L'ENTREPRISE FACE À SES ENJEUX ET RISQUES NUMÉRIQUES

GOUVERNANCE ET ORGANISATION DES SI

cigref Réseau de Grandes Entreprises

ifaci institut français de l'audit et du contrôle internes

AFAI® Pour des systèmes d'information de confiance et créateurs de valeur

REMERCIEMENTS

COMITÉ D'ORIENTATION

- Pascal Antonini, Associé EY, Président AFAI
- Farid Aractingi, Directeur de l'Audit et de la Maîtrise des Risques Renault, Président IFACI
- Jean-Pierre Bouillot, VP Information System Audit, Risk Committee Project Leader Sanofi, Représentant IFACI
- Pascal Buffard, Président d'AXA Technology Services, Président CIGREF
- Régis Delayat, DSI, Groupe SCOR, Administrateur du CIGREF et Administrateur AFAI
- Jean-Louis Leignel, MAGE Conseil, Administrateur AFAI
- Jean-Michel Mathieu, Senior Director Crowe Risk Consulting, Président d'honneur AFAI

COMITÉ DE RELECTURE

- Sophie Bouteiller, Directrice de mission, Responsable des partenariats, CIGREF
- Jean-Marie Ferrières, Consultant SI Digital, Expert près la Cour d'Appel de Paris
- Philippe Mocquard, Délégué Général IFACI
- Gérard Pomper, Délégué Général AFAI

CONTRIBUTEURS/EXPERTS

- Jean-Luc Amagat, DSI Nextira One
- Astrid Chauvin, Pekina Consulting
- David Chades, Responsable Informatique de gestion Centre France
- Régis Delayat, DSI, Groupe SCOR
- Jean-Charles Duret-Ferrari, Sécurité des Systèmes d'Information La Française des Jeux
- Emmanuelle Fines Laurent, Directrice Organisation et Gouvernance Saint-Gobain
- Henri de Foucault, Chef de bureau SIC, Marine Nationale
- Laurent Fournier, Directeur des Infrastructures, Webhelp
- Alfonso Gonzalez, DSI Manpower Group
- Philippe Lanson, DSI Renault
- Claude Le Corre, Manager Crowe Risk Consulting
- Mehdi Mohammedi, DSI Editions Lefebvre Sarrut
- Samatar Morin, DSI Citelum
- Annie Prévôt, DSI CNAF
- André Schwob, DSI CDC
- Franck Tarragnat, DSI M6
- Hubert Tournier, Adjoint DOSI Groupement des Mousquetaires
- Isabelle Vialettes, DSI Groupe Monoprix
- Antoine Vigneron, Secrétaire général AFAI

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

SOMMAIRE

PRÉFACE

Pour les dirigeants de sociétés, la transformation numérique n'est pas une option mais un impératif qui bouleverse les modèles d'affaires. Les entreprises qui négocieront trop tard ce virage numérique souffriront et risqueront même de disparaitre. Devant l'urgence des transformations à accomplir, les métiers prennent souvent en charge directement les projets numériques non sans risque en matière de gouvernance. Dans ce contexte, en effet, la DSI doit rester un acteur clé de la transformation numérique, tout en améliorant la qualité de son service..

Pour mieux comprendre les priorités des entreprises et les enjeux des DSI, le cabinet Crowe Risk Consulting et l'AFAI, Association Française de l'Audit et du conseil Informatiques se sont associés au CIGREF, réseau des grandes entreprises, et à l'IFACI, Institut Français de l'Audit et du Contrôle Internes, pour consulter des organisations de taille significative dans les secteurs privé et public.

Les trois associations ayant publié conjointement, en 2011, le Guide d'Audit de la Gouvernance des Systèmes d'Information *(Guide AGSI - voir page 6)*, ce document a servi de point de départ à l'élaboration d'un questionnaire soumis aux membres de chacune des associations (majoritairement, des DSI et des RSSI). La finalité de cette consultation était de valider la pertinence et l'actualité du guide AGSI, à travers le prisme de 3 des 12 vecteurs du guide et en prenant appui sur les 3 préoccupations majeures des DSI pour 2014 (issues d'une enquête CIGREF menée en 2013 auprès de ses entreprises membres) : la stratégie numérique, la gestion des risques et la maîtrise des coûts.

La consultation a été favorablement accueillie par les DSI, la présente étude propose une analyse synthétique des réponses reçues et permet au lecteur de situer son organisation et son niveau de maturité par rapport à ceux des répondants. Une annexe méthodologique facilite cette lecture et fournit des éléments de volumétrie.

Nous remercions les entreprises et administrations membres d'une, ou parfois plusieurs, de nos structures et qui ont accepté de répondre à cette enquête, dans laquelle nous ne doutons pas que chacun trouvera des éléments concrets et utiles pour progresser dans sa pratique professionnelle.

PASCAL ANTONINI
Président, AFAI

FARID ARACTINGI
Président, IFACI

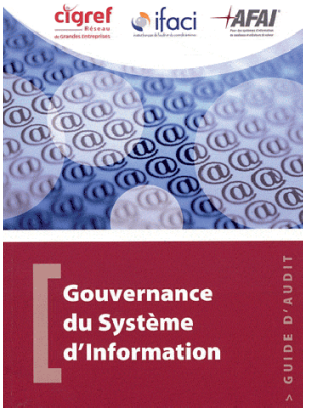
PASCAL BUFFARD
Président, CIGREF

JONATHAN BURNETT
Président, Crowe Risk Consulting

LE GUIDE D'AUDIT DE GOUVERNANCE DES SYSTÈMES D'INFORMATION

L'objectif principal de ce guide, publié en 2011 par le CIGREF, l'IFACI, et l'AFAI, est de mettre à la disposition des auditeurs et des DSI un guide pratique d'audit traitant sous un angle managérial et non pas technique, la problématique globale de la gouvernance des SI par l'entreprise. AGSI permet aux directions de l'Audit interne de répondre aux questions que se pose la Direction générale à propos du niveau de maîtrise de son SI, et de fournir aux autres fonctions de l'entreprise une assurance raisonnable que leurs processus métiers sont bien soutenus par des systèmes d'information de qualité.
Cette évaluation de la gouvernance à haut niveau permet de cerner des points de vigilance par rapport au management du SI, de nature opérationnelle, économique ou stratégique, qui doivent être sous contrôle pour que l'entreprise ou l'organisation puisse être considérée comme performante en termes de gouvernance de son système d'information.

Même si cette dernière s'évalue de façon globale, elle a été décomposée, à des fins pratiques, en 12 « vecteurs » distincts suffisamment « autoporteurs » pour pouvoir faire l'objet de missions individualisées par vecteur ou groupes de vecteurs.
Le Guide est complété d'un outil permettant de documenter les contrôles et établir une synthèse visuelle des résultats obtenus.



Guide d'audit de Gouvernance des Systèmes d'information

Contacts pour se procurer ce guide et l'outil associé :

CIGREF : cigref@cigref.fr
IFACI : recherche@ifaci.com
AFAI : afai@afai.fr

Télécharger le guide en cliquant sur le lien suivant :
www.cigref.fr/gouvernance-du-systeme-dinformation-guide-daudit

INTRODUCTION

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

CHAPITRE N. 1

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

INTRODUCTION

A un moment où le marché et les entreprises vivent l'accélération de la transition numérique avec la numérisation de leur *business* et où, concomitamment, les dirigeants exigent une plus forte maîtrise des coûts et des risques, la fonction SI se trouve directement impliquée dans la chaîne de valeur, et n'est plus une simple fonction support. Avec le développement de l'offre de services et l'ouverture des entreprises, la fonction SI a beaucoup à faire pour assurer à la fois convergence et cohérence du SI, sécurité et agilité, innovation et gestion du parc applicatif existant...

En ce sens, les répondants à la consultation conjointe AFAI-CIGREF-IFACI ont apprécié l'exercice consistant à considérer la grille élaborée sur la base du guide AGSI comme une forme « d'autoévaluation », qui leur a permis de faire le bilan des changements réalisés. Certains d'entre eux ont du reste utilisé cette grille comme un outil d'Audit interne.

Quel fil conducteur trouver à la lecture des réponses apportées ? Nous retiendrons pour chaque priorité un certain nombre de messages ou de tendances fortes résumés ci-après.

STRATÉGIE NUMÉRIQUE

Même si certains le considèrent comme un exercice dépassé, le schéma directeur demeure le point d'ancrage de la stratégie SI. Beaucoup le nomment « Schéma directeur numérique ». Réalisé en association de plus en plus étroite avec les métiers, il est validé dans plus de deux tiers des cas par la Direction Générale. Il est perçu comme la résultante d'une vision à long terme, d'une urbanisation à forte composante fonctionnelle et d'un exercice budgétaire. Les DSI en communiquent les résultats en privilégiant les réunions de présentation et en évitant les diffusions élargies.

Au cœur des projets de transformation de l'entreprise, les DSI s'organisent pour répondre de la façon la plus efficace aux besoins des métiers. Cela les conduit à repenser leur organisation pour réussir la transition numérique. Cette transition est déjà accomplie pour un certain nombre d'entre elles, et 70% des répondants affirment être prêts à l'accomplir. A la question « cela conduit-il à une informatique à deux vitesses ? » (une vitesse de croisière pour les applications classiques, une vitesse accélérée pour développer l'agilité), la réponse est : ce n'est pas une fatalité. Pour accompagner cette transition numérique, les DSI sont sensibles aux enjeux de l'innovation. Pour eux, cette dernière doit nécessairement combiner un recours à des technologies bien ciblées (mobilité, objets connectés par exemple), mais aussi l'usage d'approches agiles. Le recours au SaaS et au *Cloud* se généralise avec discernement, en restant sélectif en fonction des sujets traités.

GESTION DES RISQUES

Certes, les DSI connaissent les principaux référentiels de bonnes pratiques de maîtrise de la qualité et de gestion des risques, mais ce constat mérite d'être nuancé : d'une part, cette connaissance est limitée à trois ou quatre d'entre eux (ITIL, COBIT5, ISO, CMMI), d'autre part, elle ne garantit pas la mise en pratique systématique de tels outils pour améliorer les processus SI. Le guide AGSI, quant à lui, est très méconnu : seuls 8% des répondants déclarent avoir une bonne connaissance du guide AGSI, contre 69% de réponses « Aucune connaissance »; ce qui renforce l'utilité de cette consultation.

Sur le plan humain, les préoccupations principales des DSI concernent avant tout la gestion des compétences et l'accompagnement du changement, suivis de près par le rôle du management intermédiaire et la dépendance à des personnes clés. Au niveau technique, le suivi des risques projets s'intensifie et s'intègre à leur gestion pour 90% d'entre eux. Par contre, si plus de 80% des entreprises déclarent posséder un portefeuille de projets, ce portefeuille n'est utilisé dans la gestion des risques que dans un cas sur deux. La remontée et le pilotage global de ces risques sont encore rares.

Le risque SI est perçu mais diffus, et la sensibilisation au risque numérique reste insuffisante : à peine la moitié des entreprises consultées y serait assez sensibilisée. La mise au point d'une cartographie des risques SI commence à se généraliser, avec la contribution, par fréquence descendante de citation, de l'Audit interne, du DSI, du *risk manager* et du RSSI. Il semble aussi que les interactions entre ces différents acteurs s'intensifient : la fréquence des rencontres de revue des risques SI serait dans 45% des cas trimestrielle, voir mensuelle.

Interrogés sur les mesures d'anticipation en place, les DSI semblent concentrer leurs efforts sur les applications les plus importantes, en privilégiant les analyses d'impact, suivies des plans de continuité, des dispositifs de gestion de crise et des plans de reprise d'activité. Concernant la sécurité des systèmes d'information proprement dite, les DSI ont souvent mis en place un ensemble très complet de mesures visant à se protéger contre les risques généraux ou spécifiques: définition d'une politique ou d'un plan de sécurité, création d'un *SOC (Security Operations Center),* déploiement d'outils de contrôle et de programmes de sensibilisation des utilisateurs. D'autres mesures sont citées, surtout les tests d'intrusion et les audits ISO 27001. Les DSI sont audités le plus souvent au niveau applicatif, de la sécurité et de la conformité (au regard des licences de logiciels surtout). Ils commanditent eux-mêmes peu d'audits, et plutôt sur des thèmes très ciblés : tests d'intrusion, revues de code, diagnostics de vulnérabilité, revue des coûts.

Enfin, s'agissant des relations avec les différents partenaires de la gestion des risques, celles-ci

semblent tout à fait encourageantes : jugées plutôt bonnes avec la Direction Générale, elles sont qualifiées de bonnes, voire excellentes, avec l'Audit interne, et de bonnes avec l'Audit externe, ce dernier étant perçu comme un interlocuteur régulier et utile dans les revues systématiques des contrôles généraux et des applications à caractère financier.

MAÎTRISE DES COÛTS

Notre consultation fait ressortir une forte mobilisation des DSI sur la maîtrise des coûts. Si les trois quarts d'entre elles ont des budgets SI inférieurs à 4% du chiffre d'affaires, on observe une grande disparité en fonction des secteurs et parfois, le caractère non représentatif de cet indicateur (dans le secteur public ou le secteur bancaire par exemple). Il n'en demeure pas moins que les nécessaires investissements exigés par le numérique liés au maintien et à l'évolution de l'existant conduisent à une équation difficile. Une attention toute particulière est portée par les DSI au rapport entre *build* et *run*. En dépit des efforts importants consentis en matière d'investissements *(build)*, une large part des budgets correspond aux coûts de fonctionnement *(run)*, à savoir 65% du total en moyenne.

Face à l'émergence d'une « *Shadow IT* », nos interlocuteurs semblent sereins, car 80% d'entre eux déclarent bien connaître et maîtriser la dépense informatique. Ils s'estiment aussi satisfaits des ressources internes dont ils disposent, 70% déclarant qu'elles sont en nombre suffisant. Leur effort budgétaire a porté en grande partie sur la mutualisation des moyens et les trois quarts des DSI déclarent avoir déjà mutualisé la moitié des moyens SI au sein de leurs groupes. Autre source d'économie potentielle, le recours à l'externalisation reste sélectif et concerne rarement architecture, urbanisme, études ou sécurité. Ses deux motivations principales sont la recherche de gains financiers, ou le manque de certaines compétences techniques, motivations qui peuvent paraître contradictoires car il est délicat d'externaliser des fonctions non maitrisées par les équipes en interne tout en générant des gains. Autre source de transparence et de maîtrise de la dépense, le catalogue de services se généralise. 40% des répondants en sont dotés, et 45% déclarent avoir un catalogue en cours de mise en place ou en projet.

Si des efforts réels sont faits par les DSI sur le registre des coûts, l'usage d'un contrôle de gestion approfondi n'est pas encore répandu. Le calcul du coût de revient des activités n'est pas généralisé : 40% des entreprises ne le font pas, ce qui signifie que leur catalogue de services est davantage un outil de communication en interne qu'un outil de pilotage des coûts. A ce titre, nous avons constaté que 60% des entreprises disposant d'un catalogue de services n'avaient pas de système de calcul des coûts informatiques.

FOCUS SUR LA STRATÉGIE NUMÉRIQUE

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

CHAPITRE N. 2

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

FOCUS SUR LA STRATÉGIE NUMÉRIQUE

TRIBUNE CIGREF : DE LA GOUVERNANCE DU SYSTÈME D'INFORMATION À LA GOUVERNANCE DE L'ENTREPRISE NUMÉRIQUE !

