Cigref
RÉUSSIR
LE NUMÉRIQUE

AUDITER LA GOUVERNANCE DU NUMÉRIQUE

Les évolutions majeures du Guide d'audit de la gouvernance du numérique

NOVEMBRE 2023

Cigref

Auditer la gouvernance du numérique

Les évolutions majeures du Guide d'audit de la gouvernance du numérique

Novembre 2023

ÉDITO

Les organisations constatent aujourd'hui, qu'avec l'accélération des évolutions technologiques, la *softwarisation* des produits et des chaînes de production, et la numérisation de l'ensemble des processus des organisations, la contribution du numérique à la chaîne de valeur de l'entreprise augmente considérablement. Pour les organisations membres du Cigref, ce phénomène se caractérise par un accroissement de leur dépendance vis-à-vis du numérique et une augmentation des vulnérabilités et risques afférents.

Les trois dernières années ont été riches en évolutions, certaines se sont même avérées structurantes pour les modèles opérationnels des directions du numériques et pour la gouvernance du numérique en entreprise. La croissance, la performance et la résilience des organisations dépendent désormais des technologies numériques.

Nous observons ainsi la généralisation des démarches « agiles », l'hybridation du *sourcing* de l'IT (cloud ou en interne), l'évolution des modèles de *make or buy*, mais aussi le développement de nouvelles pratiques telles que le DevOps et surtout une évolution des rôles et des missions des directions du numérique.

C'est dans ce contexte que le Cigref a lancé une réflexion portant sur l'évolution du « Guide d'audit de la Gouvernance du SI ». Elle s'est matérialisée par un groupe de travail constitué de membres aux profils métiers variés, et dont la mission était de reconsidérer les 12 vecteurs socles du Guide d'audit, au regard des évolutions de la fonction numérique depuis 2019.

Le résultat des travaux du groupe sont donc restitués dans la présente note qui offre une synthèse des bonnes pratiques à partager et qui constituera une bonne matière pour la prochaine édition du Guide, sur laquelle nous travaillerons avec nos partenaires historiques, l'ISACA-AFAI et l'IFACI.

Djilali KIES
DSI chez TDF, pilote du groupe de travail

REMERCIEMENTS

Nos remerciements vont à **Djilali KIES, Chief Information Officer** chez **TDF**, qui a piloté ce travail, ainsi qu'à toutes les personnes qui ont participé et contribué à ce groupe de travail Cigref (ordre alphabétique) :

Olivier CAIL - MAÏSADOUR

Michel CAPEL - FAYAT

Claudio CIMELLI - MINISTERE

Fabienne CHEVALIER - MINISTÈRE ÉCOLOGIE

Michel DEBLBECQ - ELIS

Erik DU BOISHAMON - MINISTÈRE INTÉRIEUR

Bruno GIVELET - SYSTÈME U

Gaëlle GOSSE DE GORE - DPD GROUP

Mélanie GRAS - SAVENCIA

Nicolas GRIMAULT - SODEXO

Michel HALABI - AIR FRANCE KLM

Franck HOSTIOU - PIERRE FABRE

Julien JOLIBOIS - MALAKOFF HUMANIS

Bertrand LASQUELLEC - GROUPE AVRIL

Frédéric LEBOEUF - VINCI

Thibaut MITANCHEZ - SFR

Julien MONTAROU - TOTALENERGIES

Guillaume MONTIGNY - BNP PARIBAS

Coralie NICOLLET - MATMUT

Stéphane OLIVE – ACCOR

Michel PEPINO - VIRBAC

Sofiane SAMAH - MSA

Nadia SELLAMI - ACCOR

Vasco ROGEON - SNCF

Nicolas VACHÉ - SYSTÈME U

Nos remerciements vont aussi à Aliette DIÉVAL, juriste, qui a contribué à ces travaux au cours de son stage au Cigref. Ce document a été construit et rédigé par Elena SILVERA, Chargée de mission au Cigref.

TABLE DES MATIÈRES

1 INTRODUCTION

Pourquoi mettre à jour le Guide d'audit de la gouvernance des systèmes d'information ?

En 2019, année de la dernière version du *Guide d'audit*, on constatait déjà l'empreinte accrue de la technologie numérique sur les activités des entreprises et des administrations. Depuis, les évolutions technologiques et les transformations se sont nettement accélérées.

L'extension des missions acquises par les « Directions des systèmes d'information » influence la terminologie même de ces entités dans certains groupes. On parle aujourd'hui de « Direction du numérique et de la transformation », de « Direction de la technologie et de l'innovation » ou encore d'autres déclinaisons de ces appellations, qui reflètent bien les changements qui affectent la « DSI » depuis quelques années. Pour cette raison nous avons choisi d'intituler ce rapport *Auditer la gouvernance du* numérique*,* et non pas « auditer la gouvernance du SI ».

L'accélération des transformations induit naturellement une inflation des attentes que les « clients de la DSI » expriment (attentes des métiers notamment), ainsi qu'une évolution de l'offre de services et du modèle opérationnel de la DSI. Ces éléments appellent donc une actualisation de la gouvernance des systèmes d'information, ou, pour être plus proche des nouvelles réalités de la DSI, de la « gouvernance du numérique ».

Le Guide 2019 présentait la DSI comme une entité investie de rôles et mandats liés entre eux, pour assurer le *RUN*, le *BUILD* et la « vision » au sein de l'organisation (cf schéma ci-dessous)[1].

