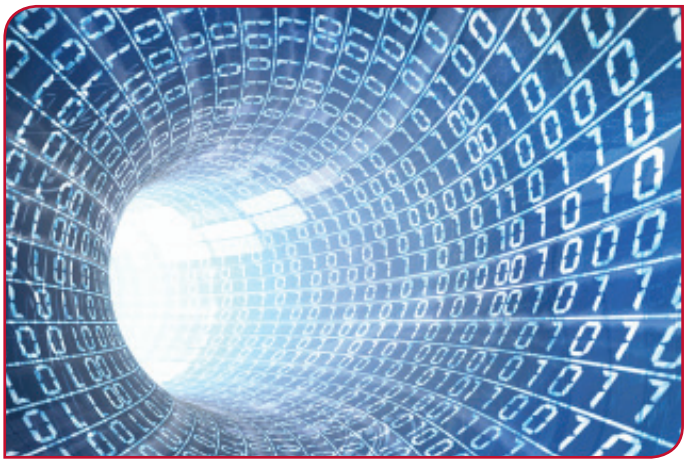
IFA Institut Français des Administrateurs

cigref Réseau de Grandes Entreprises

Le conseil d'administration et la transition numérique de l'entreprise



Qui dit informatique ne dit plus nécessairement DSI (Direction des Systèmes d'Information)... Historiquement très intégrée, la technologie informatique repose de plus en plus sur des organisations complexes, des acteurs nouveaux, et des prestations extérieures plus nombreuses.

Le terme « numérique » (et son anglicisme « digital ») devient le mot clé dans l'entreprise : il irrigue désormais l'ensemble de la chaine de valeur de l'entreprise, et va même au-delà. Les métiers Ventes, Marketing, Ressources Humaines, Innovation industrielle s'approprient progressivement les technologies de l'information. Les usages de la sphère privée pénètrent la sphère professionnelle et inversement. Les lignes bougent et poussent l'entreprise à s'ouvrir, à être plus agile et flexible et à interagir avec toutes ses parties prenantes.

Cette transformation apportée par l'univers numérique est porteuse d'opportunités qu'il ne faut pas manquer, et de risques nouveaux qu'il faut appréhender et maîtriser.

Et c'est résolument un nouveau défi pour les DSI et leurs équipes, mais aussi pour l'entreprise dans son ensemble, y compris pour son conseil d'administration, que de se saisir de ces opportunités dans une perspective de création de valeur !

Afin de mieux appréhender les opportunités et les risques associés au numérique, l'IFA et le CIGREF se sont associés pour produire ce présent guide, destiné aux administrateurs d'entreprise pour leur permettre d'ouvrir le dialogue avec les DG sur la question du numérique, tant dans les Entreprises de Taille Intermédiaire (ETI) que dans les grandes.

Le présent guide a pour ambition de présenter aux administrateurs les enjeux du numérique (partie 1), les acteurs (partie 2), les nouveaux risques (partie 3), et le cadre réglementaire de cette transformation numérique. Dans la tradition des guides de l'IFA, ce document apporte des recommandations aux administrateurs pour leur permettre d'assumer leur rôle dans cette mutation, en étant conscients des enjeux du numérique.

Daniel LEBÈGUE
Président de l'IFA

Gérard LANCNER
Président du groupe de travail
« Suivi des risques numériques »

Introduction

Présence sur les nouveaux espaces de création de valeur, prise en compte des pratiques émergentes dans la sphère sociétale, structure agile[1] et processus d'innovation ouverte, souplesse de la chaine de valeur, gouvernance et leadership…Tels sont les principaux enjeux de l'entreprise numérique. Tous ces phénomènes modifient par ailleurs de nombreux aspects de la vie en société et constituent pour les entreprises une inévitable transition numérique. Ces mutations représentent non seulement une formidable opportunité de croissance mais induisent de repenser l'entreprise, sa stratégie, son organisation et les comportements, son modèle d'affaires, tout en gérant les risques associés à cette transformation. Ainsi, le numérique est une question stratégique qui doit être traitée au plus haut niveau de l'entreprise, discutée et débattue dans les conseils d'administration, qui doivent dès lors se saisir de ce sujet. Traité dans une approche business (non pas technique), le numérique doit être positionné sur le cœur de métier de l'entreprise et à ce titre, il doit être inscrit à l'ordre du jour des conseils d'administration.

1 L'agilité s'inscrit dans une dynamique de transformation, elle est plutôt réactive. Elle est en lien avec la création de valeur et correspond à la capacité du SI à faire face à l'imprévu, à intégrer des événements inattendus, qui n'ont été ni envisagés, ni imaginés. L'agilité dans le monde numérique est « directement liée à l'accélération du temps, à l'immédiateté et aux nouvelles attentes des clients et des autres parties prenantes ». Cf. Entreprises et Culture Numérique, CIGREF, (2013), p. 76.

Les administrateurs doivent avoir conscience de l'importance de l'enjeu du numérique, or cette question ne se pose pas encore assez dans les conseils d'administration... Pourtant, la transition numérique à l'œuvre actuellement dans nos entreprises comme dans notre société, dans nos vies personnelles, nos loisirs… semble marquer un changement de paradigme. C'est l'ensemble des tendances décrites précédemment qui, considérées de manière interdépendante, modifient profondément le monde dans lequel nous vivons et travaillons.

Dès lors, face à ce changement de paradigme lié au numérique, l'IFA s'est interrogé sur le rôle du conseil d'administration en la matière, et a mis en en place un groupe de réflexion sur le suivi des risques numériques :

- Comment le conseil doit-il s'organiser pour traiter du numérique ?
- Faut-il mettre en place un comité *ad-hoc* ou faut-il traiter du numérique au sein même du conseil d'administration ?
- Faut-il introduire une compétence numérique au sein du conseil ?

La transformation numérique des entreprises, porteuse d'enjeux tant en termes de performance, d'organisation, d'évolution culturelle et de risques... est un sujet stratégique pour l'entreprise.

Composition du groupe de travail

- Président : Gérard LANCNER, AMRAE, administrateur de sociétés
- Rapporteur : Sophie BOUTEILLER, CIGREF

L'IFA remercie tous les membres du groupe pour leur participation active aux travaux ici présentés.

- Rédouane BELLEFQIH, Deloitte, Associé IT Advisory
- Didier de MENONVILLE, Commissaire aux Comptes, administrateur de sociétés
- Clémence DECORTIAT, IFA
- Laurence DORS, administrateur de sociétés
- Bernard DUFAU, administrateur de sociétés
- Jean-Claude GUEZ, administrateur de sociétés
- Jérôme HUBER, MAZARS, Associé,
- Corinne JACQUIOT, Société Générale, Directeur Juridique Corporate Groupe, administrateur de société certifié ASC France
- Frédéric LAU, CIGREF
- Bruno MENARD, CIGREF, Vice Président et Sanofi, Group CIO
- Guy LE PÉCHON, Gouvernance et Structures, Gérant Associé
- Daniel LEBÈGUE, IFA, Président
- Xavier MAITRIER, PwC, Associé
- Marc MAOUCHE, Orange Participations, administrateur, administrateur de société certifié ASC France.
- Alain MARTEL, IFA, Secrétaire Général
- Eliane ROUYER-CHEVALIER, administrateur de sociétés

L'administrateur, désireux de mieux comprendre ce qui se joue au niveau de son entreprise avec le numérique, en vient à s'interroger :

- Comment le numérique impacte-t-il mon entreprise aujourd'hui ?
- Comment m'assurer que cette transformation en marche est organisée, pilotée et cohérente avec la stratégie de l'entreprise ?
- Qui sont les acteurs de cette transformation ?
- Comment penser différemment et insuffler une nouvelle culture au plus haut niveau dans l'entreprise ?
- Quels sont les nouveaux risques liés à la transformation numérique ? Sont-ils connus, gérés, maîtrisés ?

Le présent guide pratique expose les grands enjeux de la transformation numérique (I), explique en quoi le numérique impose de repenser les rôles et responsabilités des acteurs (II) et fait le point sur les challenges et les risques associés pour l'entreprise (III). Une série de recommandations et points d'attention à destination des administrateurs d'entreprise en matière de suivi des risques liés au numérique conclut ce document.

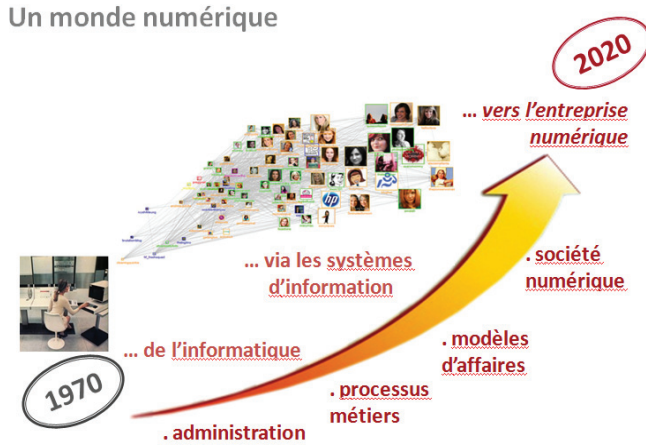
Quelques éléments complémentaires sont destinés à apporter plus de détails sur les tendances qui structurent la transformation des entreprises avec le numérique, le cadre réglementaire actuellement en vigueur (ce cadre étant en évolution, il est impossible de proposer un panorama exhaustif : les technologies évoluent très vite mais le corpus législatif s'adapte lentement).