La révolution numérique bouscule le modèle d'affaires et la culture même de l'entreprise, elle impacte son fonctionnement, son organisation, ses processus, ses équipes, et sa gouvernance.
La transformation est majeure et impose qu'une stratégie numérique, portée par la Direction Générale, soit élaborée conjointement entre les Métiers de l'entreprise et la DSI. L'entreprise en 2020 sera numérique ou ne sera pas ! Et la bonne exécution de cette stratégie numérique passe par la mise en place d'une gouvernance adaptée, au service de la transformation engagée.

Le numérique n'appartient pas à l'IT, il ne se réduit pas non plus ni à l'*e-business*, ni au marketing digital ou au client internaute. Le numérique est transverse à l'entreprise, engage toutes ses composantes (Direction Générale, Production, Marketing, Commercial, Logistique, R&D, Finance, Risques, DRH, DSI, etc.), et s'inscrit dans une démarche et dans un cadre de gouvernance globaux.

Du fait de la transversalité des impacts du numérique, chaque fonction, chaque métier de l'entreprise étant concerné, les différents acteurs doivent coopérer et se centrer sur l'atteinte des objectifs numériques, tels que définis dans la stratégie numérique. Ainsi, une gouvernance (l'art de décider ensemble) du numérique est donc nécessaire, et impose de prioriser l'allocation des moyens de l'entreprise pour innover, maximiser la création de valeur et optimiser la gestion des risques.

Dans ce contexte, la contribution de la fonction SI à la transformation numérique de l'entreprise évolue. Les technologies et usages liés au numérique la conduisent à prendre sa place dans ces stratégies de transformation qui impliquent l'ensemble des acteurs de l'entreprise. La numérisation du *business* amène le SI, et donc la DSI, à être de plus en plus partie intégrante de la création de valeur. La fonction SI évolue par ailleurs sous une double influence : à la fois interne avec une montée en maturité des utilisateurs, et externe avec la volonté de proposer une expérience unique aux clients, et le développement de partenariats dans une logique de co-création.

PASCAL BUFFARD
PRÉSIDENT, CIGREF

NOTRE PROGRAMME «DIGITAL SCOR» MOBILISE LE GROUPE DEPUIS 2013, GRÂCE À DE NOMBREUX ATELIERS DE TRAVAIL AVEC LES ÉQUIPES MÉTIERS, UNE COMMUNICATION INTERNE TRANSVERSE, ET L'AFFICHAGE D'UNE AMBITION AU PLUS HAUT NIVEAU AU SEIN DU GROUPE. IL FIXE NOTRE STRATÉGIE DIGITALE SUR UN HORIZON DE 5 À 10 ANS.

RÉGIS DELAYAT, DSI GROUPE SCOR

LE SCHÉMA DIRECTEUR RESTE LE POINT D'ANCRAGE DE LA STRATÉGIE NUMÉRIQUE

Notre étude confirme le rôle essentiel du schéma directeur comme point de départ et fil conducteur des activités informatiques.

Il est le résultat d'un exercice de planification stratégique ou à moyen terme qui définit la cible à atteindre et doit présenter plusieurs caractéristiques :

- Etre un diagnostic à date,
- Formuler des objectifs sur la base de la stratégie de l'entreprise et de l'analyse de l'existant,
- Constituer un référentiel dynamique et une feuille de route pour le DSI en matière de budgets, opérations et investissements.

Feuille de route technologique, le schéma directeur prend ainsi en compte les problématiques d'architecture technique, d'urbanisation, du *Cloud*.

Le schéma directeur informatique est devenu un point de passage obligé : 92% des entreprises qui ont répondu à notre enquête ont compris l'intérêt de le produire :

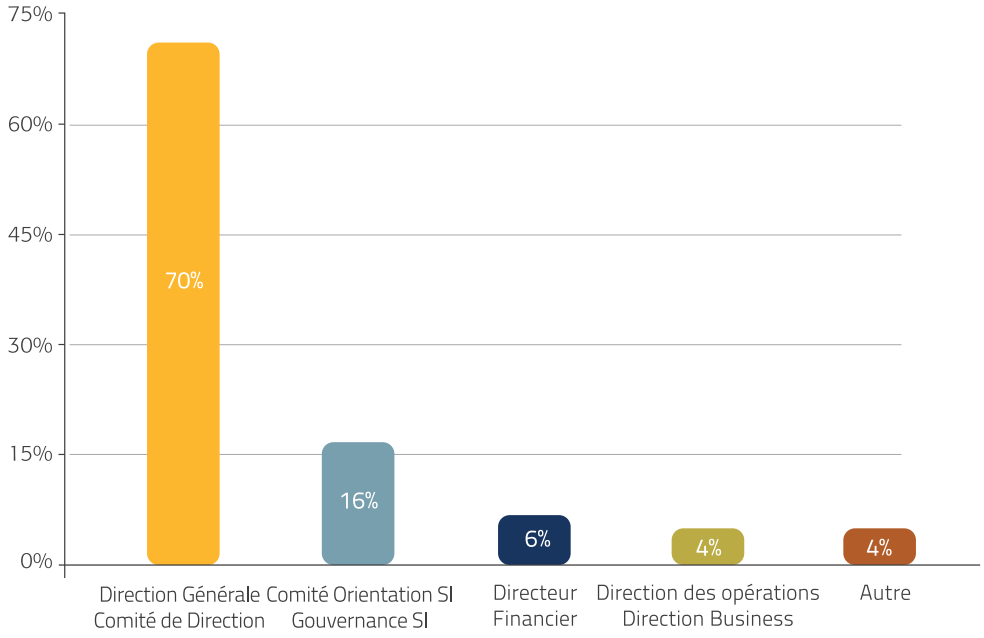
- 88% des schémas directeurs sont réalisés sur un horizon d'au moins trois ans et sont mis à jour une fois par an dans 70% des cas,
- Les métiers sont impliqués dans plus de 90% des cas.

Pour affiner l'analyse, très peu de schémas directeurs sont à moins de trois ans. Près de la moitié des schémas directeurs a pour horizon trois ans, et 15% se situe à quatre ans.
Pour le reste (25%), s'échelonnant entre cinq et dix ans, on trouve essentiellement des entreprises dont le modèle d'affaires est assez stable (peu de nouveaux entrants) ou des grandes administrations.

Si le pourcentage déclaré à propos de la mobilisation des métiers pour l'élaboration du schéma directeur et la définition de la stratégie numérique semble très élevé, il n'en demeure pas moins que les témoignages recueillis au cours de nos entretiens font apparaître qu'elle n'est pas acquise, et reste très variable en fonction des interlocuteurs et des sociétés. Les urgences opérationnelles l'emportent trop souvent sur la vision à moyen terme. Cette situation apparaît très préoccupante aux yeux de certains DSI.

La notion de schéma directeur a évolué pour mieux répondre aux enjeux de transformation des entreprises. De plus en plus, les schémas directeurs couvrent désormais le volet numérique. Dans certains cas le terme « Schéma Directeur numérique » remplace celui de « Schéma Directeur informatique ».

FIG 1. LE SCHÉMA DIRECTEUR, VALIDÉ PAR LA DIRECTION GÉNÉRALE.



Dans la majorité des cas ***(voir Figure 1)***, la validation du schéma directeur est conduite par :

- Le Directeur Général / Comité de direction (69 % des cas),
- Le Comité d'orientation SI ou de gouvernance SI (16% des cas),
- Le Directeur Financier (dans ce cas, le DSI reporte directement au Directeur Financier).

Dans le cas d'un schéma directeur très orienté «numérique», il est à noter que la validation passe nécessairement par une direction Digitale ou Métier. Ce niveau de validation accentue et confirme le caractère stratégique du schéma directeur informatique.

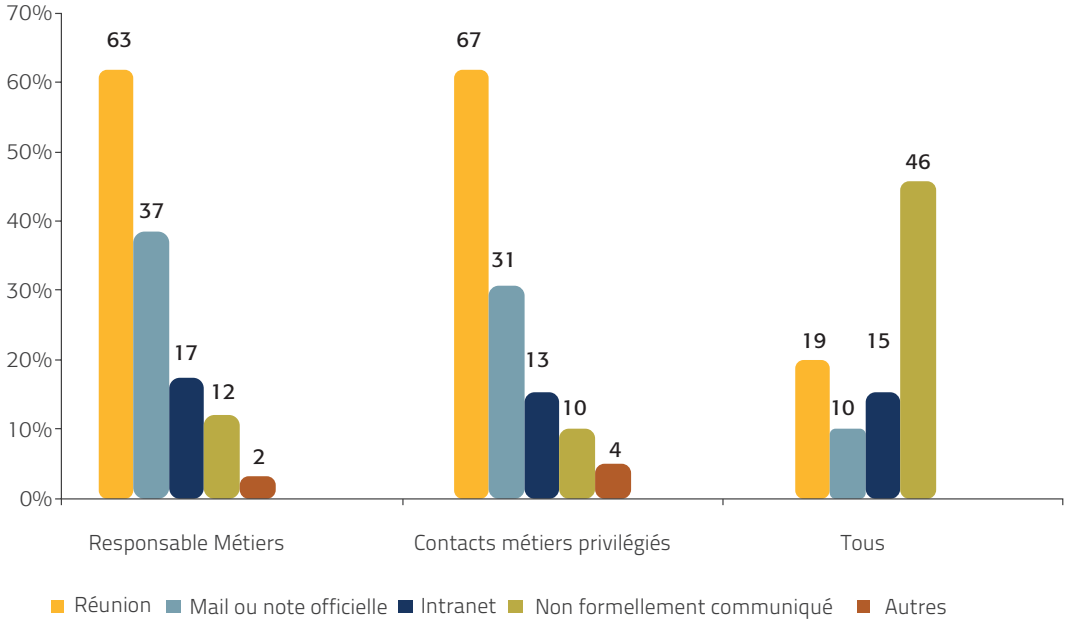
Il en découle naturellement une présentation au COMEX dans près de 80% des cas.
Dans le cas où le Groupe est de taille conséquente, il peut arriver que le schéma directeur ne soit pas présenté au COMEX, mais à un Comité de niveau intermédiaire.
La communication du schéma directeur s'adresse aux responsables métiers ou aux contacts métiers dits privilégiés. Elle se fait majoritairement au travers de réunions (75% des cas) ou par mail.

La réunion est privilégiée, car elle permet de fournir des explications appropriées aux interlocuteurs et facilite ainsi une meilleure compréhension des orientations prises et des arbitrages réalisés.
Le contenu du schéma directeur informatique n'est pas pour autant une information « publique » puisqu'il est très rarement diffusé en masse à l'ensemble des métiers ***(voir Figure 2),*** plusieurs réponses étant possibles quant au mode de communication).

La ***Figure 2*** conduit du reste à se poser la question suivante : dans les cas où le schéma directeur n'est pas formellement communiqué, se traduit-il dans la gestion du portefeuille des projets et dans les arbitrages qui en découlent (dont les budgets annuels /pluri-annuels) ?

FIG 2. COMMUNICATION DU SCHÉMA DIRECTEUR AUX METIERS

(PLUSIEURS RÉPONSES POSSIBLES)

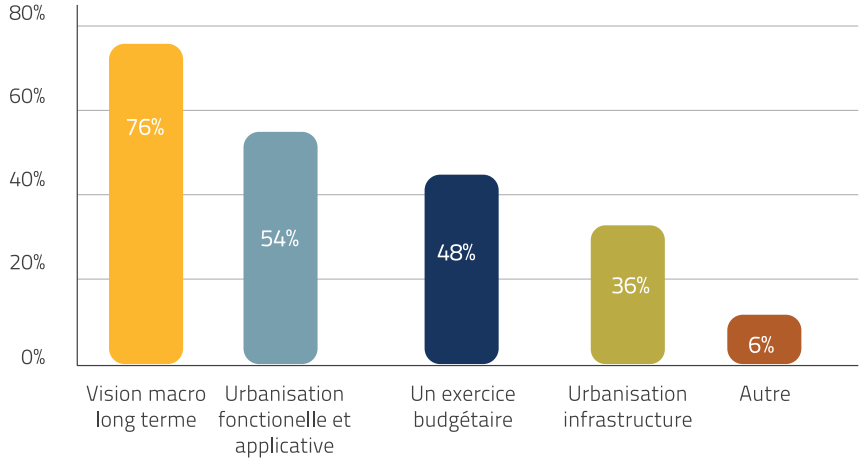


Le schéma directeur informatique est pour la majorité des répondants la formalisation d'une vision numérique commune Métiers, DSI et DG macro à moyen long terme, comme en témoigne la **Figure 3**. Si le schéma directeur permet d'établir cette vision à long terme, il fournit aussi l'occasion d'une réflexion sur l'urbanisation fonctionnelle et applicative (dans plus d'un cas sur deux), et, dans une moindre mesure, sur l'urbanisation des infrastructures.

Dans la moitié des cas, le schéma directeur reste aussi un exercice budgétaire. Une des entreprises consultées a même spécifié qu'il fournissait l'opportunité de hiérarchiser les investissements en fonction des processus métier.

FIG 3. CE QUE RECOUVRE LE SCHÉMA DIRECTEUR

(PLUSIEURS RÉPONSES POSSIBLES)



NOUS AVONS CRÉÉ UN VÉRITABLE PARTENARIAT ENTRE LA DSI ET LES MÉTIERS, GRÂCE À L'EXISTENCE D'ÉQUIPES IT INTÉGRÉES AUX MÉTIERS. CES ÉQUIPES FONCTIONNENT SUIVANT LE PRINCIPE DE DOUBLE REPORTING IT/MÉTIERS ET CECI AU PLAN GLOBAL .

RÉGIS DELAYAT, DSI GROUPE SCOR

LES PROJETS DE TRANSFORMATION DE L'ENTREPRISE SE FONT AVEC LA DSI

L'analyse des réponses permet d'affirmer que la DSI est désormais présente dans la quasi-totalité des projets de transformation de l'entreprise, en association avec les métiers. Sur les projets transverses, elle se trouve dans 20% des cas en collaboration avec :

- La Direction des Ressources Humaines, à des fins de conduite du changement et de modifications des organisations,
- La Direction Financière, car l'objectif consiste souvent à optimiser les processus et les coûts.

LA DSI S'ORGANISE POUR MIEUX RÉPONDRE AUX ATTENTES DES MÉTIERS

Dans la plupart des cas, la structuration de la DSI reflète les métiers de l'entreprise (80% des cas).

D'autres options d'organisation de la DSI liées à l'activité de l'entreprise ont pu néanmoins être observées :

- Structuration par grand programme,
- Structuration par produit,
- Structuration par *Business Unit*.

Enfin, dans certains cas, une structuration par métier de la DSI n'a pas été retenue pour des raisons liées :

- A la taille de l'entreprise, jugée trop petite pour avoir une DSI éclatée par métier,
- Au maintien des compétences techniques, grâce à des centres de services,
- A la recherche d'efficacité, en gérant des *pools* de compétences techniques du type support ; base de données ; applications. Cette structure de DSI est alors qualifiée de « classique ».

DES BUSINESS UNITS ONT ÉTÉ CRÉÉES AFIN DE COMMERCIALISER LE SI EN INTERNE OU EN EXTERNE .

