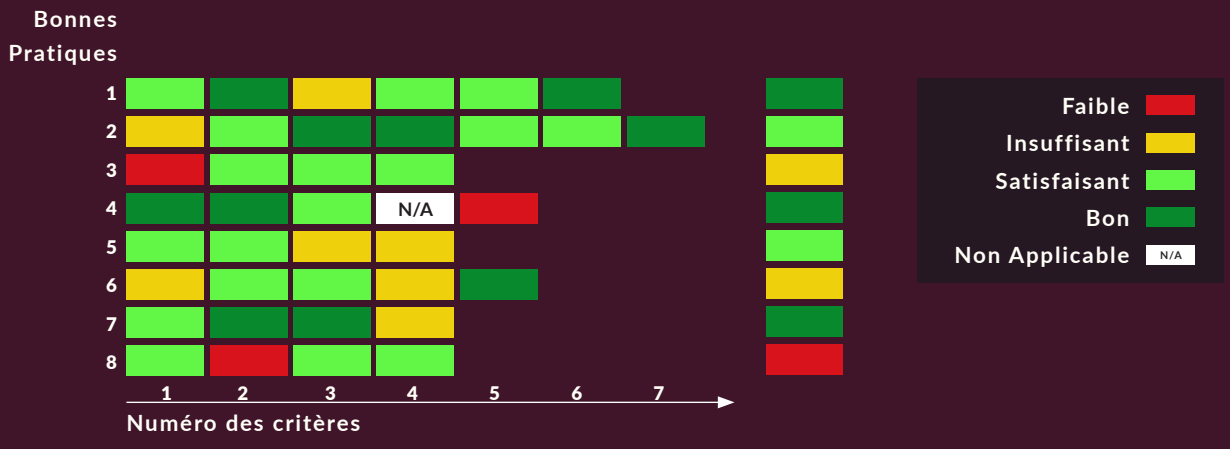
UTILISATION DE L'OUTIL D'ÉVALUATION XLS

L'outil (xls) d'évaluation propose une matrice avec à l'horizontale les bonnes pratiques et à la verticale les critères. L'échelle comporte 4 couleurs sans offrir la possibilité du choix «moyen» pour forcer à émettre une évaluation. Cela ne donne pas une note finale mais un « mur de couleurs » représentant une photo globale avec une certaine teinte.

EXEMPLE D'ÉVALUATION

ÉTAPE 1
EVALUATION
DE CHAQUE CRITÈRE

ÉTAPE 2
EVALUATION
DE LA PRATIQUE



ÉTAPE 3
EVALUATION DU VECTEUR

Evalutation globale du niveau de maîtrise du Vecteur

AFAI-ISACA

WWW.AFAI.FR

3 rue du Colonel Moll
75017 Paris
+33 1 40 08 47 81
afai@afai.fr

CIGREF

WWW.CIGREF.FR

21 avenue de Messine
75008 Paris
+ 33 1 56 59 70 00
cigref@cigref.fr

IFACI

WWW.IFACI.COM

98 bis boulevard Haussmann
75008 Paris
+33 1 40 08 48 00
institut@ifaci.com