1. Les enjeux du numérique pour l'entreprise et son environnement

« … Le digital, c'est plus que de l'informatique, c'est une transformation assez profonde. »

Henri de Castries, PDG AXA

(Cercle « Entreprises, stratégies et cultures numériques», 4 octobre 2012)



Source : *De l'informatique à l'entreprise numérique* (CIGREF, 2013)

Depuis plus de 40 ans, l'informatique se développe et révolutionne les processus et les modes d'organisation de l'entreprise, jusqu'à ses produits. De la mécanographie dans les années 70' à l'informatique de production des années 80', jusqu'à outil de management dans les années 90', l'entreprise a vu se développer les systèmes d'information comme outils stratégiques dans les années 2000, avec le développement du pilotage par les processus et l'arrivée d'Internet, qui a ouvert une nouvelle ère de communication et de partage d'information. Aujourd'hui, le système d'information s'est propagé dans toute la chaîne de valeur de l'entreprise : elle devient numérique. Dès 2010, certains acteurs avaient identifié que le mot « numérique » comprenait à la fois « *les systèmes d'information et leur ouverture. L'absence de frontière entre l'informatique professionnelle et l'informatique privée place les systèmes d'information au cœur de l'entreprise et de son écosystème, qui inclut les partenaires, les sous-traitants, les clients…* »[2].

Aujourd'hui, la pensée se précise : les enjeux de la transition numérique des entreprises résident dans leur capacité à « *(…) harmoniser vitesse, innovation et efficacité collective ; mais également [à] pouvoir concilier performance économique et transformation organisationnelle et surtout, [à] vouloir mobiliser les valeurs d'engagement, de coopération et de confiance…* »[3].

2 Ménard, Bruno, (2010), *L'entreprise numérique : quelles stratégies pour 2015 ?*, Nuvis, p. 38.

3 Buffard, Pascal, (2013), *Entreprises & Culture Numérique*, p.2.

Et dans cette transition, l'actif stratégique-clé pour l'entreprise est l'information, tant structurée que non structurée. En effet, l'entreprise qui saura créer de la valeur à partir de l'exploitation de l'information et qui saura lui donner du sens pourra développer (ou renforcer) durablement son avantage compétitif. Ceci, en particulier dans un contexte favorisé par l'Accéluction[4], qui se caractérise par l'extension des espaces de création de valeur et par l'accélération considérable des liens (transactionnels et organiques).

1.1 - Des évolutions majeures

Dans le contexte économique actuel, un grand nombre de transformations dans la sphère sociétale et la multiplication de l'offre technologique modifient le rôle et les attentes des clients/consommateurs, des partenaires et réinterrogent notre rapport au temps. L'entreprise est poussée à se dématérialiser, à repenser sa stratégie, ses formes organisationnelles et ses modes de collaboration tout en prenant en compte l'avènement de nouveaux risques (précarité de l'écosystème, e-réputation, sécurité).

L'entreprise évolue aujourd'hui dans un contexte de globalisation. Dans ce contexte économique, les transformations sociétales, que certains nomment « révolution sociétale » ont un impact sur l'entreprise dans de nombreux domaines. Elles renvoient à :

- Des **cultures différentes** qui coexistent et peuvent entrer en conflit ;
- L'augmentation du **consumérisme**, qui se traduit dans certains pays par des *class-actions* ;
- La montée en puissance du **BYOD (*Bring Your Own Device*)** permettant de satisfaire chaque utilisateur mais déplaçant les contraintes de gestion des outils ;
- Le **télétravail,** considéré comme un nouvel enjeu ;
- L'**intimité clients/consommateurs ;**
- Les **réseaux sociaux** qui participent à ces évolutions et dont le développement dans les entreprises soulève des questions de stratégie.

Par ailleurs, ces transformations sociétales s'accompagnent d'une augmentation de l'offre technologique qui s'incarne par exemple dans l'avènement de l'Internet des Objets, les ''*smart grids*'', le perfectionnement des capteurs numériques, la monétisation des échanges sur mobile…

1.2 - Un rapport au temps marqué par l'accélération et la vitesse

Le rapport au temps change lui aussi, pour accompagner ces évolutions sociétales majeures, et se caractérise notamment par l'accélération et la vitesse :

- Accélération de l'évolution des usages;
- Accélération des flux physiques;
- Accélération de l'évolution des business models.

Cette accélération bouleverse toutes les parties prenantes de l'entreprise, mais aussi les formes organisationnelles de celle-ci : entreprise étendue, organisation matricielle, segmentation, mentorat inversé[5]...

1.3 - De nouveaux modes de collaboration orientés vers le partage et l'ouverture

Les modes de collaboration et de travail entre toutes les parties intéressées sont questionnés. Certains constatent l'augmentation de la collaboration, d'autres insistent sur la multiplicité des outils collaboratifs. Le partage des données et le ''*crowd-sourcing*'' sont deux représentations incarnant ces nouvelles formes de collaboration.

Le numérique impacte également la relation avec le client, pour les entreprises B to C, en créant de nouveaux challenges et en transformant le rôle de celui-ci :

- Le consommateur pénètre l'entreprise ;
- La volatilité des clients est plus forte, la relation avec eux a de plus en plus d'importance ;
- Il existe un enjeu de personnalisation de la relation avec le client ;
- Les clients sont de plus en plus sensibles aux données ;
- Les produits « numériques » vont de pair avec des services « numériques » comme la traçabilité, la télésurveillance, la maintenance préventive, …

Sous l'influence du numérique, la relation B to B évolue également : la co-conception de produits est possible, de nouveaux modèles de support apparaissent, la traçabilité des produits et des projets s'améliore, des relations plus ou moins informelles se développent entre tous les acteurs (à la fois en internes, et avec l'extérieur) grâce notamment aux messageries et réseaux sociaux.

4 L'Accéluction est un concept développé par le Pr Ahmed Bounfour, Rapporteur du programme international de recherche ISD de la Fondation CIGREF, qui caractérise l'émergence d'un « nouveau système de production accélérée de liens », marquée à la fois par « l'extension des espaces de création de valeur et par l'accélération considérable des liens (transactionnels ou organiques) comme source de création de valeur ». In « L'Accéluction en action, programme international de recherche ISD : premier rapport d'étape, une mise en perspective des projets Vague A », Fondation CIGREF – Octobre 2011, p. 8

5 Extrait du discours de Henri de Castries, Cercle « Entreprises et Cultures numériques » (2012) : « (…) les jeunes générations ne sont pas câblées comme les vieilles ! (…) à l'intérieur des réseaux, les gens qui sont un peu plus récents ont déjà intégré une partie de cette nécessité [de la transformation numérique] et poussent plutôt à l'accélération. Il faut s'appuyer sur eux pour convaincre les autres qu'il faut changer. », p. 14.

Et la dématérialisation (factures, commandes, flux physiques, …) va de pair avec l'évolution du numérique. Cependant, celui-ci ne doit pas être simplement réduit à sa dimension de dématérialisation : l'émergence de nouveaux risques, tels que la fragilité de l'écosystème, l'e-réputation, les enjeux de sécurité, sont des sujets clés de l'entreprise numérique.

1.4 - Des modèles d'affaires à revisiter

Dix tendances semblent structurer la transition numérique des entreprises, que l'on peut regrouper en trois grands axes caractéristiques de l'entreprise : l'expérience client, l'organisation et le management, les ressources et les flux, et qui impactent directement les modèles d'affaires. C'est l'ensemble de ces 10 tendances[6] qu'il convient de considérer de manière interdépendante pour comprendre le phénomène de la transition numérique et son impact sur la stratégie de l'entreprise. Il s'agit in fine d'identifier en quoi la transition numérique transforme la vision stratégique actuelle de l'entreprise.

Primauté de l'expérience client

L'émergence du numérique au sein de notre société modifie le comportement des consommateurs, intensifie la concurrence entre les entreprises, et ouvre de nouveaux marchés. Pour répondre à ces défis, l'entreprise doit repenser dans son ensemble ses relations avec le client. En premier lieu, elle doit saisir l'opportunité offerte par Internet d'impliquer le client dans sa chaîne de valeur, en ouvrant son espace de co-création de valeur, afin de coller au plus près à ses attentes et lui apporter les produits et les services associés dont il a besoin. La création d'un écosystème de marque vient compléter cette démarche. Il permet à l'entreprise, grâce à une approche cross-canal, de fidéliser le client et de s'ouvrir à de nouveaux marchés émergents. Enfin, l'entreprise est face à un défi majeur : celui d'animer sa communauté de ''fans'', fidèles et potentiels prescripteurs, dans son écosystème et sur les réseaux sociaux, afin d'en faire un relais de communication efficace et de croissance durable.

Ainsi, sur l'axe de l'expérience client, les tendances structurantes sont :

1. **Les services associés aux produits : mettre en valeur l'expérience client**
2. **La plate-forme clients : un espace central de promotion de l'expérience client**
3. **L'importance d'une communication interactive avec les communautés de ''fans'' pour tirer partie de leur influence**

Organisation et management liés à la co-création de valeur

L'ensemble des transformations numériques montrent qu'il est primordial d'accepter que la création de valeur soit entrée dans une dynamique collective. Aussi, les exigences managériales et structurelles deviennent claires : rendre les communications organisationnelles plus transparentes pour partager une vision stratégique commune, adopter une architecture agile et ouverte vers tout l'écosystème de l'entreprise, mettre en place un mode de gouvernance fondé sur la concertation et l'implication de tous les acteurs de la chaîne de valeur.

Sur l'axe organisation et management, les tendances structurantes sont :

4. **L'adoption d'une démarche d'incitation explicite à l'innovation pour engendrer de nouveaux avantages compétitifs (''open innovation'')**
5. **La promotion d'un management par les résultats**
6. **Le bénéfice des dynamiques collaboratives**

La gestion des ressources et flux accélérés

Dans un contexte d'accélération numérique, à la croisée des transformations sociétales et de la standardisation des gouvernances SI, l'entreprise doit être en mesure de capter et analyser une grande quantité d'informations provenant de sources multiples, afin de mettre en place de nouvelles propositions de valeur co-créée avec ses clients, ses fournisseurs, voire même avec ses concurrents.