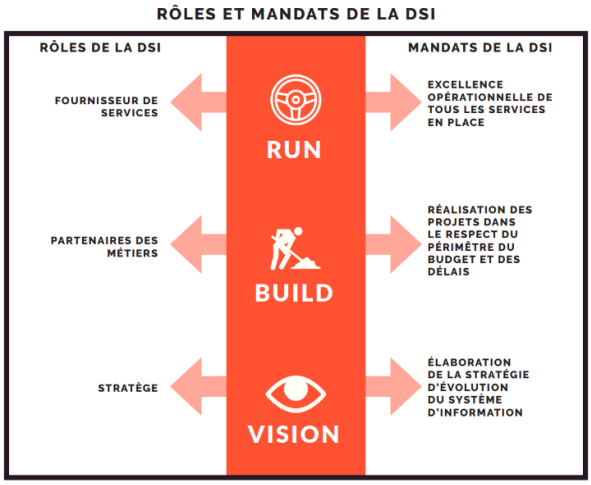

Figure 1 : Rôles et Mandats de la DSI, Guide d'audit de la gouvernance du SI, 2019

[1] « Le *RUN*, représente le 'récurrent' ce qui 'permet à une DSI de fonctionner', souvent résumé par 'maintien en conditions opérationnelles', ou encore 'tout ce qui ne relève pas du BUILD'. Pour rappel, le *BUILD* est constitué des projets, améliorations et efforts déployés pour générer de la valeur au sein de l'entreprise », Rapport Cigref *Leviers de réduction des coûts de la DSI*, juin 2023. Voir aussi le *Modèle de pilotage économique et écologique de l'IT*, éd. 2022.

Dans cette approche et s'agissant du *RUN*, la DSI a un rôle de fournisseur de services pour le « reste » de l'entreprise, et dans ce cadre, son mandat est d'assurer l'excellence opérationnelle de tous les services en place.

Pour le *BUILD*, la DSI agit en qualité de partenaire des métiers, et veille donc à la réalisation des projets dans le respect du périmètre, des budgets et des délais qui lui sont conférés.

Enfin, la « vision » place la DSI dans un rôle de stratège. Son mandat est d'élaborer et de mettre en œuvre la stratégie d'évolution du système d'information et du numérique dans l'entreprise.

Aujourd'hui, ces rôles et mandats ne semblent pas avoir perdu en pertinence, mais plusieurs paramètres rendent nécessaire une actualisation de cette description. Ces « fondamentaux de la DSI » sont directement concernés par plusieurs transformations récentes survenues dans le monde de l'entreprise.

Les grandes lignes d'évolution

Le contexte général recèle des facteurs expliquant les transformations qui touchent la DSI : la généralisation du télétravail, l'*agilisation* des pratiques ainsi que le phénomène d'*inshoring* et de retour au « local ».

Il y a encore quelques années, les systèmes d'information étaient constitués d'un patrimoine d'applications et d'infrastructures non mutualisés. Puis, ces modèles ont connu un mouvement progressif d'hybridation, qui a vu émerger une coexistence entre les anciens SI, dits « historiques » (ou « *legacy* ») et de nouveaux modèles de services tels que le *Software as a Service* (SaaS), *Platform as a Service* (PaaS) et *Infrastructure as a Service* (IaaS). Ces nouveaux modèles de services, liés au cloud, contribuent à un important bouleversement des modes de travail, des modèles de fourniture de services (*delivery*), et d'approvisionnement (*sourcing)* du SI. Si les évolutions observées aujourd'hui ne sont pas de simples tendances, c'est notamment parce que le cloud s'est généralisé, de sorte que toute entreprise ou administration utilise désormais à la fois le cloud et des solutions *on-premises*[2].

Comment lire ce rapport ?

Ce document constitue un **appendice** au *Guide d'audit de la gouvernance du SI*, publié en 2019. Il apporte donc des compléments utiles à la bonne mise en place d'une gouvernance du SI à l'aune des dernières évolutions impactantes en matière de technologie et d'innovation numérique.

La construction du document reprend celle du Guide : les vecteurs sont présentés un à un, en suivant l'ordre du Guide. Toutefois, plusieurs vecteurs n'ont pas été étudiés cette année et pourront faire l'objet de travaux futurs : « Projets », « RH », « Portefeuille projets », et « Prestataires & fournisseurs ». À noter : alors que le Guide présentait quatre dimensions pour chaque vecteur (enjeux, menaces,

[2] *On-premises* ou « sur site » se définit comme l'utilisation des matériels informatiques de l'entreprise pour ses propres systèmes et applications, cf rapport Cigref *Stratégies de migration dans le cloud. Un défi structurant pour l'entreprise, version 2023*

risques et bonnes pratiques), ce document ne considère que deux éléments : les nouvelles menaces et les nouvelles bonnes pratiques.

Il convient de rappeler que les vecteurs sont autoporteurs : ils sont analysables et « auditables » isolément. Mais ils peuvent également être considérés dans leur globalité pour une analyse holistique de la gouvernance du numérique.

2 STRATÉGIE

Le vecteur Stratégie avait pour sous-titre « Intégrer les enjeux numériques dans le plan stratégiques de l'entreprise ». Cette formulation appelle plusieurs remarques. Tout d'abord, le numérique n'est plus une entité isolée dans l'entreprise. Au contraire, il constitue un enjeu majeur pour toute organisation. Ensuite, il en découle que la stratégie de l'entreprise prend obligatoirement en compte le numérique. Enfin, ces évolutions invitent à considérer la stratégie numérique comme un pilier de la stratégie globale de l'entreprise.