FRÉDÉRIC CHARLES, RESPONSABLE DE LA GOUVERNANCE IT, LYONNAISE DES EAUX

DÈS 2008, NOUS AVONS CRÉÉ UNE DIGITAL FACTORY, PLACÉE SOUS L'AUTORITÉ D'UN CHIEF DIGITAL OFFICER. RATTACHÉE À LA DIRECTION COMMERCIALE, LA DIGITAL FACTORY COMPREND DES ÉQUIPES DÉDIÉES, POSSÉDANT UNE COMBINAISON D'EXPERTISES : INFORMATIQUE, MARKETING, COMMUNICATION. TOUS LES SUJETS MAJEURS LIÉS À LA RELATION CLIENT ET 90% DES INVESTISSEMENTS Y AFFÉRENTS Y SONT TRAITÉS

PHILIPPE LANSON, DSI RENAULT

LA TRANSFORMATION NUMÉRIQUE N'ENGENDRE PAS TOUJOURS UNE INFORMATIQUE À DEUX VITESSES

Pour une grande partie des entreprises, la transformation numérique correspond avant tout à une transformation culturelle et donc, non seulement à un changement profond des métiers de l'entreprise mais aussi à une évolution majeure du modèle d'affaires, impactant à la fois l'organisation, les processus et les pratiques de management.

Dans plus de 70% des cas, les entreprises se sentent prêtes aux changements induits par la transformation numérique. Elles l'envisagent comme un facteur positif dans leur mode de fonctionnement, leur permettant d'être plus rapides, agiles et fiables, et nécessitant la mise en place d'une gestion des risques structurée et de pôles d'innovation.

Pour autant, elles ne perçoivent pas comme une fatalité l'émergence **d'une informatique à deux vitesses**[1] et les avis diffèrent sur ce point. Dans le cas où l'existence d'une informatique à deux vitesses est avérée (une IT traditionnelle pour gérer le *legacy* – ou « dette technique » - et une *fast IT* pour répondre aux besoins d'agilité), l'accent est mis sur la nécessité d'avoir des équipes IT communes, intégrées et réactives face aux besoins métiers.

La transformation numérique passe par des interactions fortes avec les métiers et augmente le besoin de proximité, de collaboration, de partage et d'intégration entre les équipes IT et les équipes métiers. Elle suscite aussi une réflexion sur les capacités des composants du système d'information à s'adapter (résilience du SI), dans un contexte de modification des modèles d'affaires. Les DSI font également des recherches prospectives de compétences sur des sujets tels que le Big Data, dont l'enjeu peut conduire à repenser profondément les processus métiers.

LES AVIS CONVERGENT SUR LES APPLICATIONS PORTEUSES D'AVENIR

Les innovations citées comme les plus porteuses d'avenir sont nombreuses, mais on y trouve certaines tendances fortes :

- Innovations : Mobilité, voire ultra Mobilité, Géolocalisation, *Cloud* et SaaS, *Big Data*, Analyse décisionnelle, *e-Money*, Objets Connectés, Réseaux

[1] Une vitesse de croisière pour les applications classiques, une vitesse accélérée pour traiter les urgences de la transformation numérique.

TRÈS TÔT, LA DIGITALISATION DE NOS OFFRES ET PRODUITS EST APPARUE VITALE POUR LE DÉVELOPPEMENT DU GROUPE. C'EST TOUT NATURELLEMENT QUE NOUS VENONS DE REGROUPER LES ACTIVITÉS INFORMATIQUES ET L'INNOVATION NUMÉRIQUE AU SEIN D'UNE STRUCTURE TRANSVERSE. CE DISPOSITIF, DOTÉ D'UN DÉPARTEMENT RECHERCHE ET DÉVELOPPEMENT, VISE À FAIRE DÈS AUJOURD'HUI CE QUE LES AUTRES FERONT DEMAIN, EN PROPOSANT NOTAMMENT DES PROTOTYPES MÉTIERS. CELA NOUS PERMET DE RENFORCER EN PERMANENCE LE CARACTÈRE INNOVANT DE NOTRE CHAÎNE DE VALEUR TOUT EN CONSOLIDANT NOS FONDAMENTAUX EN MATIÈRE DE FONCTION INFORMATIQUE.

MEHDI MOHAMMEDI, DSI EDITIONS LEFEBVRE SARRUT

sociaux, Dématérialisation, Outils collaboratifs, Virtualisation des postes de travail et des serveurs.
- Evolution des approches : urbanisation, méthodes agiles permettant de développer des ergonomies adaptées à l'ensemble des environnements d'utilisation, projets orientés clients (CRM, gestion de la relation client).

LE RECOURS AU MODE SAAS OU CLOUD SE FAIT AVEC DISCERNEMENT

Les applicatifs RH, les serveurs, la messagerie, les outils bureautiques et le CRM sont les premiers systèmes qui ont migré en mode SaaS ou dans le Cloud ***(voir Figure 4)***. Concernant la RH, il est probable que la migration vers le SaaS soit à mettre en relation avec l'externalisation des domaines RH, qui se pratique depuis plusieurs années.

Les applicatifs Finance, *Supply Chain*, Achats ne sont pas considérés comme candidats potentiels à ce changement. Les raisons invoquées à cela sont :

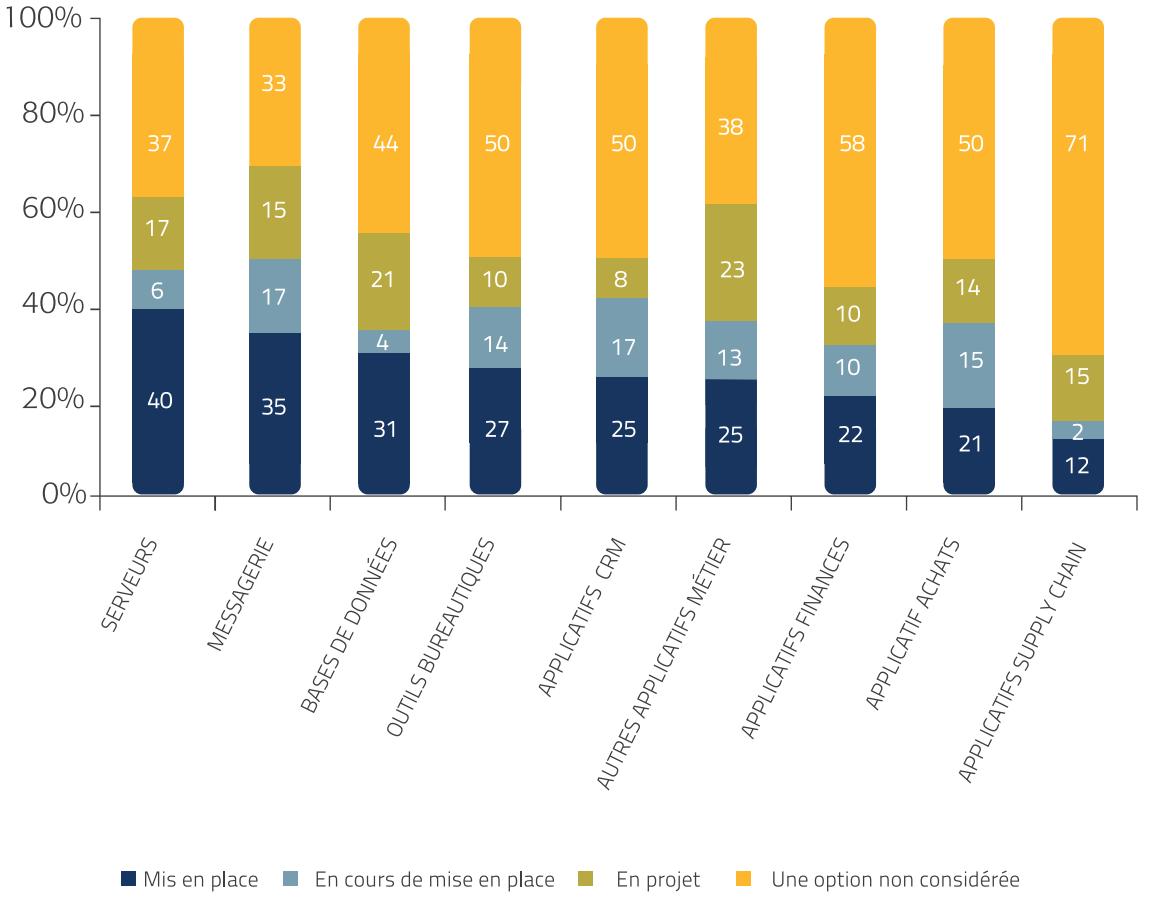
- Sécurité des données,
- Réglementation (confidentialité des données),
- Réversibilité.

Il est intéressant de voir que la sécurité des données est ici présentée comme un frein alors même que la messagerie est fortement externalisée (plus de 40% en place ou en cours de mise en place).

D'autres utilisations applicatives du SaaS et Cloud sont citées telles que :

- La gestion des notes de frais,
- La formation.

FIG 4. NATURE DES APPLICATIFS EN MODE SAAS OU DANS LE CLOUD



FOCUS SUR LA GESTION DES RISQUES

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

CHAPITRE N. 3

FOCUS SUR LA GESTION DES RISQUES

TRIBUNE IFACI : LA MORT DES BCP SIGNE-T-ELLE LE RETOUR DES DSI ?

Longtemps, les organisations ont conjugué les BCP[2], pour conforter leur résilience et le professionnalisme de leurs dirigeants – désormais, face à une indisponibilité de leur informatique, ces dossiers se révèlent d'impuissants supplétifs de leur bonne conscience, sauf si le BCP mime le DRP[3]. Car la numérisation de la société métamorphose le paysage : le digital imprègne les processus des entreprises comme les modes de vie des hommes, dans une continuité du langage et des outils.

Globalisation, concurrence, ***low cost***, interconnexion, ***cloud***, ***big data***, HD, virtuel, principe de précaution, ***compliance***,... Des mots-concepts, symboles des changements qui cernent les entreprises, entre menaces et opportunités, voire menaces et opportunités tout à la fois. Au cœur de chacune de ces transformations : les systèmes d'information. Au centre des enjeux des systèmes, le DSI. Si tout se passe bien, on l'ignore – on le laisse tranquille. S'il y a le moindre problème, on le carbonise.

Or, il surviendra toujours un problème. Par an ? Par mois ? Par jour ?

Et sinon un problème, du moins un risque de problème. C'est-à-dire un événement, doté d'une certaine probabilité, dont la conséquence sera qu'un objectif n'est pas atteint : par exemple, en matière de continuité d'exploitation, de confidentialité de l'information, de fiabilité des traitements, de gestion des jalons de projet, ou de respect des budgets... L'approche par les risques commence en effet toujours par les objectifs : pas d'objectifs, pas de risques. Et c'est le management opérationnel qui en prend l'initiative, car il est le responsable ultime de la performance des activités de son ressort, avec l'aide des fonctions de support et des fonctions spécialisées, comme le contrôle interne et la gestion des risques.

Pour les risques informatiques, c'est le DSI qui est le ***manager*** opérationnel : à lui de décider des plans de réduction et de traitement du risque qu'il convient de mettre en place. C'est à présent la cible prioritaire de ses préoccupations, car les risques informatiques figurent désormais en tête de liste des risques majeurs des entreprises. Quelques-uns sont même des ***best sellers*** dans toutes les cartographies : PCA, cybercriminalité, conduite de projets, fraude, accompagnement des métiers et des transformations.

[2] Business Continuity Plan : Plan de continuité d'activité
[3] Disaster Recovery Plan : Plan de reprise d'activité

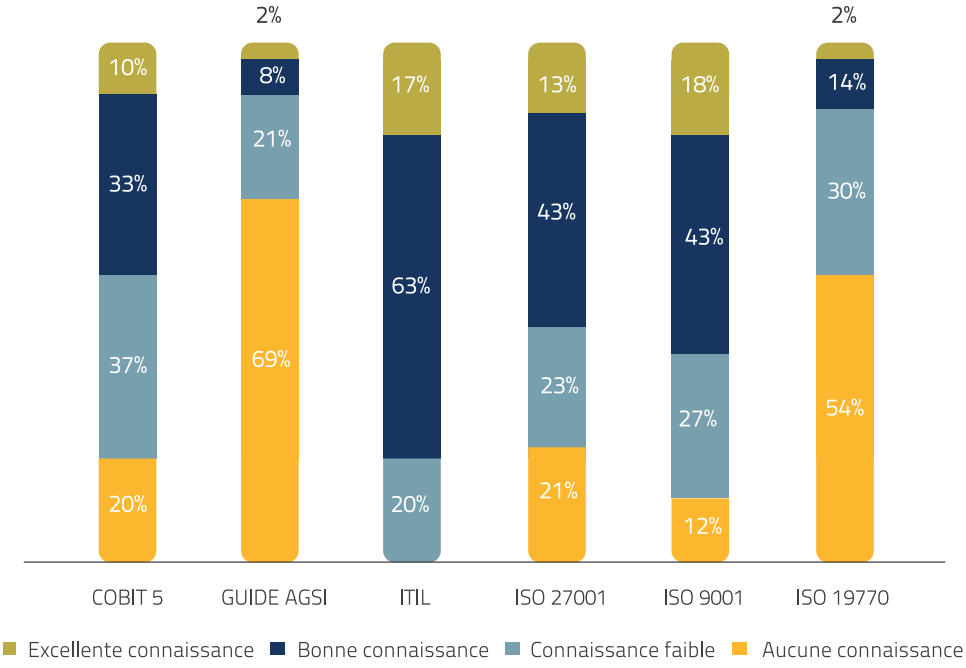
Au fil du temps, les enjeux du DSI étaient passés de la maîtrise des technologies à celle des coûts. L'une et l'autre dimension ne sont pas miraculeusement devenues obsolètes, mais désormais le DSI doit les positionner dans une vision plus globale, articulée autour des risques. Au cœur des objectifs du DSI, la capacité des systèmes à accompagner l'évolution des métiers. Au cœur de sa performance, l'approche par les risques, pour déterminer toutes les mesures, qu'il doit mettre en place ou qu'il doit inciter l'organisation à mettre en place, par une animation transversale et résolue des fonctions, par exemple à travers un Comité des risques informatiques. Le DSI veillera à l'équilibre de la ligne de crête de la gestion des risques informatiques, pour éviter de verser caricaturalement dans l'une des deux attitudes :

- Céder à la paranoïa entretenue par les marchands de peur, qui généralisent des exemples catastrophiques singuliers pour vendre des dispositifs ;
- Se laisser endormir par la qualité du service opérationnel rendu, car une informatique performante ne constitue pas une garantie de maîtrise des risques.

Le DSI fut jadis un technologue au langage ésotérique. Plus tard, il muta en contrôleur de gestion focalisé sur la rentabilité des projets. Désormais, il doit devenir un visionnaire et un leader. Un visionnaire à l'écoute des sources d'information de plus en plus variées sur les évolutions technologiques et économiques. Un leader capable de pédagogie et d'assertivité. C'est beaucoup plus difficile – mais son impact sur la performance globale de l'entreprise devient ainsi de plus en plus crucial et visible. Vive la complexité !

FARID ARACTINGI
PRÉSIDENT, IFACI
DIRECTEUR AUDIT, MAÎTRISE DES RISQUES
ET ORGANISATION, RENAULT
PRÉSIDENT DE RENAULT CONSULTING

FIG 5. MAITRISE DES BONNES PRATIQUES EN MATIÈRE DE GESTION DES RISQUES



LE RÉFÉRENTIEL COBIT5 FIGURE EN BONNE PLACE PARMI LES RÉFÉRENTIELS DE LA DSI

Les DSI maîtrisent un certain nombre de référentiels, en particulier ITIL et ISO. COBIT 5 apparait dans près de la moitié des cas comme un référentiel dont ils ont une bonne, voire une excellente connaissance *(voir Figure 5)*.

Par ailleurs, nos entretiens nous ont permis de constater que l'application de ces référentiels est loin d'être systématique, à l'exception d'ITIL qui accompagne souvent des refontes complètes de processus.

LE GUIDE AGSI EST ASSEZ PEU CONNU

Seuls 8% des répondants déclarent avoir une bonne connaissance du guide AGSI, contre 69% de réponses « Aucune connaissance »...ce qui renforce l'utilité de cette consultation.