Les tendances structurantes en matière de gestion des ressources et des flux sont :

7. **Le SI comme future plate forme de services pour l'entreprise**
8. **Le Big Data décuple les sources et natures d'information pertinentes pour l'entreprise**
9. **Le Cloud comme agent transformateur de la fonction SI**
10. **Gestion de la mobilité : un défi pour assurer la permanence du service**

1.5 - Un actif stratégique-clé à protéger : l'information

S'il semble clair aujourd'hui que l'information est l'élément clé du business des entreprises, celles qui gagneront en performance demain sont celles qui sauront intégrer les informations non structurées dans leurs systèmes décisionnels, les croiser avec les données externes de leurs partenaires, et adapter l'architecture de leur système d'information pour optimiser le traitement des informations, tant d'un point de vue quantitatif que

6 Ces 10 tendances identifiées par le CIGREF sont détaillées pages 22 et 23

qualitatif. Les dirigeants d'entreprise sont convaincus que la culture numérique et le développement des usages numériques sont des sources d'innovation et de création de valeur pour les organisations qu'ils dirigent, et l'avènement des médias sociaux laisse émerger des nouveaux espaces d'échanges et de création de valeur, dans lesquels vivent ensemble vie privée et vie professionnelle.

Ces nouveaux espaces émergent du fait d'une profonde évolution des usages, en particulier avec les nouvelles générations, et favorisent l'explosion des volumes d'informations, structurées et non structurées (Big Data) pouvant renfermer une forte valeur ajoutée. Que faire de ces données ? Comment les gérer ? Les stocker ? Les utiliser ? Les traiter ? Quelle valeur ont-elles pour l'entreprise ?

La valeur des contenus numériques pour l'entreprise

Les enjeux du numérique en matière d'information et de données posent les questions du droit à l'oubli d'une part, et de l'exploitation des données à des fins de publicité comportementale servant les stratégies marketing des entreprises d'autre part.

Deux questions se posent alors :

- Comment le numérique peut-il permettre « d'humaniser » la relation client ?
- Quels sont les nouveaux modèles d'avenir ?

Les nouveaux enjeux de la protection des données

Comme évoqué précédemment, le BYOD marque une forte évolution des modes d'organisation et des pratiques dans les entreprises. Il répond à des usages hétérogènes, marqués par une aisance technique des utilisateurs avec les appareils. Ainsi, le BYOD est une tendance de fond contre laquelle l'entreprise ne peut pas aller.

Cependant, selon le CLUSIF[7], les nouveaux risques liés au numérique portent essentiellement sur l'utilisation de matériel personnel à usage professionnel (BYOD, réseaux sociaux, …), qui accroissent de manière importante les vulnérabilités :

- Fuite d'informations ;
- Destruction de données ;
- Pénétration dans le SI ;
- Banalisation de l'accès à l'information.

Tirer parti de l'échange de données numériques dans la relation client-fournisseurs

L'accélération de la circulation des informations et des échanges, les besoins de traçabilité mais aussi d'instantanéité sont des réalités désormais indiscutables. Tout l'enjeu pour l'entreprise est d'arriver à protéger et développer ce qui fait de la valeur (valeur d'échange). La protection des données est devenue aujourd'hui plus critique que la protection des produits, il est donc nécessaire de se protéger, sans paranoïa, mais de manière appropriée.

Les données sont à la fois structurantes et complexes, elles fondent les processus de captation et de fidélisation des clients. L'entreprise tire de la valeur des données relatives à ses clients, ces données recouvrent donc des enjeux commerciaux et financiers. Leurs protection et sécurisation recouvrent quant à elles des enjeux stratégiques et politiques pour l'entreprise.

Gouvernance de l'information

Certaines entreprises ont d'ores et déjà bien compris les enjeux de compétitivité, mais aussi juridiques, autour de l'information et de sa gestion. Devenue un actif stratégique clé, les entreprises placent de plus en plus souvent la gouvernance de l'information au cœur de leur stratégie numérique, marquée par une préoccupation majeure sur la sécurité : protéger les données gérées par l'entreprise, par des tiers et vice-versa, protéger le capital informationnel. Et partant du constat que la protection des données est critique, certaines entreprises ont repensé la protection de l'information à partir d'un modèle d'organisation spécifique, qui associe les systèmes d'information, le juridique, le risk management et les ressources humaines.

7 Une enquête CLUSIF, menée début 2012, met en évidence que 45% des utilisateurs utilisent leur matériel professionnel pour un usage personnel (usage mixte), contre 35% qui en font un usage professionnel uniquement et 20% qui en font un usage personnel uniquement (ce qui peut sembler surprenant). Par ailleurs, cette même enquête révèle que 40% des salariés français ont demandé à la DSI d'ouvrir le SI à leur matériel personnel (refus fréquent des DSI qui freinent l'utilisation des matériels personnels au travail, et quand le SI est ouvert, près des trois quart des utilisateurs utilisent leur matériel en dehors du temps de travail).

En résumé

La transformation de l'entreprise dans le monde numérique implique de gérer les ruptures, grâce notamment à l'innovation et au développement de nouveaux produits et services. Les objectifs sont d'utiliser le numérique pour conquérir de nouveaux marchés et réduire le time to market. Les enjeux pour les entreprises sont contextuels et liés à leur cœur de métier. Ainsi, le numérique est une composante essentielle de la réflexion stratégique : la rapidité d'évolution des marchés, des besoins et des attentes des clients exigent des entreprises une très forte capacité à déployer ou à redéployer rapidement leurs activités.

- *Le numérique est un vecteur d'innovation des produits et des services de l'entreprise ; il permet de mieux analyser les marchés et les attentes des clients et de concevoir des offres plus ciblées.*
- *Le numérique constitue aussi un canal complémentaire, voire parfois principal, de distribution des produits et des services de l'entreprise et rend accessibles de nouveaux marchés.*
- *Le numérique est un levier d'amélioration de l'efficacité opérationnelle ; à titre d'exemple, il peut offrir pour la gestion des processus de l'entreprise une alternative à certaines solutions informatiques, en permettant d'adopter des solutions souples, accessibles en mode web, raccourcissant les délais de mise en œuvre.*
- *Le numérique peut constituer un véritable relais de croissance pour l'entreprise autant qu'une menace importante vis-à-vis de positions réputées établies, par la puissance et la rapidité avec laquelle des activités concurrentes peuvent se développer.*

Mais au-delà des opportunités qu'il crée, le numérique est aussi porteur de nouveaux risques. Les Métiers, à la recherche de plus de flexibilité et d'agilité, vont chercher à l'extérieur de leur entreprise – c'est-à-dire sans passer par leur DSI – des solutions de gestion répondant à ces exigences. Deux raisons principales peuvent expliquer cette tendance : une plus grande facilité de déploiement et d'utilisation de ces solutions de gestion portées par les nouvelles technologies et l'encombrement fréquent des portefeuilles de projets des DSI. Le numérique interpénètre les métiers de l'entreprise et crée de nouveaux risques, liés à la protection des données. Nous sommes dans un système complexe, qui rassemble des éléments de nature et de matières différentes : dimensions juridiques, humaines, organisationnelles, techniques, relationnelles, …

2. Les interlocuteurs du conseil sur le numérique

Le développement d'une vision stratégique commune et partagée sur le numérique passe par la diffusion d'une culture numérique, au-delà de la seule optimisation des systèmes. La pédagogie est clé pour faire comprendre les bénéfices du numérique et susciter l'intérêt du business.

Dans ce cadre :

- Les dirigeants de l'entreprise ont besoin d'être éclairés sur le « virage » numérique ;
- Les Métiers doivent imaginer de nouveaux services, supportés par les nouvelles technologies.

Pour cela, la perception du SI qu'ont les Métiers et la DG doit évoluer d'une vision « SI = centre de coûts » à une vision « SI = source de valeur et d'économies ». Les interactions DG-Métiers-DSI deviennent plus que jamais nécessaires dans ce contexte :

- Les dirigeants doivent avoir une ''vision numérique'' ;
- Les Métiers et la DSI doivent développer des synergies porteuses de valeur, en cohérence et dans le cadre de la stratégie de l'entreprise ;
- La DSI est garante du maintien de la cohérence globale du SI dans ce contexte d'ouverture.

Il appartient donc au conseil de s'assurer que ce triptyque DG / DSI / Métiers fonctionne effectivement dans l'entreprise et que les rôles et contributions attendus de chacun sont clairement identifiés et appropriés par les différents acteurs.

2.1 - Les interactions du conseil avec la direction générale

La direction générale est bien évidemment l'interlocuteur naturel du conseil sur le sujet du numérique. Le conseil peut entendre chaque année la direction générale sur sa vision du numérique, d'un point de vue général, sur son marché puis dans l'entreprise.

Il s'agit pour le conseil d'apprécier l'usage qui est fait dans l'entreprise, des nouvelles technologies. Le numérique est-il vu :

- **Comme un levier d'amélioration de l'efficacité opérationnelle ?**

La dématérialisation, le *Cloud Computing*, les outils de mobilité constituent autant d'opportunités d'améliorer l'efficacité des processus internes de l'entreprise et d'en réduire les coûts de fonctionnement. Comment l'entreprise intègre-t-elle le numérique dans ses modes

de fonctionnement opérationnel ?

- **Comme un moyen de communiquer de l'information en interne comme en externe** ?

Le web 2.0, les outils de mobilité permettent un nouveau mode d'échange plus immédiat, plus interactif, avec les clients, les fournisseurs et les collaborateurs. Comment l'entreprise intègre-t-elle ces nouveaux modes de fonctionnement et leurs impacts sur les relations, le style de management et la culture ?

- **Comme un outil pour le marketing ?**

Les nouvelles technologies permettent de mieux analyser la qualité de service perçue par le client, elles offrent aussi de nouveaux canaux de communication des offres et des produits, voire permettent de constituer un canal de distribution à part entière. Comment l'entreprise a-t-elle intégré le numérique dans le marketing de ses offres ?

- **Comme un vecteur d'innovation ?**

Le numérique contribue aussi à enrichir les produits et services de l'entreprise. Comment l'entreprise aborde-t-elle la conception de ses offres à l'heure du numérique ?

- **Comme un axe de développement de nouvelles activités pour l'entreprise ?**

Les savoir-faire de l'entreprise et sa position sur les marchés, conjugués avec les potentialités des nouvelles technologies peuvent générer de nouvelles lignes d'activité. Comment l'entreprise réfléchit-elle à valoriser ses actifs à l'aide du numérique pour enrichir ses métiers ?