La principale évolution constatée est l'importance croissante du numérique dans les chaînes de valeur et les produits de l'entreprise. La stratégie numérique tend à se confondre avec la stratégie globale dans certaines entreprises et certains secteurs d'activité. Le numérique est désormais, un facteur principal de croissance, de performance et aussi de risque industriel, et ce pour toutes les organisations. Le rôle des DSI se voit évoluer vers un rôle régalien allant au-delà des systèmes d'information et qui porte sur le numérique dans sa globalité, qui recouvre l'*Information Technology*, *l'Operational Technology* (IT et OT) et les produits. Pour finir, la valeur des produits est appréciée avec le bénéficiaire de celui-ci, à savoir les métiers, ce qui implique une collaboration étroite entre DSI et métiers au service de la stratégie.

2.1 LES NOUVELLES MENACES

La menace principale qui pèse sur le vecteur Stratégie est la prise en compte insuffisante du numérique dans la stratégie de l'entreprise, dit aussi « manque de vision ». Minimiser l'importance du numérique et des technologies, ou bien ne pas suffisamment anticiper les risques ou opportunités qui y sont liés serait une grande erreur stratégique. L'entreprise encourt alors un risque de disruption et ou de perte de parts de marché. La DSI doit donc plus encore qu'auparavant porter la « vision » de l'entreprise sur ces sujets pour lui permettre d'atteindre ses objectifs. Cette capacité à analyser les situations présentes, à se projeter, et à prendre les bonnes décisions en conséquence est requise non seulement à la DSI mais aussi dans les autres entités de l'entreprise, ce dont on peut déduire plusieurs bonnes pratiques.

2.2 LES NOUVELLES BONNES PRATIQUES

- ***Les sujets de transformation numérique bénéficient d'un sponsoring au plus haut niveau de l'entreprise.***
- Les dirigeants du numérique siègent au sein des instances exécutives de l'organisation.
- Des instances de gouvernance (avec les dirigeants) et de pilotage transverses assurent le suivi de la stratégie numérique de l'entreprise et sa traduction en projets.
- La stratégie et le risque numérique font partie de l'agenda du conseil d'administration.

- ***La veille stratégique est assurée largement au sein de la DSI et des Métiers.***

Le Guide recommandait que les « résultats de la veille [soient] partagés avec les responsables impliqués dans l'élaboration de la stratégie de l'entreprise ». Cette recommandation est toujours d'actualité mais elle doit s'étendre à l'ensemble de l'entreprise.

- ***La stratégie est déclinée et actualisée régulièrement en feuille de route de la transformation et en différentes politiques (architecturale, cyber, résilience).***

- Cette feuille de route doit témoigner de la capacité de l'entreprise à décliner sa stratégie et à intégrer de nouveaux projets en fonction des besoins et du contexte.
- La stratégie numérique comprend la résilience : elle est suffisamment modulable pour pouvoir intégrer les imprévus et réagir en cas de crise de nature économique, politique, sanitaire, cyber….

- ***L'organisation engage une réflexion autour de la RSE.***

L'entreprise met en place une commission de réflexion autour de la mesure de performance des enjeux RSE. Cela doit permettre à l'entreprise d'être préparée à l'hypothèse où une obligation réglementaire ou légale imposerait de rendre des comptes sur la performance RSE de l'entreprise (au titre du *reporting* extra-financier de l'entreprise).

3 INNOVATION

Alors que « tout devient numérique », la volonté de « diffuser la culture numérique et de promouvoir les technologies innovantes »[3] ne suffit plus. L'innovation est de plus en plus souvent confiée à la DSI, ou en tous cas, elle est traitée conjointement, par les mêmes acteurs que la technologie. L'innovation a désormais pour ambition d'« explorer et promouvoir les nouvelles technologies et usages numériques au service de la performance et de la croissance ». L'exploration des nouvelles technologies et des nouveaux usages numériques sont essentiels à l'exercice des missions de la DSI en matière de vision et d'anticipation des évolutions business.

Les principales évolutions relevées sont tout d'abord le travail en *labs,* des espaces dédiés à la qualification, l'expérimentation et à l'exploration (au sein de la DSI). Les DSI favorisent aussi « l'intrapreunariat numérique »[4] et utilisent le *Shadow IT* comme laboratoire pour détecter, tester et promouvoir de nouveaux usages. L'objectif est de susciter l'envie de tester et d'explorer ces technologies. Ces nouvelles méthodes sont vectrices de progrès mais font aussi apparaître de nouvelles menaces.

3.1 LES NOUVELLES MENACES

Le travail en *lab* s'inscrit dans une dynamique d'innovation à la DSI. Toutefois, l'innovation ne doit pas ignorer les problématiques de scalabilité, car elle risquerait de cantonner la DSI à un terrain de jeu et d'exploration qui ne donne jamais naissance à un produit. La valeur et la capacité à industrialiser doivent être prises en compte très tôt dans le processus d'exploration.

De plus, à travers ses *labs* et son travail de veille, la DSI identifie les innovations qui peuvent répondre à des besoins métiers. La menace inhérente à ce foisonnement d'innovation est de ne pas être capable de faire la part des choses entre ce qui est porteur de valeur et ce qui ne l'est pas. La DSI, en partenariat avec les métiers, doit être en mesure de discriminer les éléments à faible valeur ajoutée, ou sans intérêt pour l'entreprise.

3.2 LES NOUVELLES BONNES PRATIQUES

- ***Favoriser et encadrer l'intrapreneuriat numérique***

Le *Shadow IT* n'est plus considéré comme une menace en soi. En effet, il est plutôt perçu comme une opportunité pour l'entreprise, dans la mesure où il offre aux utilisateurs l'occasion de se familiariser avec les technologies, et, potentiellement, de faire des découvertes intéressantes pour l'entreprise. Les organisations sont donc invitées à « organiser et encadrer un espace de liberté » dans l'objectif de

[3] Vecteur Innovation, *Guide d'audit*, 2019, p20.