ITIL de son côté s'impose comme un véritable standard au sein des DSI. Plus de 80% de nos interlocuteurs en ont au minimum une bonne connaissance. Les DSI consultés le mettent plus en avant comme référentiel de bonnes pratiques que comme un référentiel de gestion des risques, même si la version 3 traite cette thématique à travers la gestion des services.
Les Normes ISO 27001 et 9001 sont plutôt bien connues. Par contre ISO 19770, standard récent sur le *Software Asset Management* (SAM), l'est beaucoup moins.

Sont notamment cités parmi les autres référentiels : CMMI et Prince2.

CERTAINS ENJEUX HUMAINS PRÉOCCUPENT LES DSI

Les préoccupations principales des DSI concernent avant tout la gestion des compétences et l'accompagnement du changement, suivis de près par le rôle du management intermédiaire et la dépendance à des personnes clés. L'adaptation de l'organisation et le stress au travail sont un peu en retrait. Quant à la rotation des équipes et la parité Homme / Femme, elles apparaissent comme de faibles préoccupations, même si beaucoup admettent que leurs équipes sont majoritairement masculines. *(voir Figure 6)*.

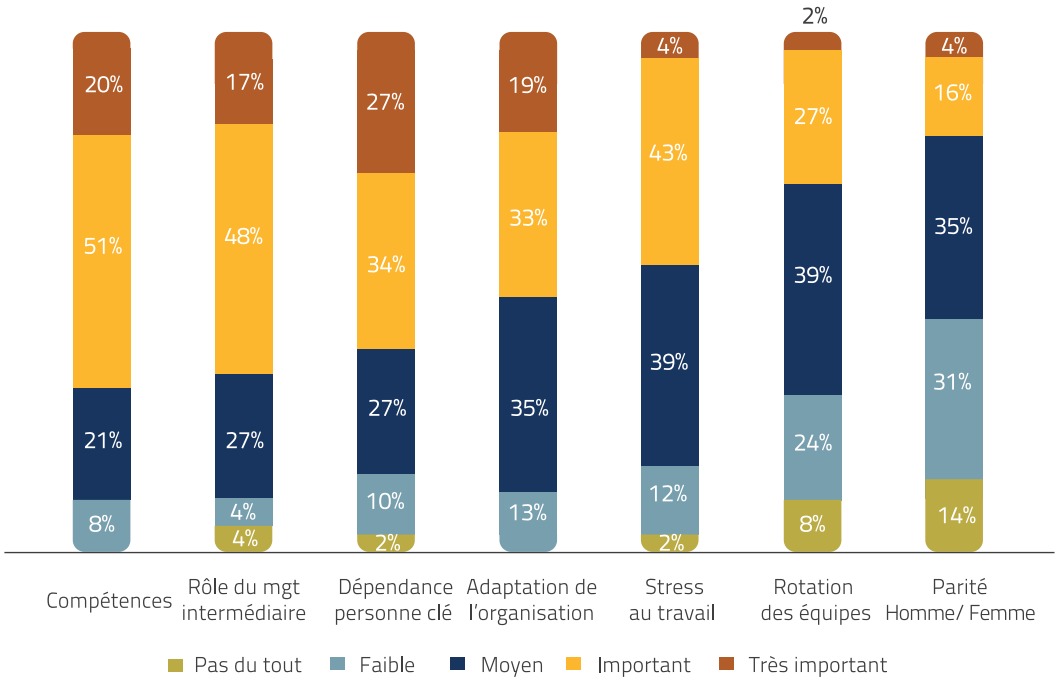
DES BILANS PROJETS SYSTÉMATIQUES SONT RÉALISÉS GRÂCE À DES OUTILS BASÉS SUR LE RÉFÉRENTIEL COBIT, AFIN D'ÉTABLIR UNE ANALYSE DU NIVEAU DE MATURITÉ ATTEINT. LE BILAN PROJET PERMET DE MESURER L'ÉCART ENTRE LA SITUATION INITIALE ET LE RÉALISÉ.
UN RETOUR SUR EXPÉRIENCE DE CHACUN D'ENTRE EUX EST PRÉSENTÉ EN COMITÉ ETUDES ET PROJETS

JEAN-CHARLES DURET FERRARI, SÉCURITÉ DES SYSTÈMES D'INFORMATION, LA FRANÇAISE DES JEUX

En complément de cette analyse, les répondants nous ont fait part de certaines préoccupations qui éclairent ce qui est dit à propos de la stratégie numérique :

- Qualité de la relation avec les métiers,
- Adaptation des formations pour aider ces derniers à gagner en maturité et en sensibilité à certains sujets (exemple : sécurité),
- Capacité à motiver les cadres seniors pour qu'ils progressent technologiquement et accompagnent le changement.

FIG 6. NIVEAU DE PRÉOCCUPATION DES DSI FACE AUX ENJEUX HUMAINS



NOTRE GOUVERNANCE INFORMATIQUE S'APPUIE NOTAMMENT SUR L'EXISTENCE DE TROIS COMITÉS MENSUELS :
- UN COMITÉ STRATÉGIQUE DES SI (CSSI), OPÉRATIONNEL DEPUIS 2 ANS, AUQUEL PARTICIPENT LES DIRECTEURS MÉTIERS, QUI EXAMINE LA PROGRAMMATION, LES QUESTIONS TRANSVERSES, ET L'AVANCEMENT DES PROJETS STRATÉGIQUES ;
- UN COMITÉ D'ENGAGEMENT (LE COMITÉ DE PILOTAGE DES INVESTISSEMENTS INFORMATIQUES), AUQUEL SONT PRÉSENTÉS TOUS LES DOSSIERS D'INVESTISSEMENT SUPÉRIEURS À 300 K€, LES PRISES DE DÉCISIONS SE FAISANT À PARTIR DE DOSSIERS TRÈS ÉTAYÉS ;
- UN COMITÉ DES MOA, À VOCATION D'ANIMATION ET D'ÉCHANGE, AUQUEL SONT NOTAMMENT PRÉSENTÉS LES BILANS DE FIN DE PROJET, SUIVANT UNE GRILLE FORMALISÉE.

ANDRÉ SCHWOB, DSI CAISSE DES DÉPÔTS ET CONSIGNATIONS

LE SUIVI DES RISQUES PROJETS SI S'INTENSIFIE ET ENTRE DANS LE DOMAINE DES COMITÉS STRATÉGIQUES

La gestion des risques se systématise dans les projets et figure dans près de 90 % d'entre eux. A y regarder de plus près ***(voir Figure 7)***, cette dimension des risques est systématique pour moins de la moitié des répondants ; les autres se concentrent sur les projets critiques ou stratégiques (27%), ou les grands projets (18%). Ceux qui ne font cette analyse que rarement, voire jamais, soulignent que leurs responsables de projets manquent de compétences ou de maturité, voire d'une politique d'analyse des risques bien définie.

Si les résultats sont globalement encourageants, on peut se poser la question de l'impact de la réglementation sectorielle (Etablissements financiers, assurance, secteur pharmaceutique, agro-alimentaire), voire de SOX, sur les résultats affichés. Une grande proportion de nos répondants correspond à ces critères.

FIG 7. GESTION DES RISQUES INTÉGRÉE DANS LES PROJETS SI

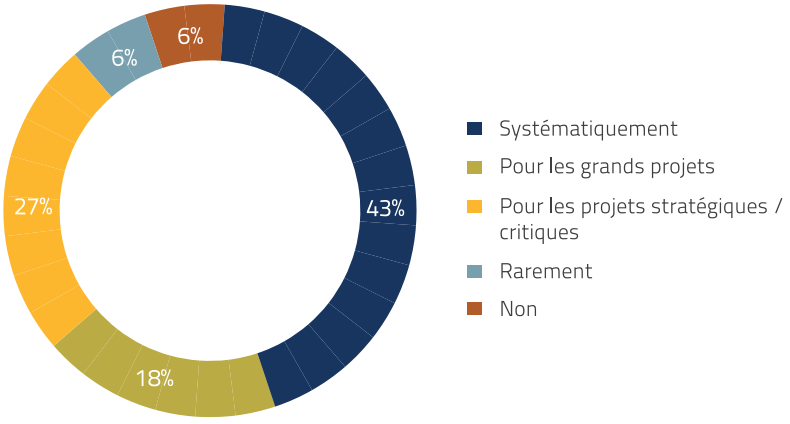
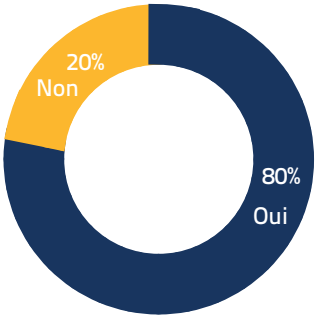
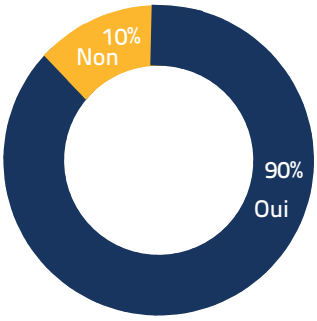


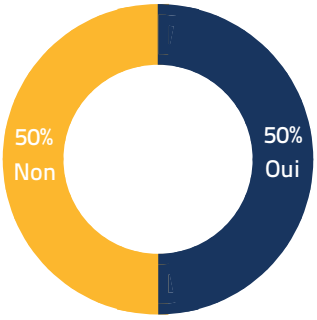
FIG 8. NIVEAU DE SENSIBILISATION DE L'ENTREPRISE AU RISQUE SI



SI perçu comme une zone de risque majeur



Connaissance des risques majeurs identifiés par l'entreprise



Entreprise suffisamment sensibilisée aux risques numériques

LA GÉNÉRALISATION DU PORTEFEUILLE DE PROJETS NE SEMBLE PAS CONTRIBUER AU SUIVI DES RISQUES

Un peu plus de 80 % des entreprises déclarent posséder un portefeuille de projets. Néanmoins, ce portefeuille n'est utilisé dans la gestion des risques que dans un cas sur deux. Cela conduit à se poser deux questions :

- Les répondants partagent-ils la même vision du portefeuille projets ?
- Peut-on concevoir un tel portefeuille sans y intégrer un minimum d'informations sur les risques liés aux projets ?

A ces questions vient se greffer une interrogation complémentaire: si près de 90% des entreprises déclarent intégrer une gestion des risques dans leurs projets, pourquoi une sur deux seulement a-t-elle recours au portefeuille de projets pour suivre ces risques ? On peut supposer que l'appréhension des risques projets se fait par d'autres moyens : revue projet par projet, alertes, etc. De grands progrès restent à faire dans la mise en place et le suivi systématique d'indicateurs de risques, tels que le préconise le référentiel *Risk IT*.

LE RISQUE SI EST PERÇU MAIS DIFFUS, ET LA SENSIBILISATION AU RISQUE NUMÉRIQUE RESTE INSUFFISANTE

L'articulation entre risque lié au SI et le risque d'entreprise est un sujet central et délicat. Si les SI apparaissent à nos répondants comme une zone de risque majeur dans près de 90% des cas, les cartographies des risques d'entreprises semblent loin de faire apparaître le même constat ***(voir Figure 7)***.

Pour autant, notre consultation met en relief une très bonne connaissance par les DSI, des risques majeurs

NOUS AVONS SIMPLIFIÉ NOTRE VISION DU PORTEFEUILLE PROJETS EN L'ORGANISANT PAR PROGRAMME. CETTE NOTION DE PROGRAMMES NOUS A PERMIS D'AVOIR UNE VISION COHÉRENTE DES PROJETS ET DE FACILITER LES ARBITRAGES MAJEURS AU SEIN DU GROUPE.

SAMATAR MORIN, DSI CITELUM

NOUS OPÉRONS UNE SÉCURISATION PLUS OU MOINS POUSSÉE, SELON LE NIVEAU DE SENSIBILITÉ DES TRAITEMENTS ET DONNÉES, EN UTILISANT LE RÉFÉRENTIEL OWASP (OPEN WEB APPLICATION SECURITY PROJECT) POUR PRENDRE EN COMPTE LES BESOINS DE SÉCURITÉ DÈS LA CONCEPTION ET LE CODAGE DES APPLICATIONS.

HUBERT TOURNIER, ADJOINT DOSI GROUPEMENT DES MOUSQUETAIRES, DG ADJOINT STIME

de l'entreprise. Il est possible que cette connaissance ne soit pas liée à l'examen de cartographie Groupe proprement dit, mais à une participation à différents Comités de direction.

Certes, le SI paraît être pris en considération comme une zone de risque significative, mais il n'en est pas de même de la sensibilité aux risques numériques ; à peine la moitié des entreprises consultées serait suffisamment sensibilisée. Il reste encore beaucoup à faire à ce niveau ***(voir Figure 8)***.

Interrogés sur les cinq risques majeurs auxquels les DSI doivent faire face, nos interlocuteurs citent essentiellement, par ordre d'importance décroissante :

- Cybercriminalité et fraude informatique,
- Incidents de production,
- Continuité d'exploitation,
- Perte de compétences (ou dépendance à des ressources clés),
- Sécurité.

Parmi les risques fréquemment cités, on relève aussi : crise sur des projets sensibles, confidentialité des données, obsolescence technique, défaillances d'infrastructures.

LE PILOTAGE DES RISQUES SI SE FAIT AVEC L'APPUI DE L'AUDIT INTERNE ET DU *RISK MANAGEMENT*

La pratique d'assurance des risques SI est encore peu usitée ***(voir Figure 9)*** et concerne les entreprises dont l'assurance est le cœur de métier, celles où le risque d'activité est extrêmement élevé et celles dont

FIG 9. PILOTAGE DES RISQUES SI
(PLUSIEURS RÉPONSES POSSIBLES)

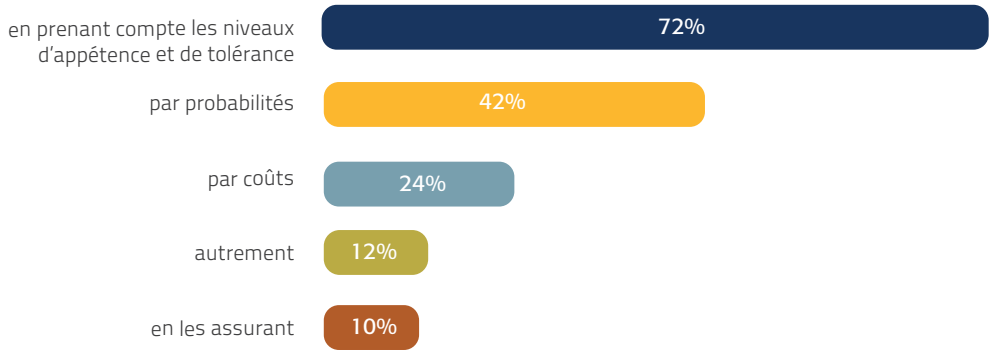
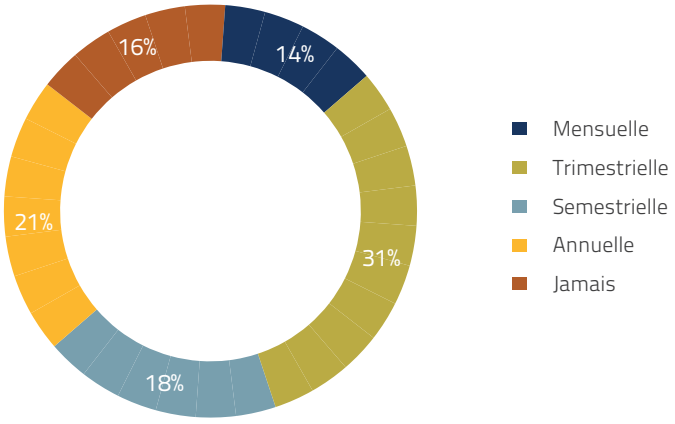


FIG 10. RÉGULARITÉ DES INTERACTIONS AVEC LA DIRECTION DES RISQUES



l'activité a une dépendance très forte à l'informatique. Dans la majorité des cas, le pilotage des risques se fait sur une base d'analyse d'appétence et de tolérance, comme on peut le constater dans la ***Figure 9***. Dans un seul cas, il est fait mention d'une coopération avec l'Audit interne dans le pilotage des risques SI. Ce constat confirme que l'Audit interne se situe plus au niveau de la détection des risques qu'en accompagnement fort à leur réduction.