La vision du dirigeant permet au conseil de se forger une opinion sur l'impulsion donnée au numérique dans l'entreprise et d'en confronter la pertinence via des benchmarks sectoriels ou par analogie avec des initiatives lancées dans d'autres secteurs d'activité.

Il s'agit ensuite pour le conseil d'apprécier la façon dont la direction générale décline cette vision dans l'entreprise, en termes stratégiques et opérationnels, par une approche des opportunités et des risques. Cette déclinaison peut prendre différentes formes :

- Un document de stratégie
- Un plan à moyen terme
- Un schéma directeur des systèmes d'information
- Un plan numérique, accompagné d'une cartographie claire pour les non informaticiens

Ce document, quel qu'il soit, doit intégrer l'analyse des risques, et être accompagné d'un volet management visant à impliquer les directions fonctionnelles et opérationnelles de l'entreprise, et à sensibiliser le personnel, …

Le conseil suit la mise en œuvre des initiatives numériques en s'informant des grands investissements informatiques, et en revoyant chaque année le portefeuille des grands projets de transformation : justifications, apports, retours sur investissement, risques…

Le conseil s'assure que la direction générale a pris la mesure des enjeux liés à l'utilisation du numérique dans le fonctionnent courant de l'entreprise :

- Il questionne la direction générale sur le niveau de dépendance de l'entreprise à ses fournisseurs stratégiques ;
- Il apprécie la pertinence des dispositifs mis en place pour assurer la continuité de service et garantir la sécurité de l'information de l'entreprise ;
- Il s'informe des indicateurs dont dispose la direction générale pour suivre l'exécution du plan informatique, des grands projets et des principaux risques informatiques.

Enfin, en cas de crise majeure liée au numérique ou à son usage, susceptible de mettre en cause significativement l'atteinte des objectifs de l'entreprise, son image ou sa réputation, le conseil peut être amené à questionner la direction générale, à apprécier son niveau de maîtrise de la situation et le cas échéant à s'impliquer plus fortement dans la résolution de la crise.

2.2 - Le directeur des Systèmes d'Information, un interlocuteur privilégié du conseil

A des fins d'approfondissement ou pour étendre son champ d'appréciation, le conseil peut demander à entendre le Directeur des Systèmes d'Information de l'entreprise. Cet échange qui pourrait être annuel vise à compléter la compréhension du conseil sur des enjeux importants associés aux évolutions du numérique et à apprécier le positionnement de la DSI dans l'entreprise, ses interactions avec les métiers et la direction générale, ainsi que la contribution du système d'information à la réalisation des objectifs de l'entreprise.

Concrètement, le conseil peut entendre le Directeur des Systèmes d'Information sur la gestion d'ensemble du système d'information, l'impact des arbitrages budgétaires sur les opportunités et les risques, l'évolution des menaces liées aux nouvelles technologies et à leurs usages, …

En préliminaire à cet échange, il serait utile que les membres du Conseil disposent d'une vue d'ensemble des missions, des principes d'organisation et des rôles et responsabilités des principaux acteurs d'une DSI[8].

Plus spécifiquement, le conseil pourrait questionner le DSI sur les thèmes suivants :

- L'existence, l'actualisation et le niveau d'application de la politique de sécurité de l'information, ainsi que les principaux incidents survenus ou failles constatées en matière de sécurité informatique ;
- La cartographie explicite des applicatifs et de leurs inter relations

8 CIGREF, (2011), *Les métiers des systèmes d'information dans les grandes entreprises*

- Les grands contrats de sous-traitance informatique et le niveau de maîtrise en interne des prestations externalisées du point de vue de la qualité et du contrôle interne ;
- L'avancement des grands projets SI de l'entreprise, ainsi que le suivi des retours sur investissement …

2.3 - Le conseil et les autres parties prenantes

Compte tenu des enjeux, il peut être utile pour le conseil d'entendre ponctuellement d'autres acteurs de l'entreprise impliqués dans le numérique.

Ainsi le conseil peut solliciter les responsables des grandes directions fonctionnelles ou opérationnelles de l'entreprise, sponsors de grands projets de transformation à forte connotation informatique / numérique. Ces projets représentent des investissements majeurs. Leur maîtrise et leur bonne fin sont critiques pour l'entreprise. Il convient alors pour le conseil de questionner le sponsor sur un certain nombre de points de vigilance de ces grands projets, tels que :

- Son implication en tant que sponsor du projet, la justification Métiers de l'investissement et la confiance dans la capacité à livrer ce qui est attendu dans le respect des délais et des budgets annoncés ;
- La robustesse du business case et du retour sur investissement, qu'il soit financier ou qualitatif ;
- L'ampleur du changement apporté par le projet et le niveau de préparation de l'organisation et des collaborateurs ;
- Sa vision des principaux risques, y compris technologiques …

Selon les enjeux, le conseil peut recommander un audit du projet à l'occasion du passage des grands jalons ou s'il identifie une dérive significative d'un des paramètres du projet.

Selon les organisations, des fonctions spécifiques peuvent avoir été créées autour du numérique et de la gestion de l'information de l'entreprise. Les responsables de ces fonctions peuvent aussi éclairer le conseil dans son rôle de surveillance des risques numériques de l'entreprise.

A titre d'exemple :

- Le *Chief Digital Officer*, en charge de la transformation numérique de l'entreprise a pour mission d'animer en transversal, la réflexion et les démarches sur le numérique dans l'entreprise, de coordonner les initiatives dans ce domaine et d'en assurer la cohérence d'ensemble ;
- Le *Chief Security Officer*, ou le Responsable de la sécurité des systèmes d'information, la définition des missions, du périmètre d'intervention et du positionnement dans l'entreprise peut être variable et mérite donc d'être préalablement précisé ;
- Le *Risk Manager* et l'Auditeur interne, sur leurs travaux relatifs à l'informatique …

2.4 - Dans quelle instance du conseil le sujet du numérique peut-il être abordé ?

La question mérite effectivement d'être posée. En effet, le numérique, qui en première approche peut être perçu comme un sujet très technique, affaire de spécialistes, est en fait un sujet transverse à l'entreprise, intimement lié à sa stratégie, pouvant nécessiter des investissements significatifs, et porteur de risques spécifiques.

Quelle est donc l'instance du conseil la plus appropriée pour traiter le sujet :

- Le conseil en formation plénière ?
- Le comité d'audit ?
- Le comité des risques ?
- Le comité stratégique ?
- Un comité spécialisé du conseil sur le numérique ?

La réponse à cette question n'est pas universelle et dépend du contexte spécifique de chaque entreprise. Elle peut être abordée sous deux angles :

- La place et les enjeux du numérique dans l'entreprise appréciés relativement au regard des autres sujets centraux liés à l'activité et au développement de l'entreprise, compte tenu notamment de son secteur d'activité et de sa maturité sur le sujet ; avec comme corollaire le niveau de rattachement hiérarchique du responsable du sujet dans l'entreprise (DSI, Chief *Digital Officer* …) qui en découle : direction générale, direction financière, autres directions ;
- L'organisation des travaux du conseil, et notamment :
  - L'existence de comités spécialisés et leurs missions,
  - L'actualité de l'entreprise, les priorités du conseil et le planning des réunions.

Intrinsèquement, chaque solution possède des avantages et des inconvénients, que l'on peut résumer comme suit :

Instance en charge	Intérêt	Points de vigilance
Conseil en réunion plénière	Appropriation homogène par tous les membres du conseil Approche globale du numérique dans l'entreprise	Disponibilité suffisante pour traiter le sujet avec la profondeur nécessaire et assurer la surveillance des investissements
Comité d'audit	Suivi des investissements Possibilité d'un suivi plus régulier des grands projets	Prise en compte des enjeux stratégiques et opérationnels, et des risques Appropriation par l'ensemble du conseil
Comité des risques	Approche transversale Enjeux / Risques Adaptation des dispositifs de maîtrise des risques aux nouvelles menaces engendrées par le numérique	Prise en compte dans la réflexion stratégique Appropriation par l'ensemble du conseil
Comité stratégique	Intégration du numérique dans la stratégie Possibilité d'un suivi Métiers des grands projets et de leur contribution aux objectifs de l'entreprise	Prise en compte des risques Appropriation par l'ensemble du conseil
Comité spécialisé	Profondeur des réflexions Capacité à suivre les réalisations	Synergie et interaction avec les travaux des autres comités Appropriation par l'ensemble du conseil Risque d'une évolution vers une posture d'expert

Quelle que soit la solution retenue, comme pour tous les travaux d'un comité spécialisé, il appartient au conseil, in fine, en session plénière, de s'approprier le sujet du numérique dans son ensemble. Ce point mérite une attention car certains administrateurs peuvent être encore peu familiers avec le numérique, ce qui pourrait nécessiter un temps d'appropriation plus important que pour les autres travaux habituellement préparés par les comités spécialisés.

Notre recommandation à ce jour serait de conserver le sujet numérique au niveau du conseil afin de permettre à chaque administrateur de s'approprier le sujet et d'éviter sa « ghettoïsation » débattu entre experts.

En résumé

Aux côtés des projets informatiques classiques se placent désormais les grands projets de transformation, qui embarquent du numérique. Ces projets nécessitent d'être mis en œuvre de manière plus rapide, plus souple, plus agile, et en collaboration permanente avec les Métiers. Ainsi, les interactions permanentes entre DSI – DG – Métiers sont incontournables pour mener à bien ces grands projets de transformation.

3. Les nouveaux risques liés au numérique

L'un des rôles du conseil d'administration est d'assurer le suivi de l'efficacité des systèmes de contrôle interne et de gestion des risques. Or, les nouveaux enjeux numériques redessinent les frontières de l'entreprise, dans un contexte de compétitivité accrue, de mondialisation et d'ouverture. L'entreprise doit en appréhender les nouveaux risques encourus en particulier en matière de systèmes d'information.