[4] Le terme « intraprenariat » résulte de la contraction de « intra », « à l'intérieur de », et « entreprenariat ». Il désigne la possibilité offerte aux collaboateurs d'une organisaton d'entreprendre et d'innover *au sein-même* de l'organisation.

favoriser « l'intrapreunariat » numérique, détecter les initiatives à généraliser (évolution des processus et des outils) et celles à encadrer ou bannir (risque sécurité ou conformité).

- La DSI accompagne les métiers dans le *low-code* de façon à encourager l'entreprenariat numérique.

➢ ***Des événements de promotion des nouvelles technologies numériques sont animés.***

Ces événements favorisent la culture de l'innovation au sein de l'entreprise. Ex : hackathons.

➢ ***La DSI organise avec les métiers des process d'idéation et d'exploration des nouveaux usages numériques.***

Le rôle de la DSI est la maîtrise de la technologie, dont elle doit assurer la fiabilité, l'exploitabilité et la maintenance. L'usage final de la technologie se situe côté métier. La DSI doit plus que jamais se doter de moyens de qualification des nouvelles technologies et d'anticipation des évolutions. Elle définit avec le métier les nouveaux usages à explorer. Ces usages portent sur la disruption des processus[5] ou des nouveaux concepts produits, pour accompagner la croissance. Des nouvelles compétences d'animation de l'innovation avec les métiers et les partenaires externes font désormais partie des compétences de la DSI.

➢ ***L'entreprise met en place une « Digital factory ».***

L'organisation de la DSI passe en « mode produit », via une généralisation de la culture « agile »[6]. Elle accélère la transformation en fonction des incréments de valeur. *In fine*, cette démarche permet de de faire face à l'incertitude.

[5] La disruption des processus est le fruit d'un questionnement en deux étapes 1 : « si on faisait autrement ? », par exemple, l'organisation choisit d'utiliser de l'IA pour planifier la maintenance ; et 2 : « si on faisait autre chose ? », par exemple, utiliser le numérique pour lancer un nouveau produit.

[6] L'agilité est définie dans le rapport Cigref *Agile at scale* comme « un moyen pour parvenir à s'adapter plus rapidement aux besoins du marché, détecter de nouvelles réserves de performance, livrer plus de valeur, plus vite à ses clients, attirer les talents et les fidéliser. L'agilité permet également de piloter au plus juste des budgets, souvent à la baisse, en mettant à la disposition des utilisateurs les fonctionnalités apportant le plus de valeur ». Selon ce même rapport, les organisations passent « du mode projet au mode produit pour livrer un produit clé en main et améliorer en continu la valeur apportée ».

4 RISQUES

Le vecteur Risque avait pour objectif de « prendre en compte les risques numériques dans les enjeux stratégiques et les processus métiers ». Ces risques numériques recouvraient deux volets : les risques technologiques et les risques cyber.

Au plan des risques technologiques, la principale préoccupation est celle des dépendances et du « verrouillage » (fournisseur ou technologique). Au plan de la cybersécurité, on relève que celle-ci a gagné en importance, non pas par changement de mode opératoire des attaquants, mais en raison de l'industrialisation de la cybercriminalité et de l'augmentation du volume des attaques.

4.1 LES NOUVELLES MENACES

Les nouvelles menaces sont de trois ordres : les menaces normatives, les menaces cyber et celles liées au cloud.

Le Guide proposait comme bonne pratique : « les risques SI prennent en compte les contraintes réglementaires, juridiques, contractuelles et sociales. »[7] Force est de constater qu'au cours des dernières années, le **paysage législatif et réglementaire** français, et plus encore européen, a connu de nombreuses évolutions. Les impacts sur le numérique sont significatifs. Outre le texte de la loi, ce sont les délais impartis pour la mise en conformité qui souvent mettent en difficulté les organisations. Le risque de non-conformité s'aggrave d'un risque financier puisque les entreprises encourent des sanctions économiques et/ou recourent aux conseils d'experts pour les aider à comprendre la portée des dispositions en cause, et les actions que cela suppose de leur part pour s'y conformer.

Ensuite, le **risque cyber**, déjà identifié dans le Guide, connaît pour principale évolution l'augmentation du volume des attaques. Cela implique de repenser les modalités de traitement de la cybersécurité au sein de l'organisation, en sachant que les dispositifs de protection et de réaction évoluent plus lentement que la menace.

Enfin, le **cloud**, en particulier le SaaS, comporte un risque accru de dépendance à l'égard des éditeurs. C'est un enjeu de souveraineté et un risque de verrouillage nouveau à prendre en considération[8].

Ces trois principales menaces confrontent l'entreprise à des défis divers mais aussi à un défi commun : la menace de ne pas pouvoir activer rapidement ses mécanismes de réponse. Elle doit donc se doter des ressources nécessaires pour réagir en cas de survenance d'une crise (cyber, géopolitique …).

[7] Critère n° 7, Bonne pratique n°3, Vecteur Risque, *Guide d'audit*… précité, p31.

[8] Sur ce point, consulter les « *11 Fair Principles* », rédigés par le Cigref avec les associations partenaires européenne Beltug, CIO Platform Netherland et VOICE.

4.2 LES NOUVELLES BONNES PRATIQUES

- ***L'entreprise met en place la sensibilisation continue et l'implication de tous les acteurs dans la prévenance des risques.***

Les métiers, tout comme la DSI, sont formés à prévenir les risques, à les anticiper et à y réagir lorsqu'ils surviennent. La cybersécurité et la conformité sont deux exemples significatifs : il est pertinent de rappeler que l'humain est le principal vecteur de risques. On peut donc en améliorer la maîtrise grâce à une bonne sensibilisation des acteurs de l'entreprise.