Comment identifier les risques IT ? Si certains pratiquent une analyse *top down* (un quart) ou *bottom up* (20%), plus de 50% combinent les deux approches. Par ailleurs, près de 80% des répondants déclarent posséder des cartographies de risques (à jour dans 60% des cas).

La mise au point de cette cartographie des risques fait appel, par fréquence descendante de citation, à :

- Audit interne,
- DSI,
- *Risk Manager*,
- RSSI.

Souvent, cette cartographie est menée par des équipes mixtes (RSSI/DSI ou DSI/Audit interne).
Par ailleurs, plus de 40% des répondants déclarent ne pas avoir de système spécifique de détection des risques informatiques. Les mieux équipés évoquent certains outils internes ou des systèmes d'alerte.
Dans près de la moitié des cas, la discussion sur les risques numériques se fait à un rythme trimestriel, voire *a minima* dans un cadre formalisé ***(voir Figure 10)***. Dans 40 % des cas, il s'agit d'une rencontre semestrielle ou annuelle. A l'opposé, dans 16 % des cas il n'y a aucune interaction entre les acteurs.

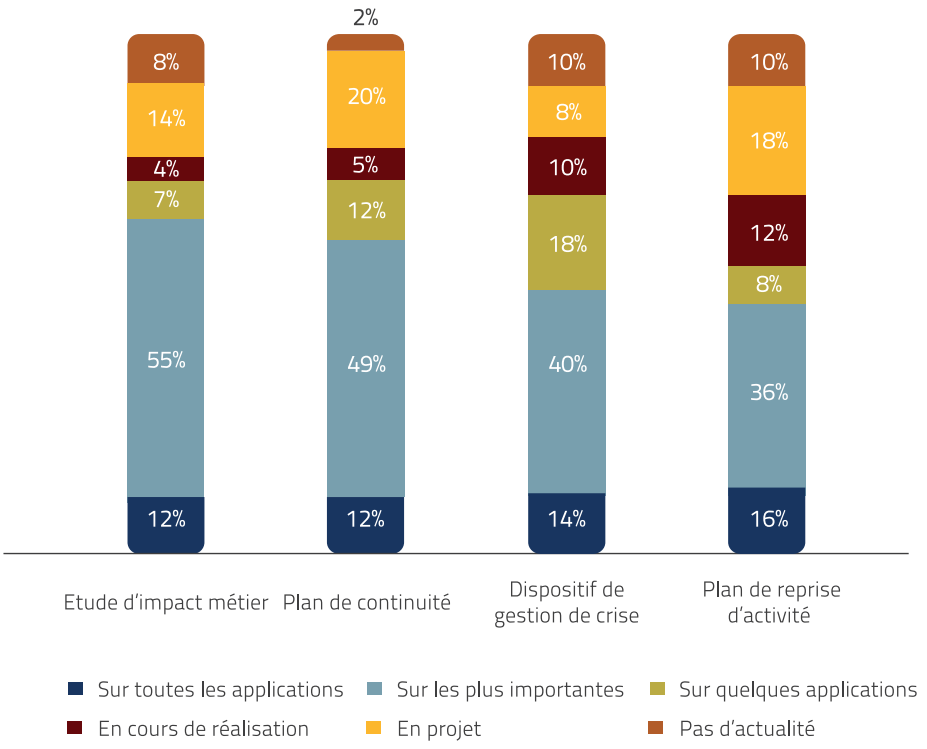
Il en ressort que les systèmes d'information sont perçus comme un risque diffus plus que comme un risque spécifique suivi comme tel. Dans la plupart des cas, il apparaît que cette discussion sur les risques numériques se fait notamment à l'occasion de grands projets de transformation et qu'elle ne constitue pas un exercice récurrent.

Malgré 11 cas où le sujet n'est pas traité, on note une bonne sensibilisation aux risques de la Cybercriminalité notamment au niveau du COMEX, du Comité d'Audit, du Comité des Risques et des responsables Métiers.

En ce qui concerne le degré d'imbrication des risques SI et métiers, il est considéré comme fort voire total dans au moins 45% des cas, exemples à l'appui : interruption des chaînes de production, des télécommunications par exemple.

Interrogés sur les mesures d'anticipation en place, les DSI semblent concentrer leurs efforts sur les applications les plus importantes, en privilégiant les analyses d'impact, suivies des plans de continuité, des dispositifs de gestion de crise et des plans de reprise d'activité. Mais le schéma ci-après ***(voir Figure 11)***

FIG 11. MESURES D'ANTICIPATION



montre que beaucoup de progrès sont à réaliser dans ce domaine.

Les raisons invoquées pour l'absence de dispositifs sont diverses : manque de motivation des métiers, maturité insuffisante, absence de prise de décision.
S'agissant de la maintenance de ces différents dispositifs :

- Les plans de continuité sont testés tous les ans ou plus souvent dans un cas sur deux,
- Les dispositifs de gestion de crise sont testés annuellement ou plus dans deux cas sur trois,
- Les plans de reprise d'activité sont testés annuellement ou plus dans 3 cas sur 4.

Concernant la sécurité des systèmes d'information proprement dite, les entreprises ont souvent mis en place un ensemble très complet de mesures visant à se protéger contre les risques généraux ou spécifiques :

- Parmi les mesures les plus courantes : la définition d'une politique ou d'un plan de sécurité, la nomination d'un RSSI, le déploiement d'outils de contrôle ou la mise en place d'un programme de formation à destination des utilisateurs. Plus récente, la création de SOC (*Security Operation Centers*) est également mentionnée.
- Parmi les autres mesures spécifiques citées, notons les tests d'intrusion et les audits ISO 27001.

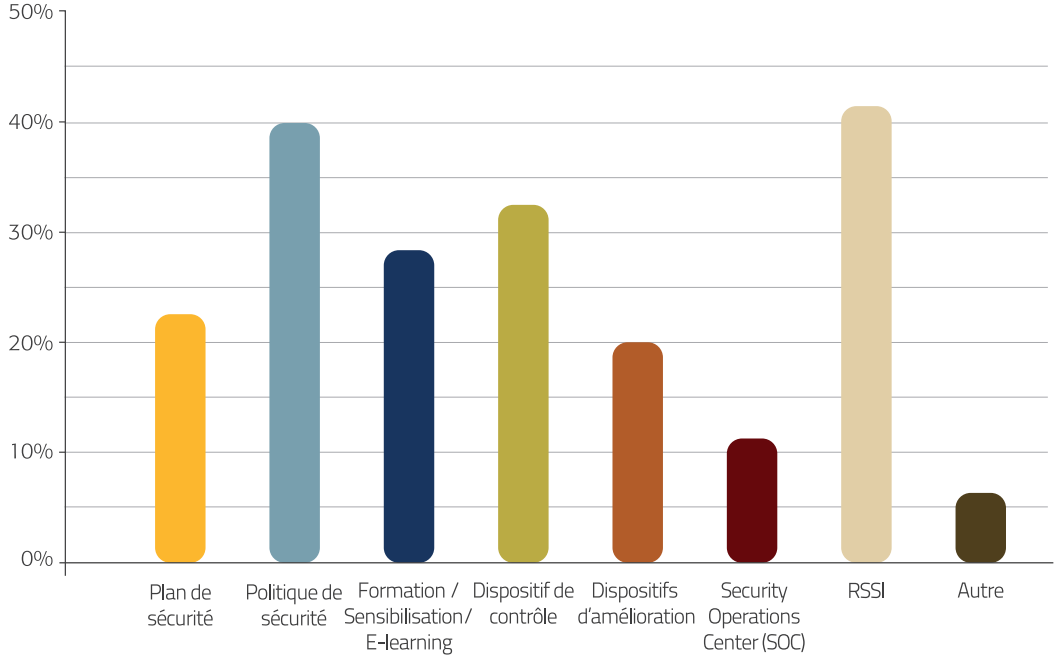
Les améliorations prévues pour une meilleure maîtrise des risques sont très larges, à savoir : une gouvernance unifiée des risques, des tableaux de bord sécurité assortis de *KPIs*, la généralisation des PCA et PRA, un *serious game* sur la cybersécurité (à l'image de celui développé pour le compte du CIGREF), un programme de sensibilisation des métiers. La ***Figure 12*** récapitule ces mesures.

En ce qui concerne les mesures d'audit dont les DSI font l'objet, les réponses soulignent une généralisation de ces pratiques sur un grand nombre de sujets, et avec une fréquence significative :

- Les audits applicatifs sont fréquents, à un rythme quasiment annuel,
- Les audits de sécurité se pratiquent plusieurs fois par an,

FIG 12. ÉLÉMENTS MIS EN PLACE EN TERME DE SÉCURITÉ INFORMATIQUE

(PLUSIEURS RÉPONSES POSSIBLES)



- Les cartographies des risques se font à un rythme plus variable,
- La revue de la gouvernance informatique est plus rare (tous les 2 à 5 ans),
- Les revues de maturité de processus sont peu fréquentes,
- Les revues de conformité sont en majorité annuelles,
- Les revues de licences se font presque tous les ans, voire plusieurs fois par an,
- Les revues de projet sont peu fréquentes
- Les audits de conformité de tiers restent l'exception,
- Pour les autres revues, beaucoup citent les tests d'intrusion, les audits SOX, les PCI/DSS, les diagnostics d'Audit interne.

Par contre, il est intéressant de noter que les DSI eux-mêmes ne commanditent pas beaucoup d'audits et que le spectre de ces derniers est plus ciblé : tests d'intrusion, revues de code, diagnostics de sécurité, revues tierces, audits de coût ou d'organisation.

S'agissant des relations avec les différents partenaires de la gestion des risques, elles semblent encourageantes : jugées bonnes avec la Direction Générale, elles sont bonnes voire excellentes avec l'Audit interne, et bonnes avec l'Audit externe. A ce sujet, de nombreux interlocuteurs ont souligné le rôle constructif de l'Audit externe, qui apparaît fréquemment comme un interlocuteur régulier et utile dans les revues systématiques des contrôles généraux et des applications à caractère financier.

FOCUS SUR LA MAÎTRISE DES COÛTS

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

CHAPITRE N. 4

FOCUS SUR LA MAÎTRISE DES COÛTS

TRIBUNE AFAI : MAÎTRISER LE *RUN* ET OPTIMISER LE *BUILD*

Les systèmes d'information restent pour de nombreuses directions d'entreprise un sujet complexe dont on ne sait pas toujours quoi penser. Au-delà de la qualité des services bureautiques, intuitivement mesurable, les systèmes de l'entreprise sont-ils bien adaptés ? Ne sont-ils pas trop complexes ? Trop chers ? Sont-ils un atout ou plutôt un frein ? Le fait d'évoquer si souvent l'alignement de l'informatique avec le Métier comme un facteur clé de succès illustre bien que cet alignement ne va pas de soi. Même si cet alignement est la priorité absolue en termes de contribution de l'informatique à la création de valeur pour l'entreprise, il est également important de maîtriser les indicateurs économiques qui lui sont attachés : le contrôle des coûts d'une part, et l'atteinte des bénéfices Métier d'autre part.
Pour ce faire, il est indispensable de répartir les activités de l'informatique en 2 volets, qu'il importe de bien distinguer, car chacun relève d'un mode de gestion complètement différent :

01 ***Run*** (produits/services récurrents) : comme pour une usine de production, il s'agit de produire à moindre coût pour un niveau de qualité donné. L'évolution dans le temps du coût unitaire des produits/services, pour un niveau de qualité égal, est alors l'indicateur de productivité et donc de performance dans la gestion de cette partie du budget.
Le calcul du coût unitaire des produits/services fournis par la DSI à ses clients est également essentiel pour pouvoir établir le rapport « qualité/coût » des services en corrélant leur coût avec le niveau de qualité convenu et formalisé dans des contrats de niveau de service (SLA).

Pour établir cette corrélation, la mise en œuvre d'un catalogue de « services clients » fournis par l'informatique à ses clients internes est donc un prérequis, car sans lui aucun rapprochement pertinent entre qualité et coût n'est possible.
Une fois le catalogue établi en commun entre la DSI et ses clients, il est indispensable d'analyser les coûts de la DSI par activité (ex : ***hot line***) pour pouvoir valoriser le coût complet du « service client » (ex : mise à disposition de l'application X). C'est alors que démarches de type ABC *(Activity Based Costing = Valorisation basée sur les activités)* prennent toute leur signification en permettant de calculer ces coûts complets *(TCO = Total Cost of Ownership)* sur les bases les plus factuelles possibles.

En l'absence de standards établis, le CIGREF et l'AFAI ont défini, dans le cadre de l'IGSI (Institut de la Gouvernance des Systèmes d'Information), un modèle dit « modèle de ***benchmarking*** des coûts informatiques ». Ce modèle s'appuie sur un référentiel technico-économique qui normalise les ressources (personnel, prestations externes, matériels, logiciels, ...), les activités (hot line, maintenance, développement, réseau, gestion administrative, ...) et les « services clients » de la DSI (mise à disposition de postes de travail, mise à disposition d'applications, projets techniques et Métiers,...).

Ce modèle, basé sur les principes de la démarche ABC, vise non seulement à faciliter les comparaisons entre entreprises pour dégager des pistes d'amélioration, mais aussi à élaborer en interne des coûts unitaires sur la base d'un modèle reconnu afin qu'ils ne soient pas sujets à caution et qu'ils puissent faciliter ainsi le dialogue entre les différentes parties-prenantes du SI.
Disposer d'un calcul de coûts étayé par des éléments factuels et s'appuyant sur un modèle reconnu est une condition « sine qua non » pour pouvoir prendre, en connaissance de cause, des décisions, aussi bien à caractère opérationnel telles que l'ajustement de la production des services au niveau de qualité requis ou encore leur facturation interne, qu'à caractère stratégique telles que l'externalisation de tout ou partie de tel ou tel service… A ce titre, c'est donc un facteur de progrès très puissant.

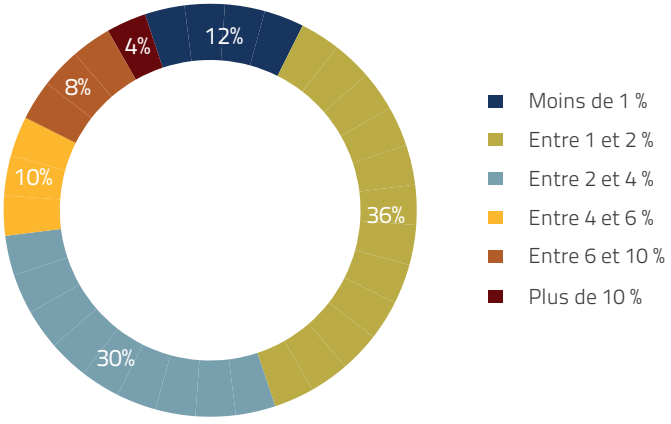
02 ***Build*** (Projets de transformation et d'adaptation) : les projets obéissent à une logique complétement différente de celle de la production. Il s'agit, cette fois, d'un investissement pour le futur, dont l'entreprise est en droit d'attendre un « retour » en termes de « création de Valeur », soit sous forme de gain financier, soit sous une forme plus qualitative (amélioration de la traçabilité, réduction des délais de développement, etc…). Dans le contexte de la « transformation numérique », il en va même de la compétitivité de l'entreprise voire de sa survie.
Le lancement de tels projets métiers ayant une composante SI significative est donc une décision de la Direction Générale et des Directions Métiers, après consultation de la DSI. En aucun cas, il ne peut s'agir d'une décision de la seule DSI.