Le conseil d'administration doit donc s'assurer qu'au regard de cet environnement mouvant, l'entreprise adapte ses dispositifs internes pour :

1. Favoriser la prise de conscience des nouveaux risques numériques afin d'adapter son dispositif de maitrise des risques en conséquence ;

2. S'approprier le cadre règlementaire évolutif ;

3. Intégrer les nouveaux risques.

3.1 - Favoriser la prise de conscience des nouveaux risques pour adapter le dispositif de maîtrise en conséquence

Dix tendances majeures sont observées, qui influencent la prise de conscience des nouveaux risques numériques :

1. Une sensibilisation accrue des directions générales, directions Métiers et Fonctions Supports aux problématiques de contrôle et de gestion des risques numériques, du fait de la complexification croissante des organisations et des SI, ainsi que de l'extension des périmètres géographiques.

2. Le développement de projets de transformation de grande ampleur, transverses à l'entreprise.

3. Le développement des référentiels de bonnes pratiques en matière de contrôle interne et de gestion des risques numériques (COSO, COBIT, ITIL, …) et de normes internationales qualitatives (ISO/BSS, ...).

4. La recherche de synergies et de complémentarités entre les différents acteurs de la filière Risques dans son ensemble (Inspection générale, contrôle permanent, direction des Risques, direction de la conformité, direction de la qualité, direction de l'audit, ...).

5. Une forte internationalisation des activités des entreprises qui complexifie la maîtrise du portefeuille de projets dans toutes ses dimensions.

6. Le recours accru à l'externalisation de processus clés comme accélérateur du déploiement des activités des entreprises et/ou comme levier d'optimisation des coûts.

7. L'intensification et la diversification des menaces qui pèsent sur la sécurité du système d'information (cybercriminalité, fraudes, perte et fuite de données sensibles, …).

8. Le développement du Big Data, marqué par l'explosion du volume de données externes disponibles (structurées et non structurées).

9. Les outils collaboratifs et les réseaux sociaux utilisés par les entreprises comme canal de fourniture de service, de diffusion de leur offre, et comme moyen de valorisation de leur image (e-réputation).

10. Le développement des outils de mobilité (smartphones, tablettes, réseaux de données sans fil, …) dans les entreprises, rendant le SI accessible depuis l'extérieur, et accroissant sa vulnérabilité.

3.2 - S'approprier un cadre réglementaire évolutif

Le développement du numérique et la nécessité de protéger et réguler ses usages conduisent à une évolution importante du cadre réglementaire et des pratiques contractuelles.

Il importe au conseil de s'assurer que l'entreprise a bien intégré ce nouvel environnement dans son fonctionnement au quotidien et dans ses dispositifs de contrôle.

Le cadre réglementaire présenté en annexe répertorie - à date et de manière synthétique - les principaux textes législatifs relatifs à la sécurité des systèmes d'information, les normes, standards et référentiels de bonnes pratiques, qu'il s'agisse de dispositions générales applicables ou de textes spécifiques propres à certaines pratiques ou à certains secteurs d'activité.

3.3 - Intégrer les nouveaux risques

Les SI sont, en soi, porteurs de risques « classiques » inhérents à leur fonctionnement, leur disponibilité, leur contrôle et leur maitrise[9] (vol, altération des données par les employés, par des pirates, par des programmes malveillants, négligence des salariés, déni de services dû à la saturation des réseaux ou des processus, interruptions des activités, ...).

Le développement du numérique fait apparaître de nouveaux risques[10], qu'il importe désormais de savoir identifier et maîtriser :

- Stratégiques : absence ou défaillance de stratégie numérique, *lock in* , concurrence entre deux canaux de vente ou familles de produits ;
- Liés aux ressources humaines : manque d'adhésion à la stratégie numérique (niveau d'acceptabilité du numérique dans l'entreprise), risques sociaux et psychosociaux, sclérose des compétences ;
- Liés à la dématérialisation des rapports humains : « infobésité », interpénétration des sphères privées et professionnelles, affaiblissement de la communication interpersonnelle, perte de souplesse liée à la numérisation des processus clients, perte de réflexion liée à l'accélération des échanges, droit à la déconnexion ;
- Marketing : e-réputation, mondialisation de la concurrence ;
- Éthiques et juridiques : évolution du droit et de la jurisprudence, authenticité des documents, hétérogénéité des lois nationales, respect de la vie privée, confidentialité des données ;
- Liés au patrimoine : mauvaise protection ou conservation des données numériques.

En résumé...

Les évolutions technologiques et les nouveaux enjeux numériques redessinent les frontières de l'entreprise.

Le conseil d'administration doit donc s'assurer qu'au regard de cet environnement mouvant, l'entreprise adapte ses dispositifs internes pour :

1. Favoriser la prise de conscience des nouveaux risques numériques afin d'adapter son dispositif de maîtrise des risques en conséquence ;

2. S'approprier le cadre réglementaire évolutif ;

3. Au-delà de la maîtrise des risques « classiques » inhérents aux systèmes d'information, intégrer les nouveaux risques propres au développement du numérique et à ses usages.

9 CIGREF, (2002), Sécurité des systèmes d'information : quelle politique globale de gestion des risques ?

10 CIGREF, (2011), Les risques numériques pour l'entreprise

SUR LES ENJEUX DU NUMÉRIQUE POUR L'ENTREPRISE ET SON ENVIRONNEMENT (partie 1)

1 S'assurer que l'entreprise dispose d'une « vision numérique » partagée (stratégie et politique d'adaptation à l'ère numérique), en lien avec sa stratégie globale et dotée de moyens financiers et organisationnels adaptés : se faire présenter cette vision et son déploiement (dont une cartographie de synthèse) une fois par an en conseil d'administration, par le directeur général, le DSI ou le *Chief Digital Officer* (ou équivalent, s'il existe dans l'entreprise). Cette vision doit contenir une analyse de l'environnement, avec une projection des tendances d'évolution de la concurrence et l'identification des nouveaux entrants.

2 S'informer sur l'organisation des systèmes d'information (internes et externes) utilisés par l'entreprise et identifier les systèmes clés indispensables au bon déroulement de son activité.

3 S'assurer que l'entreprise dispose d'un schéma directeur (vision stratégique évolutive) des systèmes d'information et de gestion de l'information, en phase avec la stratégie globale, ayant pris en compte les besoins des utilisateurs, doté de moyens financiers, humains et d'une organisation adaptée : se faire présenter et discuter ce schéma une fois par an avec le DSI.

4 S'interroger sur la pertinence et l'utilité de mettre en place un comité spécialisé en charge du suivi des sujets liés au numérique : Comité Numérique (ou *Digital Agency*).

5 S'assurer que le patrimoine informationnel de l'entreprise est protégé et que la gouvernance de l'information est prévue, pensée et organisée :

a. Dans le respect des réglementations existantes et du droit des tiers ;
b. Avec une identification et un traitement appropriés des informations sensibles ;
c. Avec une classification et une gestion adaptées des droits d'accès.

SUR LES INTERLOCUTEURS DU CONSEIL SUR LE NUMÉRIQUE (partie 2)

6 S'assurer que le conseil dispose d'administrateur(s) ayant des compétences ou expérience(s) sur le numérique ; et à défaut, organiser des formations.

7 S'assurer que le numérique est à l'ordre du jour des travaux annuels du conseil d'administration (ou d'un comité spécialisé le cas échéant) : sujet traité au moins une fois par an en conseil.

8 S'assurer que, quelles que soient la taille et l'activité de l'entreprise, les rôles et responsabilités en matière de gestion des SI sont clairement répartis entre des acteurs (internes et / ou externes), et que ceux-ci sont conscients de leur mission :

a. Se faire présenter cette organisation, et en particulier les interactions avec les Métiers et le reporting avec la DG ;
b. S'assurer qu'elle est dotée de moyens humains et financiers suffisants ;
c. S'assurer régulièrement de l'efficience de la gestion des SI (via un audit par exemple).

9 S'assurer que les compétences clés liées aux systèmes d'information font l'objet d'une gestion prévisionnelle des besoins et d'une adaptation régulière.

10 S'assurer que les grands projets de transformation (projets informatiques majeurs) ont un « propriétaire métier » (utilisateur responsable), que le contrat (rôles et responsabilités) entre les directions Métiers (utilisateurs) et la DSI (développements, exploitation, sécurité, coordination,...) est clairement défini et déployé ; questionner le ROI (financier ou non) attendu de ces projets et le suivi qui en est fait.

11 S'assurer que les partenaires stratégiques qui affectent l'entreprise de manière structurelle sont encadrés par un processus clair et mis en oeuvre, que les responsabilités de chacun sont bien définies et que les risques associés sont bien connus et traités.

12 S'assurer que les couvertures d'assurances de l'entreprise sont adéquates et suffisantes au regard des risques (impact + probabilité) encourus.

SUR LES NOUVEAUX RISQUES LIÉS AU NUMÉRIQUE (partie 3)

13 S'assurer de l'efficacité des systèmes de Sécurité / Continuité, de Contrôle Interne et de Gestion des Risques spécifiques aux systèmes d'information : entendre annuellement les acteurs internes (DSI, RSSI, Risk Manager, Audit Interne ou équivalent) et externes (Commissaires aux comptes, experts ad hoc, ...) sur un retour d'expérience interne et une revue des incidents, et faire des benchmarks avec l'extérieur ; en cas de doute, demander un audit spécifique par des experts extérieurs spécialisés.

14 S'assurer que les systèmes de Contrôle Interne et de Gestion des Risques intègrent bien le respect des réglementations et les risques spécifiques aux systèmes d'information.

15 S'assurer que l'entreprise dispose et a déployé une politique, des moyens et une organisation pour garantir la sécurité et la continuité des systèmes d'information.

16 S'assurer que l'entreprise encadre les usages du numérique à travers des chartes, voire les adosse au règlement intérieur en y intégrant un chapitre sur le numérique : la charte permet d'harmoniser les pratiques de manière globale, mais elle n'a aucune valeur juridique (contrairement au règlement intérieur) ; cependant, elle permet de définir – a minima – clairement les droits et devoirs des collaborateurs dans l'entreprise.