- ***La cybersécurité est considérée comme un risque stratégique ou industriel pour l'organisation.***

Maîtriser le risque cyber est un enjeu de résilience pour l'entreprise. Il ne s'agit pas seulement de chercher à empêcher la survenance du risque ou à réduire son impact, mais *d'assurer la continuité de fonctionnement de l'organisation* dans l'hypothèse où une crise surviendrait.

5 DONNÉES

Pour le vecteur Données, le Guide mettait en avant une première bonne pratique « Référentiel de données », en vertu de laquelle « l'entreprise [devait] identifier les données et les gérer comme un actif majeur de l'entreprise ». Cette bonne pratique est désormais un prérequis évident pour l'ensemble des organisations, qui doivent aller plus loin dans leur gestion des données. Aussi, une nouvelle formulation est proposée : *« L'organisation doit mettre en place sa propre gouvernance de la donnée, et la gérer comme un de ses actifs majeurs »*

5.1 LES NOUVELLES MENACES

Le Guide recommandait qu'en fonction des enjeux, « une cartographie des risques […] basée sur la criticité des données (confidentialité, intégrité, disponibilité, traçabilité) » soit mise en place dans le cadre de la protection des données de l'entreprise. Cette cartographie doit être mise à jour de façon très régulière, en raison de l'évolution rapide des risques.

5.2 LES NOUVELLES BONNES PRATIQUES

- ***L'entreprise dispose d'une stratégie autour de la donnée.***

Cette stratégie prend en compte les nouvelles possibilités technologiques ainsi que les contraintes techniques, juridiques et réglementaires. Elle opère dès la conception du produit et intègre une réflexion sur la vocation de la donnée : va-t-elle rester en interne ? être partagée ?... Dès la conception, il faut systématiser le traitement des conditions d'accès, les questions de confidentialité et veiller à la prise en compte des obligations réglementaires applicables.

- ***L'entreprise met en place une entité de type « Data factory ».***

Cette entité est chargée de la mise en œuvre et de la gestion du catalogue de données, de la standardisation des échanges de données et de la gestion des flux interapplicatifs. Elle travaille également sur les besoins en *analytics*.

- ***Les métiers sont accompagnés sur la gestion de la donnée et les risques afférents.***

Cette montée en compétence des métiers sur la gestion de la data peut être opérée par la DSI ou bien par le *Chief Data Officer*.

- ***L'entreprise met en place une politique autour de l'intelligence artificielle.***
  - Les cas d'usage de l'intelligence artificielle sont en cours d'identification ou déjà identifiés par l'entreprise.
  - Un travail de veille juridique et technologique dédié à l'intelligence artificielle est effectué.

6 ARCHITECTURE

Le vecteur Architecture connaît plusieurs évolutions ; l'architecture devient plus stratégique, s'harmonise et évolue avec l'adoption large du cloud.

Le sous-titre du vecteur, « Aligner l'architecture du SI avec les enjeux stratégiques », laissait déjà apparaître un lien entre architecture et stratégie. Ce lien s'est confirmé dans le temps : en effet, en tant que fournisseur de services, la DSI veille à assurer l'excellence opérationnelle de tous les services en place. Par ailleurs, le Guide recommandait la mise en place d'une « organisation […] pour assurer l'application du cadre de référence et piloter son évolution pour répondre aux besoins des projets et prendre en compte les évolutions technologiques ». Une évolution apparaît sur ce point : cette organisation prend la forme d'une autorité globale qui définit et actualise une politique architecturale et technologique qui doit permettre l'anticipation des évolutions business. Cette autorité actualise la politique architecturale de l'entreprise pour en faire un facteur d'accélération et de résilience.

Aussi, les travaux menés au Cigref sur la migration cloud révélaient que l'adoption massive du cloud impacte particulièrement le vecteur Architecture :

> **L'architecture du SI à l'ère du Cloud**
>
> La proposition de services cloud sur mesure facilite la prise en main, l'utilisation, et l'évolution des infrastructures ou des applications par l'utilisateur ainsi que l'adoption de solutions standards par le mode SaaS. L'architecture du SI devient alors plus flexible et résiliente et permet également de délivrer des services « agiles » (« *Business as a Service* »), et donc d'innover et de s'ouvrir plus facilement à l'écosystème des utilisateurs.
>
> **Extrait du rapport *Stratégies de migration dans le cloud*, 2023**

La simplification que permet le cloud a pour pendant l'obligation de construire une architecture résistante. L'objectif est que cette architecture soit suffisamment solide pour encadrer les usages mais suffisamment souple pour s'adapter au cloud.

6.1 LES NOUVELLES MENACES

- ***Perte de contrôle, dégradation de l'évolutivité et de la performance***

Cette menace n'est pas nouvelle, mais la démocratisation de l'accès au numérique et la multiplication des *citizen developers* accroit la menace tout en étant porteuse d'innovation. La principale difficulté est de rendre l'architecture plus systémique et d'encourager une pensée globale chez les acteurs de l'entreprise. Or, les *citizen developers* créent des applications sans avoir suffisamment de connaissances informatiques, ce qui pose des problèmes de gestion des données, de développement

de scripts, et inclut un risque de non-portabilité lors des migrations. Leurs initiatives peuvent ouvrir des frontières difficiles à maîtriser, augmentant le risque de fuite de données ainsi que les enjeux liés au *Shadow IT*.

De façon générale, une mauvaise maîtrise de l'architecture conduit à une faible évolutivité de la DSI, et donc par ricochet de l'entreprise, et créé des risques en matière de sécurité.

Pour autant, il est impossible d'interdire ces initiatives, d'autant qu'elles présentent des aspects très positifs sur différents plans : innovation, culture d'entreprise, engagement des métiers et amélioration des process d'idéation. Il faut donc que quelques bonnes pratiques encadrent ce champ en plein expansion.