Pour que la DG puisse arbitrer entre les projets, en toute connaissance de cause, il est indispensable que ceux-ci soient présentés, dans le cadre d'une gestion globale d'un portefeuille de projets, sous la forme d'un « *business* case » validé à la fois par les Directions Métiers et par la DSI.
Une fois la décision de lancement prise par la DG, la DSI sera responsable du respect des aspects « Coût, Délai, Qualité » des projets lancés et de leur impact sur le Budget Informatique. Toutefois l'impact principal sur le Budget Informatique provient évidemment de la décision de lancer ou non tel ou tel projet.

La négociation budgétaire, qui va allouer les ressources de l'entreprise à l'informatique, doit donc évidemment tenir compte de ces deux volets distincts et de leurs caractéristiques propres notamment en termes de responsabilité dans l'engagement de la dépense.
À iso budget, il est évidemment souhaitable de réduire le volet « ***Run*** » par des actions de type mutualisation, *benchmarking,* externalisation, simplification du parc applicatif,… pour pouvoir consacrer davantage de ressources aux projets de transformation indispensables à sa survie, notamment dans le contexte de l'économie numérique.

ANTOINE VIGNERON
SECRÉTAIRE GÉNÉRAL DE L'AFAI

FIG 13. BUDGET ENTRE 1 ET 4% DU CA



LES DSI VEULENT MIEUX CONNAÎTRE ET MAÎTRISER LEURS COÛTS

Près de 75% des répondants ont des budgets SI inférieurs à 4% de leur chiffre d'affaires. ***(voir Figure 13)*** Les organisations publiques et les établissements financiers sortent de cette fourchette :

- Les premières raisonnent en budget et non en chiffre d'affaires,
- Les seconds peuvent avoir, selon la taille de l'établissement, un montant très élevé en valeur absolue, mais minime en pourcentage du produit net bancaire ou, très fort en valeur relative pour des établissements de taille modeste.

Dans 44 % des cas, le budget DSI n'est pas mis en rapport avec les frais généraux, ce qui confirme un faible recours à cet indicateur dans l'analyse des coûts informatiques. Les DSI interrogés nous ont confirmé ce point, en nous confiant que leur Direction Générale leur demandait rarement de commenter ce pourcentage.

Pour les 56% de DSI qui suivent cet indicateur, on observe ***(voir Figure 14)*** :

- 16% ayant un budget à moins de 10% des frais généraux,
- 30 % ayant un budget entre 10 et 20% des frais généraux,
- 10% dépassant 20% des frais généraux.

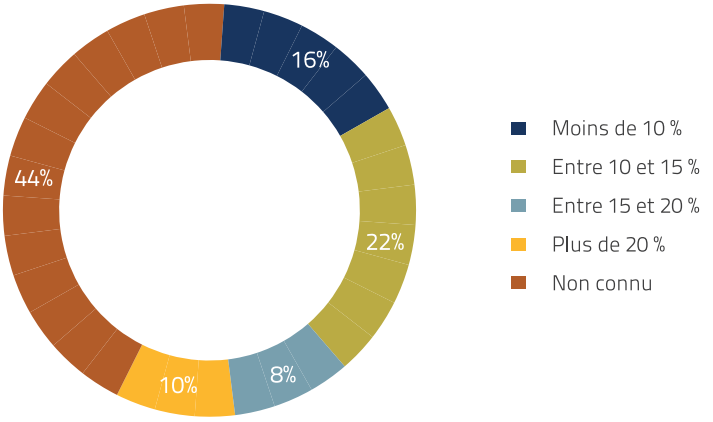
LA PART RESPECTIVE RUN/BUILD EST MIEUX CONNUE QUE LA PROPORTION OPEX/CAPEX

15% des entreprises n'ont pas su donner une estimation de la répartition entre leurs coûts projets et leurs coûts récurrents (ou coûts de fonctionnement). Environ 30% des répondants ne savent pas non plus déterminer la part des OPEX / CAPEX de leur budget. Une telle situation prouve qu'en dépit des efforts réalisés, les DSI peuvent encore progresser dans la connaissance précise des coûts IT. Cela peut se faire grâce au concours de la Comptabilité Générale et du Contrôle de gestion.

Pour les entreprises qui ont répondu ***(voir Figure 15)***, on observe :

- Une répartition moyenne de 35% pour les coûts projets et 65 % pour les coûts de fonctionnement. Cette répartition est homogène car seules 10% de ces entreprises allouent jusqu'à 50% (et plus) aux coûts projets.
- Une répartition moyenne de 66% des charges en OPEX et 34% en CAPEX : cette répartition est moins homogène que dans le cas précédent - les charges en OPEX par exemple varient de 20 à 95 %. Il est à prévoir que le développement du SaaS aura un impact non négligeable sur cette proportion.

FIG 14. BUDGET PEU RAPPORTÉ À CELUI DES FRAIS GÉNÉRAUX



Investissements logiciels / Matériels

Dans plus de 80% des cas, la DSI maîtrise les investissements logiciels et matériels. Si l'investissement échappe à son contrôle, il s'agit souvent de cas prévus tels que :

- une procédure simplifiée,
- un logiciel très spécialisé dans le métier concerné,
- un recours métier à une solution SaaS,
- une réponse à une spécificité locale.

L'enquête ne nous a pas permis d'établir la part relative des montants d'investissements non maîtrisés par la DSI.

La forte décentralisation d'un groupe ou l'adoption d'une gouvernance d'entreprise différente peut également conduire à des investissements non directement traités par la DSI (*in-business computing*).

Statistique de fonctionnement

Le recours aux équipes externes est très généralisé, puisque ces dernières représentent en moyenne un tiers des effectifs. Au global, 70% des répondants estiment que leurs ressources informatiques correspondent à leurs besoins. Pour les autres, ce besoin identifié avoisine 25% des ressources en place.

FIG 15. UNE LARGE PARTIE DU BUDGET DÉDIÉE AUX COÛTS DE FONCTIONNEMENT

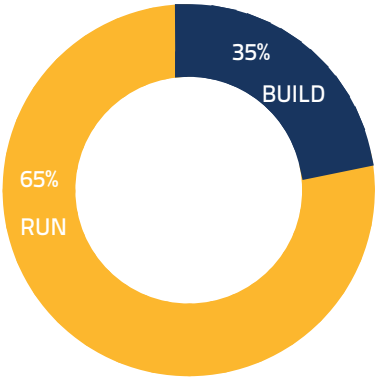
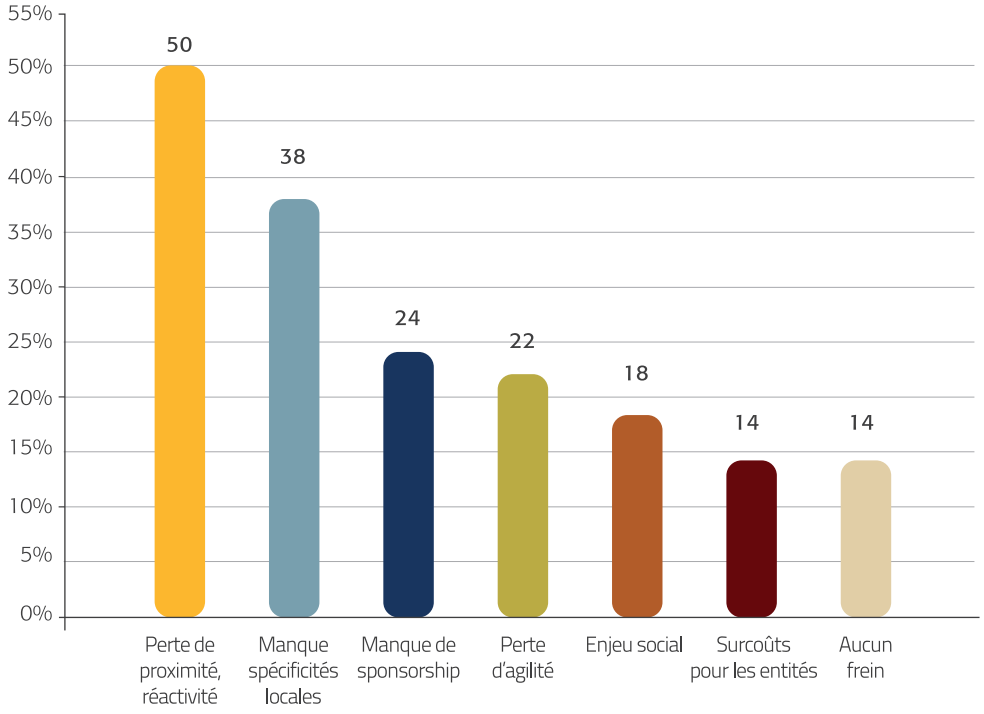


FIG 16. FREINS RENCONTRÉS POUR LA MISE EN PLACE DE LA MUTUALISATION

(PLUSIEURS RÉPONSES POSSIBLES)



Les compétences identifiées comme manquantes recouvrent plusieurs cas de figure :

- Sécurisation de l'existant : expertises spécifiques sur des technologies ***mainframe*** par exemple, administration système, réseau, bases de données et sécurité SI.
- Evolution et Innovation : architecture, urbanisation, expertises Cloud ou SaaS, Big Data, méthodes agiles, nouvelles technologies et numérique.
- Renforcement de la relation avec les métiers et du PMO, grâce à des chefs de projets polyvalents et de bon niveau.

LA MUTUALISATION CROISSANTE CONTRIBUE À UNE MEILLEURE MAÎTRISE DES COÛTS

Une majorité d'entreprises (75%) a globalisé plus de la moitié de ses services informatiques entre le groupe et ses filiales.

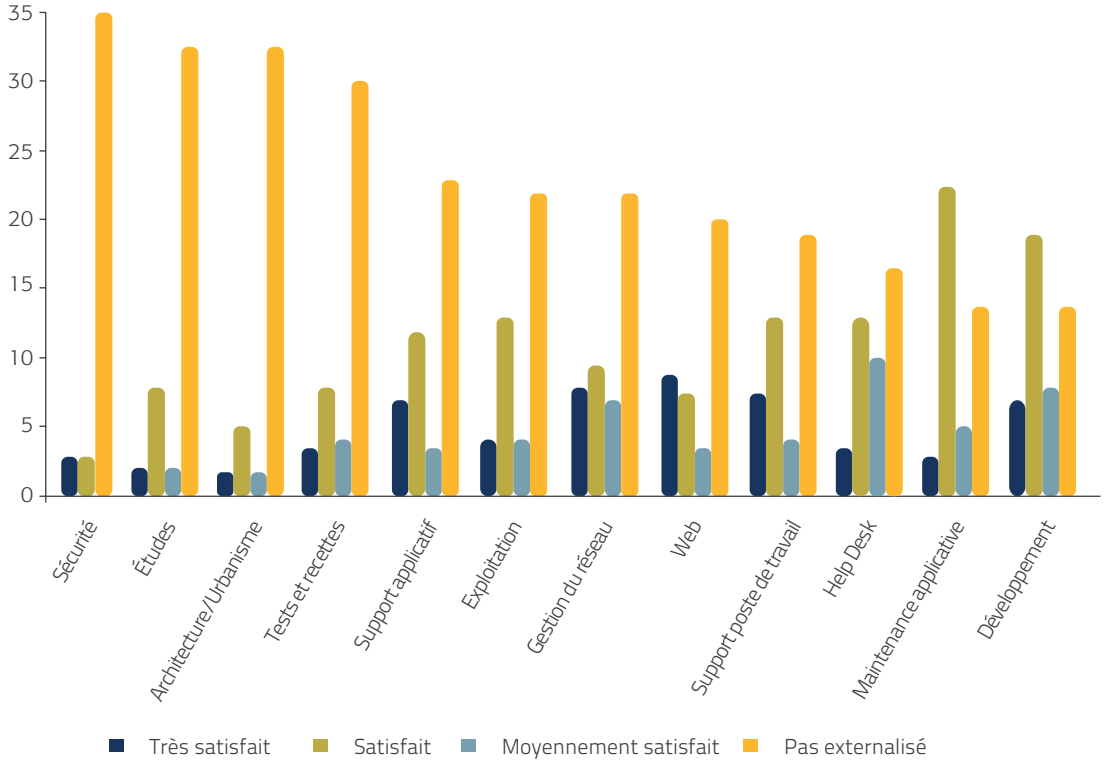
De la même façon, les entreprises qui ont répondu à notre questionnaire envisagent généralement de renforcer cette globalisation. Ne pas renforcer cette globalisation correspond à une décision stratégique ou à un potentiel maximal déjà atteint (globalisation à 100%).

UN APPSTORE INTERNE EST EN COURS DE RÉALISATION POUR FAIRE CONNAÎTRE ET VALORISER LES APPLICATIONS LOCALES .

ANNIE PRÉVÔT, DSI CNAF

FIG 17. EXTERNALISATION DE FONCTIONS ET NIVEAU DE SATISFACTION EXPRIMÉ

(NOMBRE DE RÉPONDANTS)



Les éléments principaux déjà mutualisés sont les infrastructures, le réseau, le support et les applications transverses telles que les ERP.
Les freins rencontrés à la mutualisation sont pour la plupart liés à la crainte ***(voir Figure 16)*** :

- De la perte de proximité, de réactivité,
- Que les spécificités locales ne soient pas complètement prises en compte.

Pour autant près de 14% considèrent qu'aucun frein n'a entravé la mise en place de cette globalisation, comme en témoigne la ***Figure 16*** .

LE RECOURS À L'EXTERNALISATION RESTE TRÈS SÉLECTIF

Les entreprises ayant répondu externalisent peu l'architecture /urbanisme, les études et la sécurité. ***(voir Figure 17)*** Nous n'avons pas trouvé de lien apparent entre cette faible externalisation et la taille des entreprises considérées.