17 Si l'entreprise est certifiée, vérifier le niveau, le périmètre et la date de délivrance de la certification : demander à connaître la portée des conclusions de l'audit de certification et s'assurer que celle-ci est bien effective.

Remarque : La certification ne se suffit pas à elle-même pour prévenir le risque. Sur le périmètre des normes, la portée des travaux est différente : la certification ISO est orientée Qualité, alors que d'autres types de certification vont plus loin, le périmètre de la certification dépendant de la norme appliquée. Ainsi, l'application de certaines normes inclut des tests d'efficacité pas toujours prévus dans ISO (exemple avec ISO et SSAE16 ISAE3402).

Pour aller plus loin…

IFA : www.ifa-asso.com

- La Vade-mecum de l'administrateur, 2008
- IFA IFACI - Le rôle de l'audit interne dans le gouvernement d'entreprise, 2009
- Rapport IFA-AMRAE : Rôle de l'administrateur dans la maîtrise des risques, 2009
- De quelle information l'administrateur a-t-il besoin ? 2011

CIGREF : www.cigref.fr

- L'entreprise numérique : quelles stratégies pour 2015 ?
- 10 tendances structurantes de l'entreprise numérique
- La gouvernance juridique de l'entreprise numérique
- E-réputation, étude sur les risques et opportunités liés à l'e-réputation
- Les risques numériques pour l'entreprise
- Eduquer les acteurs de l'entreprise aux risques numériques
- Protection de l'information et Cloud Computing
- Sécurité des SI, rôle et responsabilités de l'État
- Entreprises et culture numérique

Glossaire

Big Data : littéralement « grosses données », Big Data est une expression anglophone qui désigne des ensembles de données devenant tellement volumineux qu'ils en deviennent difficiles à exploiter avec des outils classiques de gestion de base de données ou de gestion de l'information. Les perspectives du traitement des Big Data sont très importantes pour les entreprises. Le phénomène Big Data est considéré comme l'un des grands défis informatiques de la décennie 2010-2020.

Source : http://fr.wikipedia.org/wiki/Big_data

BYOD (Bring Your Own Device) : pratique qui consiste à « utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel. Cette tendance pose des questions sociales, juridiques et sur la sécurité de l'information. En 2013, ce phénomène se répand au sein des entreprises. Selon une étude menée par un cabinet d'étude indépendant, 71 % des collaborateurs interrogés utiliseraient à titre professionnel des solutions non mises à disposition par leur entreprise. »

Source : http://fr.wikipedia.org/wiki/BYOD

Comité numérique (ou *Digital Agency*) : il s'agit de mettre en place « une équipe centrale, avec une architecture légère » et qui « intègre des collaborateurs issus des métiers et de l'IT. De très bon niveau de formation et polyvalents, ils connaissent à la fois les technologies, les usages du numérique et les métiers de l'entreprise. Curieux, ils sont en capacité d'exploiter les ressources de connaissances de l'entreprise ».

Source : Entreprises et Culture Numérique, p.35

Consumérisme : au sens « Anglic. Protection des droits et intérêts du consommateur par l'intermédiaire d'associations, d'actions collectives. », in Robert 2011.

Cross-canal : une approche *cross-canal* consiste à établir une synergie entre les différents canaux de vente et de communication (une stratégie et des objectifs communs en partageant les données), et est une évolution logique du « multi canal », qui utilise les différents canaux de vente et de communication de manière indépendante avec des objectifs propres à chaque canal.

Crowd-sourcing (en français : « externalisation ouverte » ou « collaborative ») : « domaine émergent de la gestion des connaissances, il s'agit d'utiliser la créativité, l'intelligence et le savoir-faire d'un grand nombre de personnes, en sous-traitance, pour réaliser certaines tâches traditionnellement effectuées par un employé ou un entrepreneur ». Le *crowd-sourcing* mobilise « l'intelligence des foules ».

Source : http://fr.wikipedia.org/wiki/Crowdsourcing

Digital : L'adjectif « digital » est associé au substantif « doigt » : « Digital » est un anglicisme traduit en français par « numérique », et auquel le terme « numérique » doit être préféré selon l'Académie française.

Droit à l'oubli numérique Pas encore défini juridiquement, le droit à l'oubli numérique est le thème central du futur projet de règlement européen sur la protection des données à caractère personnel. Il vise à renforcer la protection de la vie privée et les droits des internautes, pour leur permettre de mieux maîtriser leur vie en ligne.

Internet des objets : il s'agit de « l'extension d'Internet à des choses et à des lieux dans le monde physique. Alors qu'Internet ne se prolonge habituellement pas au-delà du monde électronique, l'internet des objets (IdO) a pour but de l'étendre au monde réel en associant des étiquettes munies de codes, de puces RFID ou d'URLs aux objets ou aux lieux. »

Source : http://fr.wikipedia.org/wiki/Internet_des_objets

Irradiation : perte de contrôle de l'information due à la dématérialisation (des flux financiers par exemple) favorisée et démultipliée par Internet.

Lock-in : Le phénomène de lock-in signifie qu'une entreprise devient dépendante d'un fournisseur, du fait des biens ou des services que fournit ce dernier.

Smart grids : il s'agit d'une « des dénominations d'un réseau de distribution d'électricité « intelligent » qui utilise des technologies informatiques de manière à optimiser la production, la distribution, la consommation et qui a pour objectif d'optimiser l'ensemble des mailles du réseau d'électricité qui va de tous les producteurs à tous les consommateurs afin d'améliorer l'efficacité énergétique de l'ensemble. »

Source : https://fr.wikipedia.org/wiki/Smart_grid

Sponsor : Le « sponsor » est celui qui a le pouvoir de modifier l'organisation sur le périmètre du projet.

Le cadre réglementaire actuel

1. Textes législatifs relatifs à la sécurité des systèmes d'information (non exhaustif)

Textes	Faits visés	Sanctions	Objet cible	Personnes
Art. 323-1 **Code pénal** **RISQUE PENAL**	Accéder ou se maintenir dans un système de traitement automatisé de données (STAD)	Peine d'emprisonnement : de 2 à 5 ans de prison Amende : de 30. 000 à 75.000 € (X 5 lorsque les faits sont commis par une personne morale) Peines complémentaires (interdiction de droits civiques, etc. et peines prévues à l'article 131-39 du Code pénal.)	Système d'information	**RESPONSABLE** Dirigeant de la personne morale (qui a par exemple demandé un espionnage du SI d'un concurrent) Personne morale selon l'art 323-6 du Code pénal
Art. 323- 2 **Code pénal** **RISQUE PENAL**	Entraver ou fausser le fonctionnement d'un STAD	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 75.000 € Peines complémentaires (interdiction de droits civiques, etc. et peines prévues à l'article 131-9 du Code pénal.)	Système d'information	**RESPONSABLE** **Dirigeant de la personne morale** (qui a par exemple demandé un espionnage du SI d'un concurrent) **Personne morale** selon l'art 323-6 du Code pénal
Art. 323-3 **Code pénal** **RISQUE PENAL**	Introduire frauduleusement des données dans un STAD ou modifier, supprimer frauduleusement les données qu'il contient	**Peine d'emprisonnement:** 5 ans de prison **Amende :** 75.000€ Peines complémentaires (interdiction de droits civiques, etc. et peines prévues à l'article 131-9 du Code pénal.) *Tout fait permettant de commettre les infractions susmentionnées est puni des mêmes peines (art 323-3-1 du Code pénal)*	Système d'information	**RESPONSABLE** **Dirigeant de la personne morale** (qui a par exemple demandé un espionnage du SI d'un concurrent) **Personne morale** selon l'art 323-6 du Code pénal
Art. 323-4 **Code pénal** **RISQUE PENAL**	La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1	Peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée	Système d'information	**RESPONSABLE** **Dirigeant de la personne morale** (qui a par exemple demandé un espionnage du SI d'un concurrent) **Personne morale** selon l'art 323-6 du Code pénal
Art. 323-7 **Code pénal** **RISQUE PENAL**	Vise la tentative des délits prévus par les articles 323-1 à 323-3-1 du Code pénal	Mêmes peines que si l'infraction avait été commise	Système d'information	**RESPONSABLE** **Dirigeant de la personne morale** (qui a par exemple demandé un espionnage du SI d'un concurrent) **Personne morale** selon l'art 323-6 du Code pénal

.../...

Textes	Faits visés	Sanctions	Objet cible	Personnes
Art. 432-9 **Code pénal** **RISQUE PENAL**	Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances. Le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseaux ouverts au public de communications électroniques ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu	**Peine d'emprisonnement :** 3 ans de prison **Amende :** 45000€	Système d'information (plus spécifiquement la messagerie électronique)	**VICTIME** **Personne (ex : dirigeant d'une entreprise) dont le secret des correspondances a été violé** par le dépositaire de l'autorité publique ou l'agent d'un exploitant de réseau ouvert au public
Art. 226-4-1 **Code pénal** **RISQUE PENAL**	Usurpation d'identité sur les réseaux (ex : une personne parle au nom et pour le compte d'une autre à partir d'une adresse de courrier électronique ou sur les réseaux… et ce dans une optique professionnelle)	**Peine d'emprisonnement** : 1 an de prison **Amende** : 15.000 €	Réputation d'un dirigeant, d'un salarié quelconque ou d'une entreprise (par exemple)/ Complément de l'atteinte au STAD	**VICTIME** **Dirigeant, salarié ou DSI** de l'entité ayant subi l'attaque
Art. 226-15 **Code pénal** **RISQUE PENAL**	Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance Le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions	**Peine d'emprisonnement :** 1 an de prison **Amende :** 45.000 €	Système d'information (plus spécifiquement la messagerie électronique)	**VICTIME** **Dirigeant, salarié ou DSI de l'entité** dont les correspondances ont été interceptées ou utilisées
Art. 34 **Loi Informatique, Fichiers et Libertés** **+ Art. 226-17** **Code pénal** **+ Art. 30 du projet de Règlement en matière de DCP** **RISQUE PENAL**	Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978	**Peine d'emprisonnement** : 5 ans de prison **Amende** : 300.000 € (X 5 lorsque les faits sont commis par une personne morale)	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Dirigeant de la personne morale** qui n'a pas mis en place les conditions de sécurité concernant les traitements de données à caractère personnel & Personne morale selon l'art 323-6 du Code pénal