6.2 LES NOUVELLES BONNES PRATIQUES

Une des solutions face au risque de perte du contrôle du SI est d'assurer la solidité des fondations et normes architecturales. Cela permet à la fois l'évolution des processus, l'accueil des nouvelles technologies et des initiatives innovantes. Une politique claire et connue permettra aussi d'encadrer les initiatives type *citizen developers*. Pour parvenir à établir de solides fondations et normes architecturales, la DSI et les Directions métiers doivent collaborer, en vue notamment de proposer une offre de services adaptée. Celle-ci doit prendre en compte les *inputs* des métiers, d'une part ; intégrer le risque cyber dans toutes les couches du SI et garantir l'interopérabilité des composants, d'autre part.

- ***Une politique architecturale globale est mise en place et est régulièrement actualisée en alignement avec la stratégie de l'organisation.***

Elle doit être validée au niveau Comex, partagée et appliquée dans l'ensemble des projets.

- ***Une entité est chargée de la gouvernance architecturale.***

Mise en place d'une « *design authority* » ou « autorité architecturale ».

- ***La politique architecturale est flexible et résiliente.***

Ces caractéristiques de flexibilité et de résilience sont indispensables dans un contexte de « cloudification » (cf encart *L'architecture SI à l'ère du cloud*).

- ***Les usages sont encadrés de façon à permettre l'innovation et la créativité tout en préservant la sécurité de l'entreprise.***

🔧 Une charte des bons usages est signée par chaque collaborateur de l'entreprise pour éviter toute dérive liée notamment au *low-code* ou au *shadow IT*.

7 SERVICES

Plusieurs facteurs conduisent la DSI à revoir la forme et le contenu de ses services et de son catalogue de services. Les contraintes économiques en font partie, bien qu'elles ne soient pas nouvelles en soi. En revanche, la démocratisation de l'accès au numérique, l'accélération des évolutions, les problématiques énergétiques, réglementaires et géopolitiques constituent des menaces nouvelles pour les services que propose la DSI et donc pour l'ensemble de l'organisation.

7.1 LES NOUVELLES MENACES

Tout d'abord, la démocratisation de l'accès au numérique et la richesse de l'offre externe obligent la DSI à repenser son catalogue de services et à le mettre à jour très fréquemment. Le cloud amplifie ce phénomène en accroissant la disponibilité de produits externes. Cela suppose un travail de qualification des technologies, de réflexion sur la façon de les mettre à disposition, sur leur usage et leurs droits d'usage, sur leur modèle économique et sur la refacturation au client interne.

Puis, les démarches en faveur d'un numérique responsable enjoignent la DSI à repenser certains pans de ses activités : optimisation des datacenters, réévaluation des besoins, augmentation de la durée de vie des produits et prévention des dégradations de service.

S'agissant du champ réglementaire et géopolitique, les entreprises implantées à l'international ont été sensibilisées aux risques juridiques et fiscaux encourus en cas de crise géopolitique (ex : sanctions internationales adoptées par l'Union européenne à l'encontre de la Russie, rupture d'approvisionnement stratégique…), ce qui là aussi représente un impact sur les services que propose la DSI. L'une des questions à ce titre est de savoir s'il est toujours pertinent de proposer un catalogue de services unique, ou bien s'il est préférable d'adapter le catalogue selon la filiale et sa situation géographique (et donc de l'adapter aux contraintes juridiques et réglementaires du pays concerné).

7.2 LES NOUVELLES BONNES PRATIQUES

- ***Anticipation de l'évolution des offres. La DSI amplifie sa veille et qualifie les nouveaux services/offres.***

La DSI sanctuarise des moyens de qualification des nouvelles offres notamment SaaS. Cela suppose d'être capable de mener une veille proactive sur les nouvelles offres disponibles, en devançant les demandes exprimées par les métiers. La qualification, qui s'effectue avec les *labs* dans la majorité des cas est une étape déterminante pour évaluer la pertinence d'une offre, et le cas échéant, l'ajouter au catalogue de services.

- ***La DSI augmente la fréquence d'enrichissement de son catalogue de services.***

Cette nouvelle bonne pratique doit permettre d'éviter le *sourcing* en direct de la part des métiers.

8 BUDGET & PERFORMANCE

Le vecteur Budget et performance est marqué par l'accélération de l'adoption de nouvelles technologies. En particulier, le développement du cloud fait évoluer l'entreprise, son mode de pilotage budgétaire et d'évaluation de la performance. Un projet de migration dans le cloud est coûteux et impose un changement de modèle du CAPEX vers l'OPEX. Cette évolution affecte la façon même dont la DSI présente ses budgets et les défend devant les instances décisionnaires de l'entreprise. De plus, le cloud conduit à une augmentation des coûts de RUN. Toutefois, la DSI ne peut grever son BUILD pour faire face à cette hausse du RUN, au risque de nuire à sa capacité d'innovation. C'est donc une recherche d'équilibre qui doit guider la DSI dans son pilotage budgétaire. En outre, le cloud et l'innovation en générale se mesurent via des critères traditionnels de performance, mais parfois aussi via de nouveaux critères que la DSI doit établir.

Lorsque la DSI fournit des services du SI en mode cloud (ou plus précisément en mode hybride) elle intègre souvent des service SaaS avec du patrimoine opéré en interne. Par conséquent, la DSI est obligée de repenser la performance et les SLAs convenus avec les clients internes (*i.e.* les métiers).

Une autre évolution notable est apportée par l'agilité et l'agilité à l'échelle, lesquelles remodèlent le pilotage économique du SI (cf. Modèle de pilotage des coûts de la DSI).