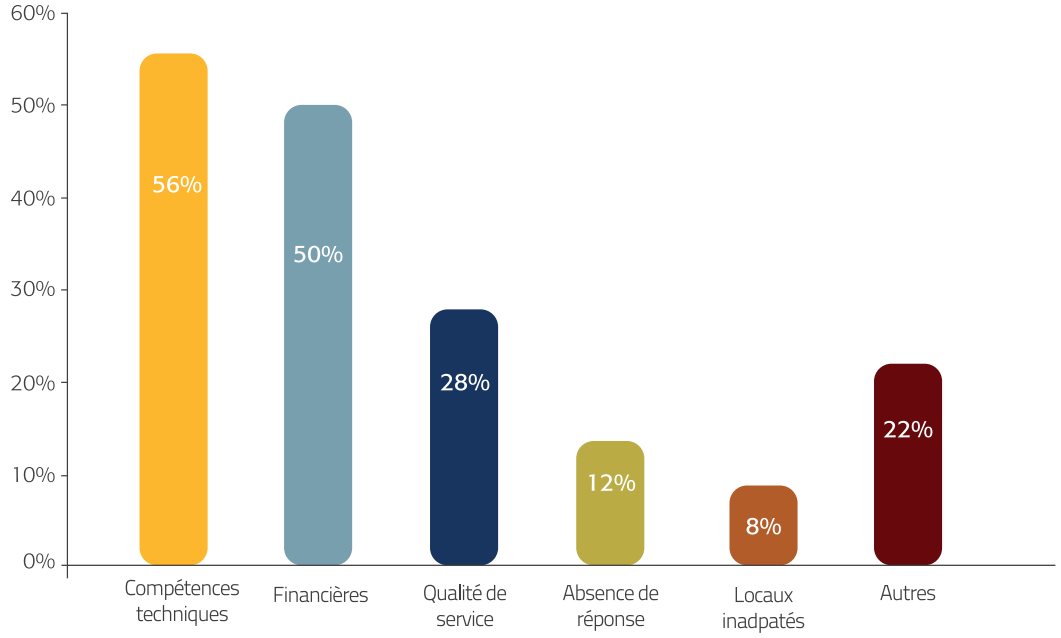
Par contre le développement, la maintenance applicative et le support (niveau 1 et poste de travail) sont des fonctions largement externalisées.
Le taux de non satisfaction exprimé (peu ou pas du tout satisfait) paraît faible ; pour autant on constate des potentiels d'amélioration du service pour le ***Help Desk***, le Développement applicatif et de la gestion du réseau.

Les préconisations recensées portent sur :

- Une plus grande proximité des infogérants avec le métier passant également par une diminution du taux de rotation des prestataires,
- Une meilleure maîtrise des processus externalisés et des contrôles renforcés à mettre en place (détection d'une sous-traitance mise en place par l'infogérant)

FIG 18. LES RAISONS QUI AMÈNENT À EXTERNALISER

(PLUSIEURS RÉPONSES POSSIBLES)



LES RAISONS QUI POUSSENT À EXTERNALISER APPARAISSENT CONTRASTÉES

Les raisons qui poussent les entreprises à externaliser ***(voir Figure 18)*** sont essentiellement de deux ordres : financières ou liées au manque de compétences techniques. Les répondants sont néanmoins conscients du fait qu'une insuffisance de compétences techniques peut constituer un handicap quand il s'agit de suivre ou de bien piloter une externalisation. La recherche de qualité des services est également citée dans les raisons qui poussent à externaliser.

Enfin, dans la rubrique « Autres » du tableau, on trouve des raisons liées à la politique RH ou au mode d'exécution du service.

LE CATALOGUE DE SERVICES SE GÉNÉRALISE

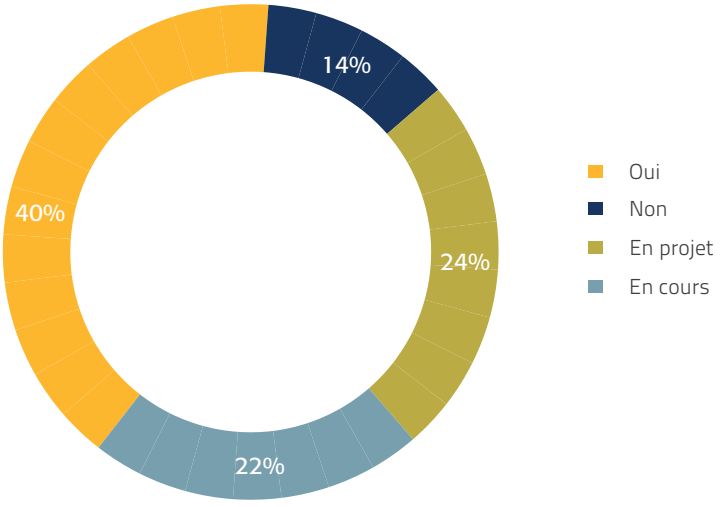
Le catalogue est devenu un référentiel répandu au sein des DSI. Il permet de décrire, de manière normalisée, les services fournis par la DSI et d'y affecter des niveaux de services et des coûts ***(voir Figure 19)*** :

- Plus de 40% des entreprises possèdent un catalogue

NOUS AVONS DÉVELOPPÉ UNE RÉELLE MAÎTRISE DES PROCESSUS DE TIERCE RECETTE APPLICATIVE, CE QUI NOUS PERMET DE TESTER NOS SYSTÈMES D'UNE MANIÈRE RIGOUREUSE SANS POUR AUTANT REMETTRE EN CAUSE LEURS DÉLAIS DE LIVRAISON.

FRANCK TARRAGNAT, DSI M6

FIG 19. POSSESSION D'UN CATALOGUE DE SERVICE



de services,
- 45% des entreprises sont en cours de mise en place du catalogue ou ont en projet de le faire,
- Seules 14% des entreprises n'envisagent pas d'engager des travaux de mise en place de catalogue.

Nous ne disposons pas d'information sur l'exhaustivité des catalogues de services, mais les entretiens menés nous ont permis de constater qu'un grand nombre de ces catalogues sont loin d'être exhaustifs. Beaucoup d'entre eux se limitent aux prestations de fourniture, mise en place et support des postes de travail, serveurs ou autres éléments d'infrastructure.

La **performance des services rendus** est mesurée dans 70% des cas, au travers de *SLA* et de *KPI*. Son suivi est alors piloté de manière généralisée au travers de la combinaison :

- D'utilisation d'outil de *ticketing*,
- De publication de tableaux de bord,
- De réunions avec les métiers.

L'USAGE D'UN CONTRÔLE DE GESTION APPROFONDI N'EST PAS ENCORE RÉPANDU

Le calcul du coût de revient des activités n'est pas généralisé : 40% des entreprises ne le font pas, ce qui signifie que leur catalogue de services est davantage un outil de communication en interne qu'un outil de pilotage des coûts. A ce titre, nous avons constaté que 60% des entreprises disposant d'un catalogue de services n'avaient pas de système de calcul des coûts informatiques.

Les entretiens avec les DSI ont révélé qu'il n'y a pas nécessairement un alignement strict entre calcul des coûts, catalogue de services et refacturation : autrement dit, certains catalogues de services ne s'appuient pas sur une analyse exhaustive des coûts, et ne servent pas de base à leur refacturation. Par ailleurs, la refacturation des coûts se fait encore souvent de façon empirique, par grandes masses.

Pour les entreprises qui calculent ces coûts (30% au total), les outils à disposition sont peu connus de la DSI et il

NOTRE SCHÉMA DIRECTEUR INFORMATIQUE A ÉTÉ VOLONTAIREMENT CENTRÉ SUR LA RÉDUCTION DES COÛTS ET L'AGRÉGATION DES INITIATIVES ISOLÉES (I*N BUSINESS COMPUTING*). A TITRE D'EXEMPLE, LA VIRTUALISATION DES SERVEURS DANS LE CLOUD PRIVÉ A PERMIS D'ATTEINDRE EN DEUX ANS UNE ÉCONOMIE DE 70% DES COÛTS INITIAUX.

JEAN-LUC AMAGAT, DSI NEXTIRA ONE

s'agit principalement d'Excel lorsque ce n'est pas traité directement par le contrôle de gestion. Le questionnaire ne nous a pas permis d'établir si ces coûts faisaient l'objet d'un ***benchmark*** avec les coûts des solutions externalisées. Par contre nous avons noté au cours de nos entretiens de bonnes habitudes de collaboration entre DSI et contrôle de gestion pour l'établissement des budgets et les calculs de prix de revient.

Refacturation des coûts informatiques

Plus de la moitié des entreprises refacturent leurs coûts informatiques.

Pour celles qui ne le font pas, les raisons sont diverses :

- L'intérêt de cette pratique ne semble pas pertinent au regard de la taille de l'entreprise,
- Il existe un frein culturel,
- La difficulté technique de mise en place est jugée importante,
- Le pilotage est effectué au travers du budget.

Fonction Contrôle de gestion intégrée à la DSI

Plus de la moitié des entreprises répondantes disposent d'une fonction contrôle de gestion intégrée à la DSI. Cette fonction prend deux formes :

- Quelques (de 1 à 4) personnes intégrées aux équipes DSI,
- Un service au sein du département informatique pouvant aller jusqu'à 80 personnes

Il reste cependant 30 % des entreprises qui ne voient pas l'intérêt d'une fonction Contrôle de Gestion (ce n'est ni en place ni en projet).

Mesure de réduction de coûts

De manière prépondérante, les réductions s'opèrent :

- Par centralisation et mutualisation (serveurs, messageries, téléphonie…)
- Par renégociation des contrats avec le support du département des achats.
- Mais aussi par le recours à certaines pratiques ou approches :
  - *Offshoring*,
  - Infogérance, externalisation, CSP,
  - Virtualisation, Cloud, SaaS.

De façon moins systématique, on note aussi les mesures suivantes :

- Passage au crible des projets visant à une meilleure compréhension par le métier des coûts engagés par la DSI (arbitrage, gestion de portefeuille projet),
- Analyse qualité, pour l'augmenter sans variation du coût,
- Réalisation d'un audit des coûts,
- Recours à l'internalisation.

L'INTERNALISATION D'UN GROS CONTRAT D'INFOGÉRANCE NOUS A PERMIS DE DIVISER NOS COÛTS PAR QUATRE, AVEC UN GAIN SENSIBLE EN MATIÈRE DE RÉACTIVITÉ

FRANCK TARRAGNAT, DSI M6

SYNTHÈSE

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

CHAPITRE N. 5

L'ENTREPRISE FACE À SES ENJEUX ET RISQUES NUMÉRIQUES

SYNTHÈSE

Drôle de numéro d'équilibriste que celui du DSI, dont le rôle est d'accompagner l'évolution des métiers et l'innovation ! Il se positionne tout à la fois comme DSI stratège, *risk manager* et contrôleur de gestion, confronté aux multiples exigences de son environnement :

- Alignement stratégique sur les enjeux de l'entreprise et le *business* qu'il doit intégrer,
- Excellence opérationnelle qu'il doit atteindre,
- Conformité technique et réglementaire qu'il doit respecter,
- Evolutions technologiques, nouveaux usages qu'il doit accélérer.

Le DSI stratège s'appuie sur des schémas directeurs, points d'ancrage d'une vision à long terme et d'une trajectoire mieux maîtrisée de son SI par une urbanisation fonctionnelle, applicative et technique devenue prioritaire.

Il doit conjuguer à la fois cohérence et agilité entre patrimoine SI et innovation, et il a pris conscience de l'impérative nécessité de faire évoluer son modèle d'affaires. Les enjeux d'innovation, loin d'être uniquement technologiques (Systèmes Multi-Agents Coopératifs, réseaux sociaux, mobilité, *Big Data*, *Cloud*, objets connectés, SAAS..) sont également méthodologiques (la méthode agile, le *real time develops*, le *co-design*,...).

La prise en compte de l'expérience client et la personnalisation de la relation client doivent maintenant être pour lui des enjeux majeurs. Il doit avoir une vision marketing, encourager le *time to market*, le cross canal, la dématérialisation des processus, et se positionner comme un véritable *business partner*.

En parallèle aux enjeux de performance opérationnelle, le DSI *risk manager* doit maîtriser l'ensemble des risques, s'appuyer plus sur des référentiels de bonnes pratiques : ITIL, ISO 2700x, CMMI ou COBIT5, ce dernier étant encore insuffisamment connu et utilisé.

La culture du risque apparaît clairement insuffisante dans de nombreuses entreprises même si elle se développe sous l'impulsion combinée du DSI, du directeur de l'audit, du *risk manager* ou du RSSI. Le risque SI est perçu mais bien insuffisamment au regard des menaces liées au numérique.

Le DSI doit intégrer la gestion des risques au portefeuille de projets, il doit systématiser la revue des risques. La confiance indispensable à la transformation numérique nécessite une communication et un accompagnement important, sans oublier la mise en place de *KPI* permettant d'agir simplement et efficacement pour réduire les risques. Les *serious games* peuvent être utilisés à profit pour sensibiliser les utilisateurs aux différentes menaces.
Le DSI contrôleur de gestion va accompagner la

transition numérique tout en améliorant la qualité de service et en optimisant les coûts. Le schéma directeur précédemment évoqué est également un outil de maîtrise des coûts.

De nombreuses mesures ont déjà été prises : négociation des achats, politique de *licencing*, stratégie de *sourcing*. Mais le sujet est loin d'être épuisé et les entreprises continuent d'affiner le contrôle budgétaire : renforcement de la globalisation (Centre de Services Partagés), mutualisation des moyens, externalisation de la messagerie et de certaines applications, parfois internalisation de quelques services critiques, utilisation du catalogue de services comme outil de gestion, challenge en continu des prestataires.

La méthode ABC et le Lean IT donnent des résultats intéressants. Le « modèle de *benchmarking* des coûts informatiques », initialement développé en commun par l'AFAI et le CIGREF et basé sur la méthode ABC, est un outil efficace d'aide à la décision pour détecter les pistes d'amélioration les plus pertinentes en facilitant les comparaisons avec d'autres entreprises ou avec les bonnes pratiques du marché.

Le DSI doit évaluer son portefeuille d'actifs SI en termes de création de valeur, de risques et bien entendu de retour sur investissement. Tout projet non stratégique ou réglementaire doit justifier d'un ROI rapide. Il reste encore un *cost killer* sur l'existant afin d'investir plus facilement sur le numérique.
Un vrai numéro d'équilibriste !

ANTOINE VIGNERON
SECRÉTAIRE GÉNÉRAL DE L'AFAI

ANNEXES

L'ENTREPRISE FACE À SES ENJEUX
ET RISQUES NUMÉRIQUES

MÉTHODOLOGIE

Cette consultation a été réalisée sur la base d'un questionnaire à destination des DSI et des Responsables de la gouvernance informatique.

Le questionnaire proprement dit est inspiré du Guide d'Audit de la Gouvernance des Systèmes d'Information (AFAI/IFACI/CIGREF, 2011) ; 3 vecteurs du guide ont été utilisés pour formuler les questions :
- Vecteur 2 : Urbanisation et architecture du SI de l'entreprise au service des enjeux stratégiques,
- Vecteur 4 : Management des risques SI en fonction de leurs impacts « métiers » et des bonnes pratiques associées,
- Vecteur 5 : Alignement de la fonction informatique par rapport aux processus métiers.