Textes	Faits visés	Sanctions	Objet cible	Personnes
Art. 34 bis Loi Informatique, Fichiers et Libertés + Art. 226-17-1 Code pénal +Art. 31 et 32 du projet de Règlement en matière de DCP	Absence de notification d'une violation de données à caractère personnel à la CNIL ou l'intéressé	**Peine d'emprisonnement** : 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**VICTIME Les dirigeants, personnes** dont les données à caractère personnel ont été accédées du fait de failles de sécurité découlant des manquements d'un fournisseur de services de communications électroniques
Art. 14 du projet de Directive relative aux mesures visant à assurer un niveau élevé de sécurité des SSI à l'échelle européenne	Absence de notification des incidents de sécurité	Non encore fixé	Système d'information	**VICTIME Dirigeants** dont les données ont été accédées du fait d'un manquement à la sécurité d'un opérateur du marché
Art. 226-18 Code pénal + Art. 5 du projet de Règlement en matière de DCP	Collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**
Art. 226-18-1 Code pénal + Art. 19 du projet de Règlement en matière de DCP	Procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**
Art. 226-19 Code pénal + Art. 9 du projet de Règlement en matière de DCP	Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation ou identité sexuelle de celles-ci. Le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté	**Peine d'emprisonnement :** 5 ans de prison **Amende** : 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**

.../...

Textes	Faits visés	Sanctions	Objet cible	Personnes
Art. 226-20 Code Pénal **+Art. 5 du projet de Règlement en matière de DCP**	Conserver des données à caractère personnel au-delà de la durée prévue par la loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la loi. Le fait, hors les cas prévus par la loi, de traiter à des fins autres qu'historiques, statistiques ou scientifiques des données à caractère personnel conservées au-delà de la durée mentionnée au premier alinéa.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Personne chargée de la collecte et du traitement** des données personnelles **Personne morale** selon l'art 226-24 du Code pénal
Art. 226-21 Code pénal **+Art. 5 du projet de Règlement en matière de DCP**	Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**
Art. 226-22 Code pénal **+Art. 6 du projet de Règlement en matière de DCP**	Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir.	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 € La divulgation est punie de **3 ans d'emprisonnement** et de **100 000 € d'amende** lorsqu'elle a été commise par imprudence ou négligence	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** **Personne chargée de la collecte et du traitement** des données personnelles **Personne morale**
Art. 226-22-1 Code pénal **+Art. 40 du projet de Règlement en matière de DCP**	Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée	**Peine d'emprisonnement :** 5 ans de prison **Amende :** 300.000 €	Système d'information, plus spécifiquement les traitements de données à caractère personnel	**RESPONSABLE** Personne chargée de la collecte et du traitement des données personnelles Personne morale

Textes	Faits visés	Sanctions	Objet cible	Personnes
Art. L. 335-1 et s Code de la propriété intellectuelle RISQUE PENAL et CIVIL	Atteinte aux droits patrimoniaux concernant une base de données, un logiciel, un logo, une marque… Contrefaçon	**Peine d'emprisonnement** : 3 ans de prison (5 ans si commis en bande organisée) **Amende** : 300.000 € (500.000 € si commis en bande organisée)	Base de données, Logiciel (libre ou propriétaire), marque, logo, charte graphique, dessin, modèle, œuvre de l'esprit,…	**RESPONSABLE Complicité du dirigeant** (ou de la personne visée dans une délégation de pouvoir)
Art. 1384 al. 5 Code civil RISQUE CIVIL	Agissements d'un salarié (y compris responsable de la sécurité informatique) dans le cadre de ses attributions et sans faute détachable de ce dernier (ex: transmission d'un spyware compris dans le cadre d'un échange par mail, sans politique de sécurité de la part de l'entreprise émettrice)	Souvent des dommages intérêts	Système d'information	**RESPONSABLE Complicité du dirigeant** (ou de la personne visée dans une délégation de pouvoir)

2. TEXTES LÉGISLATIFS RELATIFS À LA SÉCURITÉ DES SYSTÈMES D'INFORMATION PAR SECTEUR D'ACTIVITÉ (NON EXHAUSTIF)

Textes	Faits visés	Périmètre d'application (secteur, société, etc.)	Code applicable	Personnes responsables
Normes Bâle I, II et III	Normes visant en la matérialisation du risque de crédit des établissements financiers et au renforcement de leurs fonds propres. Initiées en 1988 et renforcées successivement en 2004 (Bâle II) et 2010 (Bâle III), ces normes impactent directement les systèmes d'information au travers des enjeux de traçabilité, d'archivage et de qualité de l'information nécessaire au calcul des fonds propres : - les méthodes de mesure du risque sont fondées sur une période d'observation historique minimale de 5 ans ; - les bases de données et les systèmes dédiés au calcul des ratios applicables pour ces normes doivent garantir une traçabilité des informations exploitées	Etablissements de crédit	Règlement 97-02 du Comité de la Réglementation Bancaire et Financière (CRBF) : - Article 7 et 11-3 : Séparation des fonctions - Article 12 - Piste d'audit - Article 13 - Fiabilité de l'information financière et comptable - Article 14 - Sécurisation des moyens informatiques - Article 37-2 - Continuité d'activité	Direction Générale Direction Administrative et Financière
Solvency II (Solvabilité 2)	Réforme réglementaire visant au renforcement des fonds propres des sociétés d'assurance et de réassurance. Cette réforme impacte les systèmes d'information au travers des enjeux de : - traçabilité, - archivage, - sécurité (gestion des accès, sauvegarde, continuité d'activité), - qualité des données	Sociétés d'assurance ou de réassurance	Solvency II Consultancy Papers : - CP 33 - System of governance - CP 49 - Technical Provisions - Article 86f - CP 56 - Tests and Standards for Internal Model Approval - Articles 120 à 156 - CP 58 - Supervisory Reporting and Public Disclosure Requirements	Direction Générale Direction Administrative et Financière

.../...

Textes	Faits visés	Périmètre d'application (secteur, société, etc.)	Code applicable	Personnes responsables
Hébergement de données de santé : loi Kouchner	Procédure d'agrément des hébergeurs qui gèrent des données de santé à caractère personnel. Conformément au décret, l'hébergeur se doit : - d'organiser le dépôt des données de santé dans un environnement garantissant leur pérennité et leur confidentialité ; - de mettre en place des mesures garantissant la sécurité des informations de santé (traçabilité, archivage, sécurité des SI et contrôle des droits d'accès). Le ministère délivre un agrément tous les 3 ans, avec implication de la CNIL dans la délivrance de l'agrément	Hébergeurs de données de santé	Décret n°2006-6 du 4 janvier 2006	Direction Générale Direction des Systèmes d'Information
ARJEL	Agréments accordés aux opérateurs de jeux en ligne et dont les conditions d'obtention sont soumises à la sécurisation et la traçabilité des informations des joueurs réputés français. La loi prévoit que chaque agrément donne lieu à la mise en place d'un dispositif technique qui permet de garantir une traçabilité des opérations de jeu d'une part, et de générer et de transmettre des rapports sur l'activité de jeu d'autre part	Opérateur de jeux en ligne (paris hippiques, paris sportifs, jeux de cercles)	Décret n° 2010-482 du 12 mai 2010 - Conditions de délivrance des agréments d'opérateur de jeux en ligne	Direction Générale
CFCI (Contrôle Fiscal des Comptabilités Informatisées)	Législation couvrant la présentation de documents comptables et couvre la traçabilité et l'archivage (fournir au Trésor les supports dématérialisés des comptes). Cette démarche est dorénavant obligatoire	Toute entité tenue à la présentation de documents comptables	Article L13-AA du LPF créé par LOI n°2009-1674 du 30 décembre 2009 - art. 22 (V) Article L47 A modifié par LOI n°2007-1824 du 25 décembre 2007 - art. 18 (V)	Direction Générale Direction Administrative et Financière
CNIL : loi I&L de 1978	Cette loi concerne toute forme d'organisation et couvre la traçabilité, l'archivage et la sécurité des accès à l'information + proposition de règlement européen sur la protection des données à caractère personnel. - Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. - Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des «tiers autorisés» ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc). - Les données personnelles ont une date de péremption. Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier. - Le responsable d'un fichier doit permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées. - Les traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être soumis à l'autorisation de la CNIL. - Un fichier doit avoir un objectif précis. Les informations exploitées dans un fichier doivent être cohérentes par rapport à son objectif. Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées	Toutes formes d'organisation	Loi 78-17 1978-01-06 art. 34	Propriétaire des fichiers ou des traitements informatiques de données à caractère personnel

Textes	Faits visés	Périmètre d'application (secteur, société, etc.)	Code applicable	Personnes responsables
Loi de sécurité financière, SOX, …	Sécurisation des processus concourant à l'établissement des états financiers. Les entreprises doivent mettre en place des référentiels de contrôle et évaluer l'efficacité opérationnelle des contrôles. Les processus informatiques rentrent dans le périmètre d'application pour les applications / infrastructures supportant les processus concourant à l'établissement des états financiers.	Sociétés Anonymes Sociétés faisant appel à l'épargne publique Sociétés cotées sur les bourses américaines	Article L225-68 modifié par LOI n°2011-103 du 27 janvier 2011 - art. 2 Article L225-235 modifié par LOI n°2009-526 du 12 mai 2009 - art. 46 (V)	Direction Générale Directeur Financier

3. Normes et standards relatifs à la sécurité des systèmes d'information (non exhaustif)

Textes	Faits visés	Périmètre d'application (secteur, société, etc.)	Code applicable	Personnes responsables	Remarque / Commentaires
Norme COBIT	Gouvernance et contrôle des processus, bonnes pratiques orientées Métiers, guide pour le management et les responsables de processus	Tout type d'organisation	N/A	DSI	
Norme ISO 27001	Certification relative à la sécurité des SI, depuis leur développement jusqu'à leur management	Tout type d'organisation	N/A	DSI	La certification ne porte que sur des processus et pas sur toute l'entreprise. Quand une entreprise se dit «conforme», il faut faire attention car il n'existe pas d'entreprise certifiée ISO 27001 en France. Si une entreprise se déclare certifiée, il faut regarder le périmètre d'application et le résultat de la certification
Norme ITIL	Bonnes pratiques relatives au management du SI, vise essentiellement les centres de services	Tout type d'organisation	N/A	DSI	
PCI-DSS	Norme particulière, encadrée par le PCI Security Standards Council destinée aux acteurs de e-commerce, hébergeurs de système de paiement. Elle fixe des principes de traçabilité et sécurité des accès => 6 objectifs de contrôle faisant référence à 12 exigences	Acteurs e-commerce Hébergeurs de système de paiement	N/A	DSI	PCI-DSS : est-il un *lobby* ou une norme réelle ? Les entreprises doivent mettre en place des éléments de prévention pour que, *in fine*, les banques n'aient pas à couvrir les risques entreprises….