8.1 LES NOUVELLES MENACES

Les deux premières menaces relevées dans le Guide pour le vecteur « Budget et performance » restent les mêmes : « prendre de mauvaises décisions par manque de maîtrise de l'ensemble des éléments de coûts », « ne pas maîtriser les facteurs de dérapage des projets ». S'agissant de la troisième menace, qui s'est renforcée au cours des dernières années, « l'incompréhension entre les différentes directions de l'entreprise », le rapport du Cigref *Leviers de réduction des coûts de la DSI* propose désormais plusieurs outils pour y faire face. Là encore, la difficulté réside dans la rapidité avec laquelle surviennent les menaces aujourd'hui : les DSI doivent donc faire preuve d'une grande réactivité.

8.2 LES NOUVELLES BONNES PRATIQUES

- ***Les projets sont pilotés en fonction des coûts, délais, fonctionnalités et de la valeur.***

La notion de *valeur* s'ajoute aux critères préexistants. En effet l'agilité conduit l'entreprise à revoir la fréquence des évaluations de performance, pour tenir compte des incréments de valeur. L'évaluation de la performance devient « agile ».

- ***Adapter le capacity planning à l'hybridation du sourcing.***

Cette bonne pratique concerne en particulier la maîtrise et l'anticipation des évolutions de TCO. En effet, l'évolution des coûts des services achetés auprès de fournisseurs ne permet pas des prévisions à long terme.

- ***La stratégie de sourcing est adaptée aux évolutions des besoins RH.***

Les compétences requises à la DSI et le contexte de raréfaction des talents changent les priorités RH de l'entreprise. Cette question ne relève pas uniquement des ressources humaines, puisque les projets et donc la performance de l'entreprise sont affectés en cas de non réalisation d'un projet faute de ressources disponibles.

Ces bonnes pratiques sont complétées par les recommandations formulées dans plusieurs rapports récents du Cigref.[9]

[9] Notamment en matière d'agilité, de numérique responsable et de réduction des coûts IT, cf. Ressources.

9 MARKETING ET COMMUNICATION

Le vecteur Marketing et Communication vise à « valoriser les services et communiquer sur les enjeux technologiques en situation de crise ».

Ce volet de l'activité de la DSI se tourne davantage vers la confiance. Les métiers, la DSI et les utilisateurs sont de plus en plus dans une quête de sens vis-à-vis des services qui leur sont proposés et de leurs propres activités. Ce mouvement global s'observe au quotidien dans la vie de l'entreprise, tant pour attirer de nouveaux talents que pour offrir les garanties que lui demandent son écosystème.

Plus encore, le marketing et la communication doivent permettre de « rassurer » les utilisateurs et clients de la DSI et de l'entreprise, en s'engageant non seulement au respect de la réglementation (ex : données personnelles RGPD) mais aussi en prenant des initiatives.

9.1 LES NOUVELLES MENACES

Si la communication n'est pas suffisamment appréhendée, la menace encourue est la perte de confiance des utilisateurs et des clients du SI (« clients internes ») et clients de l'entreprise (« clients externes ») induite par l'évolution des risques cyber et par l'évolution des pratiques. Certaines nouvelles méthodes, telles que l'agilité à l'échelle, peuvent susciter de l'appréhension. À l'inverse, le cycle en V pouvait paraître plus sécurisant car il reposait sur un cahier des charges précis. Ces nouvelles méthodes nécessitent un grand effort de pédagogie : elles doivent être parfaitement comprises pour gagner et conserver la confiance.

Aussi, une mauvaise communication accroît la tension sur les ressources humaines et la difficulté à retenir les talents en raison de la « perte de sens » liée à leurs activités.

9.2 LES NOUVELLES BONNES PRATIQUES

- ***La DSI fait preuve de souplesse /adaptabilité dans la communication.***

La communication se doit d'être souple / adaptable, c'est-à-dire évolutive et repensée au fil de l'eau, selon les enjeux de l'entreprise et le contexte du moment.

- ***On rappelle le plus souvent possible la contribution d'une action ou d'un projet à la stratégie de l'organisation.***

La DSI, à travers ses missions, concourt directement aux objectifs globaux de l'organisation. Le rappeler est essentiel pour éviter « boîte noire » ou « tour d'ivoire » vis-à-vis des utilisateurs finaux, deux écueils qui figuraient déjà dans le Guide en 2019, au titre des menaces (Menace n°2).

- Favoriser la collaboration entre le responsable marketing et le responsable de la communication.

- ***La DSI porte une attention particulière à l'attractivité interne et externe.***

La quête de sens mentionnée précédemment, doit être prise en compte tant dans les manifestations extérieures de l'entreprise, que dans sa communication en interne.

- Cet effort passe par la construction de supports : à destination des futurs collaborateurs et des partenaires (attractivité externe), et à destination des collaborateurs pour retenir les talents (attractivité interne).

- ***La DSI propose l'animation de communauté au sein de l'entreprise.***

Cette recommandation complète et dépasse celles que le Guide proposait au travers de sa bonne pratique n°3 « la communication au sein de la DSI est organisée et régulière ».

- Création de guildes ou de communautés pour fédérer les équipes autour de projets communs et permettre la diffusion des bonnes pratiques.

- ***L'organisation veille à embarquer tous les acteurs concernés par les projets numériques.***

Cette bonne pratique permet d'éviter de laisser les métiers en retard dans la transformation numérique de l'entreprise.

- « REX interne » : la DSI produit un plan de communication et le présente aux métiers, qui sont ensuite chargés de le relayer.
- Création d'un rôle de *Business Relationship Manager* (BRM) ou d'un Responsable de la transformation numérique des métiers.