La mise au point du questionnaire a fait l'objet de nombreux échanges au sein du Comité de Pilotage, son articulation finale reposant sur les 3 priorités des DSI ressortant d'une enquête CIGREF menée en 2013 :
- La stratégie numérique,
- La gestion des risques,
- La maîtrise des coûts,

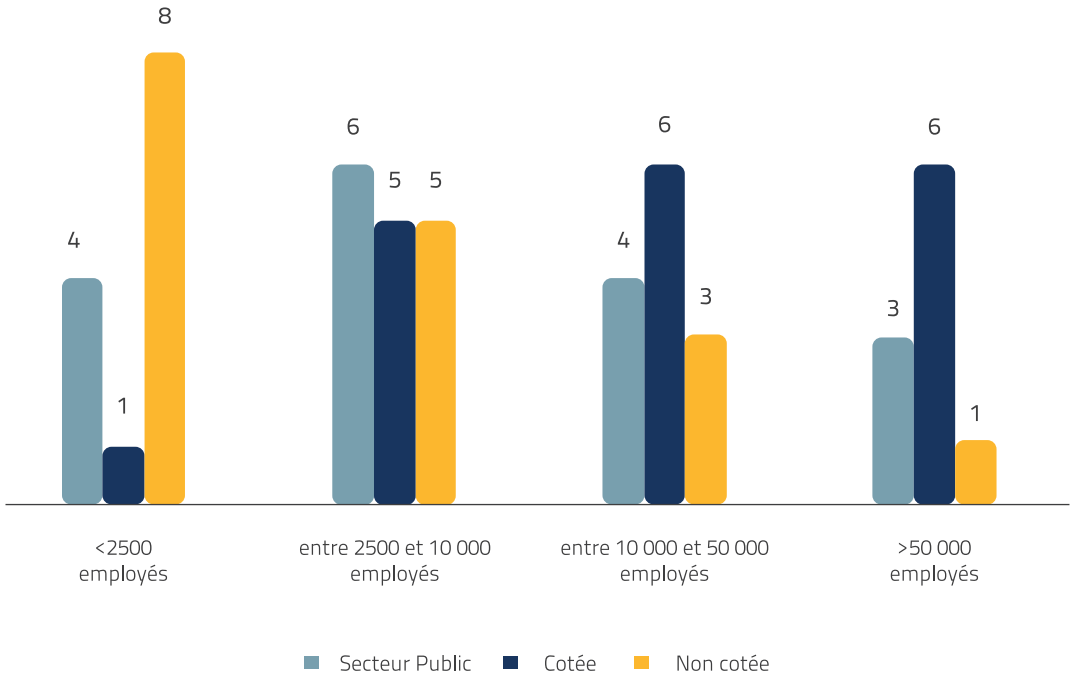
Notre questionnaire ciblait des entreprises ayant un chiffre d'affaires supérieur à 300 M€ ; certaines administrations et établissements publics de taille significative ont également été consultés.
Le questionnaire a fait l'objet d'une large diffusion, chaque Association l'adressant à ses adhérents. Des contacts directs ont permis au cabinet Crowe Risk Consulting de mener une quinzaine d'entretiens qualifiés auprès des DSI, lui permettant de recueillir des témoignages directs et des bonnes pratiques.
L'exploitation de l'ensemble des réponses a permis d'écrire cette étude et de faire le point sur les différentes priorités des DSI.

Soucieux de traiter de façon exhaustive la richesse de l'information recueillie, nous avons fait le choix de respecter dans le détail le fil directeur de l'enquête, afin que chaque répondant puisse retrouver les questions posées et situer sa position par rapport aux autres sociétés. Nous avons aussi décidé d'écarter les questionnaires remplis de façon incomplète et limiter notre analyse à 52 sociétés qui ont répondu à la totalité des questions.
Pour autant, afin de rester synthétiques, nous n'avons effectué des analyses de données croisées, ou des confrontations de résultats que dans la mesure où les tendances observées pouvaient paraître paradoxales ou mériter un complément d'analyse.

La consultation d'experts et de responsables informatiques a permis d'éclairer les résultats détaillés de l'enquête. La contribution de chaque association sous forme de tribune en tête de chapitre, fournit une mise en perspective et une prise de recul sur les trois axes :

- CIGREF pour la stratégie numérique,
- IFACI pour la gestion des risques,
- AFAI pour la maîtrise des coûts.

FIG 20. PROFIL DES ENTREPRISES AYANT RÉPONDU



Cartographie des entreprises qui ont répondu par effectif

Au total, 52 entreprises ont répondu à l'ensemble du questionnaire, représentant un bon équilibre entre entreprises cotées, non cotées, ou secteur public.

On constate une bonne couverture des différents segments en termes de tailles d'entreprises :

- Effectifs inférieurs à 2500 personnes : 13 répondants,
- Entre 2500 et 10 000 personnes : 16 répondants,
- Entre 10 000 et 50 000 personnes : 13 répondants,
- Au-delà de 50 000 personnes : 10 répondants.

Cette représentativité se retrouve aussi au niveau des **secteurs d'activité** :

On note toutefois une prédominance des secteurs services aux entreprises, transports, administration, assurances, énergie, santé. Des secteurs tels que banque, technologie de l'information, distribution, agro-alimentaire, chimie ou pharmacie ont répondu en plus faible nombre.
Parmi les « Autres répondants », on note: ingénierie, mécénat, jeu, secteur associatif.

Une majorité de DSI a répondu

Plus des 2/3 des répondants sont des DSI, ce qui prouve une bonne mobilisation et un intérêt porté au sujet. Parmi les autres répondants, on relève des responsables de la gouvernance informatique, quelques Directeurs d'Audit Interne, Directeurs Généraux ou RSSI.

Des DSI majoritairement rattachés à la Direction Générale

Les informations fournies par les répondants ont permis d'établir, que dans plus de 60% des cas, les DSI sont rattachées aux Directions Générales ; dans 20% des cas, elles dépendent de la Direction Financière, le reste se répartissant entre Secrétariat Général, Direction des Opérations ou Services Généraux.

FIG 21. SECTEURS D'ACTIVITÉ DES ENTREPRISES AYANT RÉPONDU

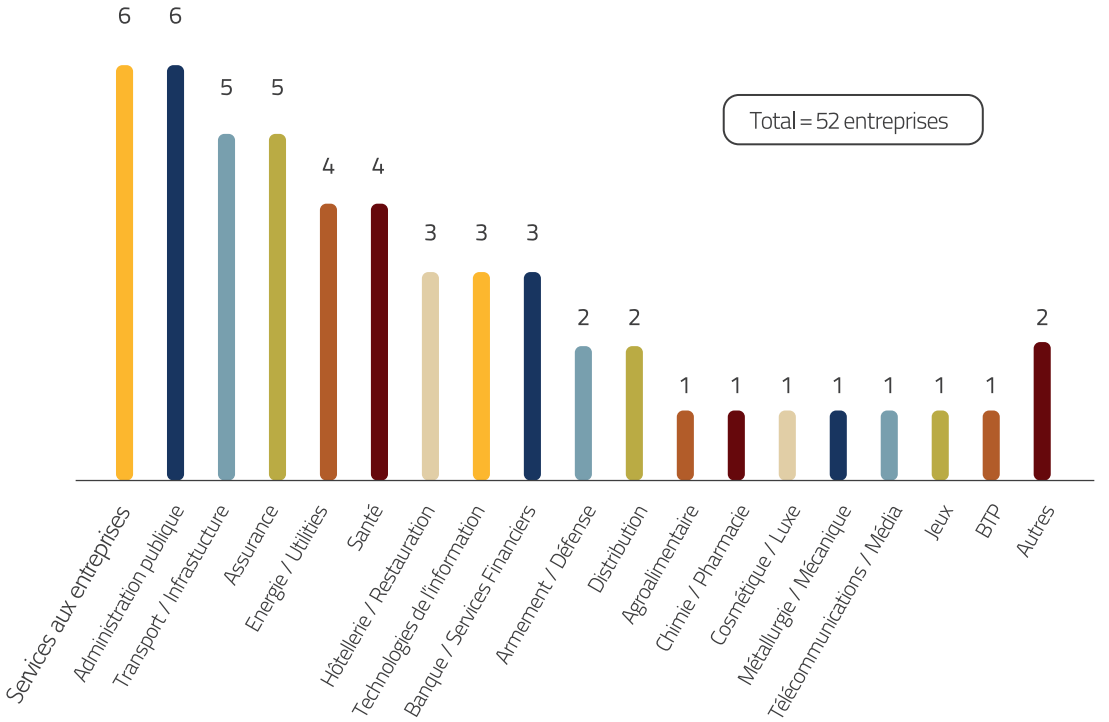


FIG 22. PROFIL DES PERSONNES AYANT RÉPONDU

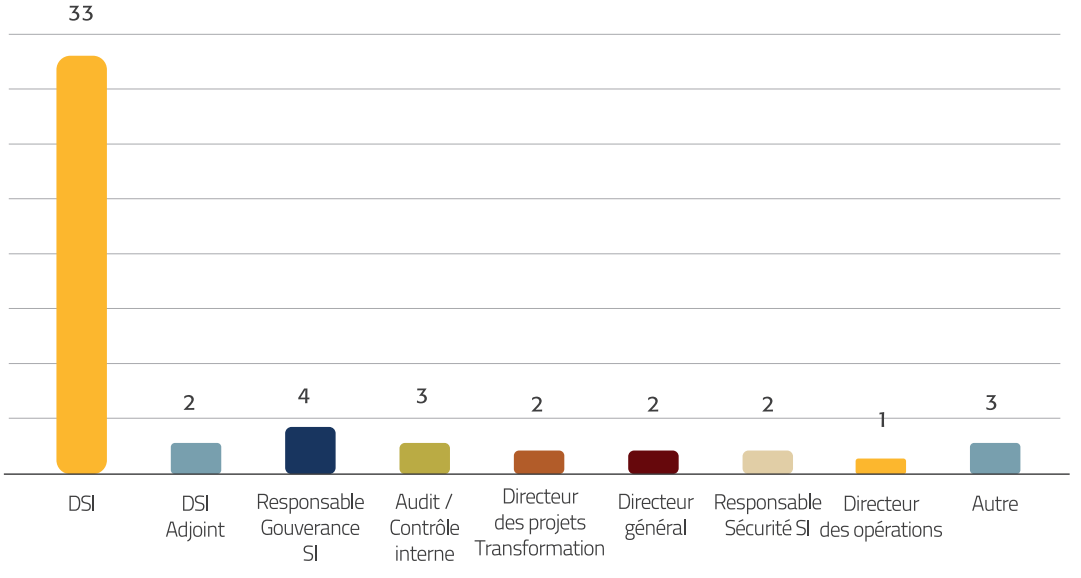
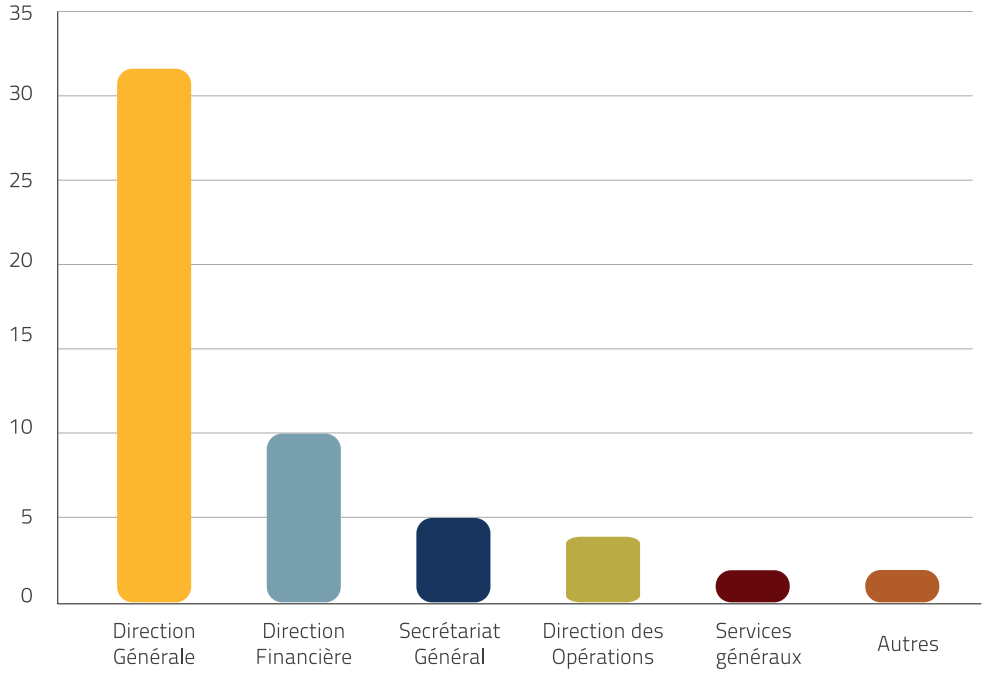


FIG 23. RATTACHEMENT DES DSI



BIBLIOGRAPHIE THÉMATIQUE

Numérique

- Entreprises et culture numérique : *www.cigref.fr/entreprises-et-culture-numerique-un-nouveau-defi*

- Cadre de référence CIGREF sur la culture numérique : *www.cigref.fr/cadre-de-reference-cigref-culture-numerique*

- Gouvernance du numérique : *www.cigref.fr/gouvernance-du-numerique-creation-de-valeur-maitrise-des-risques-allocation-des-ressources*

- Nouveaux rôles de la fonction SI : *www.cigref.fr/nouveaux-roles-fonction-si-missions-competences-marketing-de-la-fonction*

- Sûreté et risques numériques : scenario d'un serious game : *www.cigref.fr/surete-risque-numerique-scenario-serious-game*

- La sécurité numérique : *www.cigref.fr/la-securite-numerique*

- Cloud et protection des données, guide pratique à l'attention des directions opérationnelles et générales (AFAI-CIGREF-IFACI) : *www.cigref.fr/cloud-protection-donnees-guide-pratique-direction-operationnelle-generale*

- Protection de l'information et Cloud Computing : *www.entreprises-et-cultures-numeriques.org/protection-de-l-information-et-cloud-computing/*

- Les risques numériques pour l'entreprise : *www.cigref.fr/les-risques-numeriques-pour-lentreprise*

- Eduquer les acteurs de l'entreprise aux risques numériques : *www.entreprises-et-cultures-numeriques.org/eduquer-les-acteurs-de-l-entreprise-aux-risques-numeriques/*

Référentiels

- Cadre de référence international des pratiques professionnelles de l'Audit interne / IIA, IFACI – 2014. Notamment :
  - La Norme 2110.A2 – « L'Audit interne doit évaluer si la gouvernance des systèmes d'information de l'organisation soutient et supporte la stratégie et les objectifs de l'organisation ». [commentée dans la Fiche technique N°29 de la Revue Audit interne N° 199 de mars-avril 2010].
  - Les GTAGs – Global Technologie Audit Guides. IIA. (www.ifaci.com).:
  - GTAG15 : Information Security Governance
  - GTAG 17 : Auditing IT Governance

- Cobit ® 5 : Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise / ISACA – 2012

- Gouvernance du Système d'information : Guide d'audit /CIGREF / IFACI / AFAI – 2011

- Le Contrôle interne du système d'information des organisations : Guide opérationnel d'application du cadre de référence AMF relatif au contrôle interne / IFACI, CIGREF – 2009

- TOGAF ® Version 9.1: The Book. / The Open Group. I - 2011

- ITIL Version 3

Communication et système d'information

- BYOD : Quels risques et enjeux pour l'audit et le contrôle internes ? (IFACI 2014)

- Colloques « Continuité d'activité, continuité informatique et gestion de la crise : Comment maîtriser vos dispositifs ? » [Colloque du 21 mars 2012] / IFACI

- Revue Audit interne N° 206 de septembre 2011 : La gouvernance des systèmes d'information : Quel rôle pour l'Audit interne ?

- Colloques « De la gouvernance du système d'information… à la gouvernance de l'entreprise numérique : Quels enjeu pour les fonctions S.I. et Audit interne ? »[Colloque du 23 juin 2011] / AFAI ; IFACI ; CIGREF.

Gouvernance / Stratégie

- Prise de position IFA / IFACI sur le rôle de l'Audit interne dans le gouvernement d'entreprise. – 2009

- L 'Articulation gouvernance des systèmes d'information / gouvernance d'entreprise. / Georges Epinette in L'Incidence de la mise en œuvre d'un dispositif de contrôle interne sur les systèmes d'information : Du cadre de référence de l'AMF aux bonnes pratiques.

- Guide d'Audit de la Gouvernance des Systèmes d'Information, et outil associé, publication CIGREF/ IFACI/AFAI - 2011

15 RUE DE LA BAUME 75008 PARIS
+33 (0)1 53 53 03 92

WWW.CROWEHORWATHGRC.COM
CONTACT@CROWEHORWATHGRC.COM

RÉALISATION : ANTONIN LORAIN

Crowe Horwath®
Global Risk Consulting