10 tendances structurantes de la transition numérique des entreprises

Primauté de l'expérience client

L'émergence du numérique (ou digital) au sein de notre société modifie le comportement des consommateurs, intensifie la concurrence entre les entreprises, et ouvre de nouveaux marchés. Pour répondre à ces défis, l'entreprise doit repenser dans son ensemble ses relations avec le client. En premier lieu, elle doit saisir l'opportunité offerte par Internet d'impliquer le client dans sa chaine de valeur, en ouvrant son espace de co-création de valeur, afin de coller au plus près de ses attentes et lui apporter les produits et les services associés dont il a besoin. La création d'un écosystème de marque vient compléter cette démarche. Il permet à l'entreprise, grâce à une approche cross-canal, de fidéliser le client et de s'ouvrir à de nouveaux marchés émergents. Enfin, l'entreprise est face à un défi majeur : celui d'animer sa communauté de fans, dans son écosystème et sur les réseaux sociaux, afin d'en faire un relais de communication efficace et de croissance durable.

1 - Les services associés : de la proposition de valeur à l'expérience client

La conjonction de l'hyper-compétition caractéristique du contexte économique actuel avec la multiplication des artefacts numériques rend l'avantage concurrentiel d'une entreprise éphémère. Le produit seul n'est plus différenciant : l'avantage concurrentiel s'opère désormais au travers des services associés. Il ne s'agit plus de proposer aux clients un produit, mais une expérience. Ainsi, la transition numérique casse la vision traditionnelle de l'entreprise, et ouvre l'espace de co-création de valeur dans lequel s'intègre aussi le client, dans ses formes multiples, grâce notamment à la customisation.

2 - La plateforme clients : un espace central de promotion de l'expérience client

Dans un contexte hyper-compétitif, avec un développement de multiples canaux de communication et de commerce, une personnalisation des produits et des services associés, la plateforme client devient un espace central de promotion de l'expérience client. Pour tirer profit de la présence des clients sur les espaces numériques, l'entreprise doit donc non seulement intégrer le client au sein de l'espace de co-création de valeur, mais en plus créer un écosystème autour de sa marque, de ses produits, reposant sur une plateforme clients, pour permettre sa différenciation. Cette différenciation lui permettra de capter un public de clients démultiplié par le développement des pays émergents et des moyens d'accès à internet, alternatifs à l'ordinateur.

3 - L'importance d'une communication interactive avec les communautés de fans pour tirer partie de leur influence

Face à l'apparition de communautés de fans sur les réseaux sociaux et à leur influence grandissante, les enjeux pour l'entreprise portent à la fois sur son e-réputation mais aussi sur la récupération d'*insights-clients*, le *crowdsourcing* et l'utilisation de ces communautés comme un relais de communication et d'influence. La gestion de cette communauté représente de multiples challenges pour l'entreprise numérique : rapprocher au maximum l'identité de la communauté de l'image de marque qu'elle souhaite renvoyer, entretenir la vie et l'attractivité de la communauté et pour finir convertir les liens organiques qui organisent la communauté de fans en liens transactionnels.

Organisation et management liés à la co-création de valeur

L'ensemble des transformations numériques montrent qu'il est primordial d'accepter que la création de valeur soit entrée dans une dynamique collective. Aussi, les exigences managériales et structurelles deviennent claires : rendre les communications organisationnelles plus transparentes pour partager une vision stratégique commune, adopter une architecture agile et ouverte vers tout l'écosystème de l'entreprise, mettre en place un mode de gouvernance fondé sur la concertation et l'implication de tous les acteurs de la chaine de valeur.

4 - L'adoption d'une démarche d'open innovation pour engendrer de nouveaux avantages compétitifs

L'open innovation répond à la réduction du *time to market,* l'accroissement exponentiel des sources d'idées, l'essor des modes de communication digitaux interactifs et le besoin de réactivité et de différenciation. Les enjeux de l'adoption d'une démarche d'open innovation consistent en un meilleur partage des risques sur des marchés incertains et en pleine évolution. Un équilibre doit être toutefois trouvé entre le nombre potentiel de partenaires et l'intensité des partenariats. L'adoption d'une démarche d'open innovation n'empêche pas, par ailleurs, la coexistence dans l'entreprise de modèles plus traditionnels de construction de l'innovation.

5 - Vers un management par les résultats

L'arrivée de la génération Y dans l'entreprise, conjuguée à l'augmentation des *devices* personnels sur le lieu de travail (Phénomène BYOD) et l'accès permanent à Internet posent la question des nouveaux modes d'organisation du travail et de la productivité au travail. Tout se passe comme si les nouveaux collaborateurs en entreprise, plus connectés, plus polyvalents, (plus dispersés ?), réinterrogeaient par leurs valeurs et leurs comportements le sens donné au travail et la manière dont il s'effectue. Dès lors tous ces éléments conjugués semblent modifier le management vers un management par les résultats, avec un plan de charge adapté et une prise en compte de ces nouvelles pratiques.

6 - Le bénéfice des dynamiques collaboratives

La création de valeur s'inscrit dans une dynamique collective. Cette dynamique collective se traduit en entreprise par une série de phénomènes collaboratifs, aujourd'hui en émergence, qu'il convient d'exploiter. D'un point de vue managérial, les enjeux de ces dynamiques collaboratives portent autant sur la cohésion des employés, leur association et leur adhésion au projet d'entreprise, leur responsabilisation, ainsi que sur une intelligence collective partagée permettant une meilleure proposition de valeur.

Gestion des ressources et flux accélérés

Dans un contexte d'accélération numérique, à la croisée des transformations sociétales et de la standardisation des gouvernances SI, l'entreprise doit être en mesure de capter et analyser une grande quantité d'informations provenant de sources multiples, afin de mettre en place de nouvelles propositions de valeur co-créée avec ses clients.

7 - Le SI : plateforme de services pour l'entreprise ?

La mise en place de ces nouvelles propositions doit être facilitée par une architecture SI flexible reposant sur la modularité de ses composants ainsi que la maitrise des flux métiers. Cette flexibilité doit être au service de l'expérimentation et offrir des coûts maitrisés afin de proposer une capacité d'innovation basée sur non plus sur la théorie mais sur l'empirisme. Au delà du caractère technique, c'est une appropriation par le métier de l'outil SI qu'il convient d'affirmer afin de qualifier et d'exploiter les leviers de croissance à venir.

8 - Big Data : L'information donne enfin son sens au système

La multitude de capteurs et d'entrées offre un très large panel d'informations disponibles. Parallèlement, les capacités de traitement se sont améliorées et leurs coûts ont baissé. Les enjeux de cette tendance émergente portent sur le croisement des sources d'information dans le but de développer un avantage compétitif, il s'agit également de donner du sens aux données (la captation et l'exploitation des données non structurées apparait par ailleurs comme un enjeu clef pour le business) et de mettre en place des outils à la portée du métier permettant une manipulation simplifiée des informations.

9 - Le Cloud : quel avenir pour la fonction SI ?

L'intégration progressive du Cloud computing dans les entreprises génère de nombreuses problématiques : sécurité, impact organisationnel… Le Cloud semble se caractériser comme une technologie disruptive (plutôt que comme un phénomène d'*IT fashion*), qui entraine une série de ruptures : humaine (passage d'une vision technique à une vision d'usages, catalogue de services, collaboratif), technique, de marché, mais aussi sécuritaire (problématique de contractualisation, de compliance et réversibilité). Au-delà d'une baisse des coûts de maintenance, l'externalisation d'une composante technique et non cœur de métier va-t-elle permettre à la fonction SI de se recentrer sur les projets à haute valeur ajoutée ?

10 - Gestion de la mobilité : un défi pour assurer la permanence du service

Les nouveaux outils numériques conjugués à des performances techniques poussées sur les différentes plateformes entraînent une multiplication des interactions en temps réel entre les différents acteurs de l'entreprise. L'interconnectivité des informations, l'accès facilité aux données sont autant d'enjeux liés à la gestion de la mobilité. La mobilité associée au phénomène de consumérisation pose par ailleurs la problématique de la performance *versus* source de distraction. Elle interroge en outre les principes de sécurité et la permanence de services. La mobilité impacte la fonction SI au travers de la compatibilité entre les différentes plateformes, la gestion des connexions multiples et des appareils mobiles en parallèle.

Source : CIGREF

TRANSFORMATION NUMÉRIQUE

UN NOUVEAU VOCABULAIRE POUR LES CONSEILS D'ADMINISTRATION

IFA - Institut Français des Administrateurs

11bis, rue Portalis
75008 Paris
www.ifa-asso.com
contact@ifa-asso.com

CIGREF, réseau de Grandes Entreprises

21, avenue de Messine
75008 Paris
www.cigref.fr
cigref@cigref.fr

IFA-CDECORTIAT-10092013