- ***La promotion des pratiques d'hygiène numérique (cybersécurité) est mise en place.***

La communication est loin d'être l'unique solution pour remédier aux risques cyber, mais elle est un des outils qui permettent de limiter la menace. Ex : recommander le changement de mot de passe régulier aux utilisateurs. (voir RISQUES)

- ***L'entreprise promeut le numérique responsable.***

Impliquant de nombreux changements des pratiques au sein des organisations, le numérique responsable doit s'appuyer sur un effort conséquent de communication, pour sensibiliser, acculturer et pousser à l'adoption des pratiques nouvelles induites.

- Organisation d'ateliers de sensibilisation, type « Fresque du Numérique » pour faire prendre conscience aux collaborateurs des enjeux liés à l'environnement.

CONCLUSION

À l'issue des travaux menés dans le cadre du GT Modélisation organisationnelle de la DSI, il apparaît que le Guide d'audit devra faire l'objet d'une actualisation plus exhaustive dans les prochaines années, en s'appuyant sur les autres activités du Cigref. Toutefois, nous avons jugé que les évolutions détectées méritaient plus d'instruction avant une telle mise à jour.

Ainsi, les travaux en cours sur l'évolution des fonctions « Ops » pourront nourrir la réflexion autour de la gouvernance du numérique et de la technologie. De même, les activités en matière de RSE et de RH, actuellement en cours, apporteront des éléments précieux et nécessaires à l'actualisation du Guide.

De plus, il faudra poursuivre l'analyse des vecteurs qui n'ont pas été étudiés cette année, à savoir les vecteurs « Projets », « RH », « Portefeuille projets », et « Prestataires & fournisseurs ».

Vers de nouveaux vecteurs d'audit ?

Les travaux menés invitent à envisager de nouveaux vecteurs d'audit, qui pourraient être intégrés au Guide dans sa prochaine version.

Premièrement, un vecteur « responsabilité sociétale de l'entreprise » pourrait apparaître. Le changement notable est que la dimension RSE n'est plus seulement un risque parmi d'autres. À ce stade, elle figure déjà dans plusieurs bonnes pratiques. À l'avenir, il faudra aborder la difficulté de concilier les ambitions de l'entreprise en matière de performance, de modes de travail (télétravail) avec ses objectifs de réduction de l'empreinte environnementale et énergétique. La RSE tend donc à s'affirmer comme une entité indépendante, auditable isolément.

Deuxièmement, l'inflation normative européenne et française renforce les exigences de conformité dont la DSI a à connaître. Si elle est bien souvent présentée comme une des facettes du vecteur Risques, il semble plus opportun de la considérer comme un « vecteur Conformité », ce qui implique donc une prise en charge globale allant de l'anticipation à la prise en compte de l'évolution normative et à sa mise en application concrète.

Troisièmement, on note que plusieurs facteurs, tels que la menace cyber croissante, ou la pandémie et la rupture qu'elle a entraînée dans les modes de travail, ont induit de nouvelles bonnes pratiques, visant à « être préparés » à une crise, de quelle que nature qu'elle soit. Ces éléments peuvent être distillés dans chacun des vecteurs existants, mais ils pourraient aussi être rassemblés au sein d'un vecteur Résilience.

Le quatrième et dernier point a trait à l'expansion de l'intelligence artificielle, à ce jour intégrée dans le vecteur Données, et qui pourrait à terme justifier de l'ajout d'un vecteur à part entière.

Conformité, RSE, Résilience, IA sont donc autant de champs à explorer non seulement en vue de la mise à jour du Guide, mais surtout, pour que les organisations soient pleinement actrices de leur transformation numérique.

RESSOURCES

Rapports Cigref sur des sujets connexes

Agile at scale : Pérenniser la transformation agile à l'échelle et la piloter, 2022

Leviers de réduction des coûts de la DSI, 2023

Modèle de pilotage économique et écologique de l'IT, 4ème édition, mise à jour 2022

Nouvelles pratiques de développement Low Code / No Code : Libérer la valeur en maîtrisant les risques, 2022

Politique RSE au sein de l'IT : Contributions positives de la DSI à la politique RSE de l'entreprise, 2022

Réagir à une cyberattaque massive, 2023

Stratégies de migration dans le cloud. Un défi structurant pour l'entreprise, *version 2023*

À PROPOS DU CIGREF

Au service de la croissance économique et de la compétitivité de nos membres, grandes entreprises et administrations publiques françaises, utilisatrices de solutions et services numériques, par la réussite du numérique.
Le Cigref est un réseau de grandes entreprises et administrations publiques françaises qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un acteur fédérateur de la société numérique. Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative.

Pour réussir sa mission, le Cigref s'appuie sur trois métiers, qui font sa singularité.

Appartenance
Le Cigref incarne une parole collective des grandes entreprises et administrations françaises autour du numérique. Ses membres partagent leurs expériences de l'utilisation des technologies au sein de groupes de travail afin de faire émerger les meilleures pratiques.

Intelligence
Le Cigref participe aux réflexions collectives sur les enjeux économiques et sociétaux des technologies de l'information. Fondé il y a près de 50 ans, étant l'une des plus anciennes associations numériques en France, il tire sa légitimité à la fois de son histoire et de sa maîtrise des sujets techniques, socle de compétences de savoir-faire, fondements du numérique.

Influence
Le Cigref fait connaître et respecter les intérêts légitimes de ses entreprises membres. Instance indépendante d'échange et de production entre praticiens et acteurs, Il est une référence reconnue par tout son écosystème.

NOUS CONTACTER

www.Cigref.fr
21 av. de Messine, 75008 Paris
+33 1 56 59 70 00
Cigref@Cigref.fr


Cigref
RÉUSSIR
LE NUMÉRIQUE