Executive Summary

Le grand défi 2024 des DSI Banque & Assurance face au nouveau cadre réglementaire

Croissance du Shadow SaaS/AI : quelle gouvernance pour concilier agilité business et cyber compliance (DORA) ?

Avec les propos recueillis de :

Olivier Colin
Corporate CIO

BNP PARIBAS CARDIF

Éric Ughetto-Couturier
CIO

BNP PARIBAS REAL ESTATE

Fabrice Thorinius
CISO group

covea

Florent Canonne - *CISO*
Dominique Duboc - *Deputy CIO*

STELLANTIS FINANCIAL SERVICES

Ce présent document est une synthèse des partages d'expériences de **Fabrice Thorinius**, CISO Group - Covéa, **Éric Ughetto-Couturier**, CIO - BNP Paribas RE, **Dominique Duboc**, DSI adjoint & **Florent Canonne**, RSSI - Stellantis Financial Services et **Olivier Colin**, CIO - BNP Paribas Cardif.
Lors de notre dernière table ronde du 18 octobre 2023, ils ont partagé leurs meilleures pratiques pour aborder les défis de conformité, de réduction des risques et de gouvernance IT liés aux SaaS, en particulier dans le contexte actuel de la réglementation DORA.

Ces dernières années, la source et la nature des risques liés aux incidents informatiques (cyberattaques et fuites de données) ont connu une augmentation significative et leur impact est de plus en plus important. L'essor fulgurant des logiciels en tant que service (Software-as-a-Service—SaaS) a joué un rôle majeur dans cette croissance, augmentant considérablement la surface d'exposition aux risques, surtout au sein des grandes entreprises.

Dans ce contexte, les gouvernements ont été poussés à réagir en imposant des réglementations strictes. L'objectif est de prévenir les risques cyber, la protection des données personnelles et de garantir la continuité d'activité.

Afin d'unifier et renforcer les différentes mesures en vigueur des pays membres de l'UE, le Parlement européen a adopté un règlement spécifique (DORA) au secteur financier. DORA n'est pas une mesure de plus, mais une consolidation de toutes les normes existantes (EBA, ACPR, NIS2..) sous forme d'une réglementation dont la mise en oeuvre est rendue obligatoire, à compter de janvier 2025.

Cette réglementation pousse les acteurs financiers à renforcer le pilotage des activités de sous-traitance et à systématiser l'évaluation des risques de sécurité associés à ces nouvelles solutions. En parallèle, les équipes IT sont face à un défi complexe : trouver l'équilibre entre la sécurité et la conformité du Système d'Information (SI) et le besoin d'autonomie et d'innovation des métiers.

L'objectif demeure d'établir une gouvernance IT claire et solide face aux risques associés aux SaaS.

50% des établissements bancaires les plus importants de la zone euro ont indiqué avoir été la cible d'au moins une cyberattaque réussie en 2021

Source : Banque centrale européenne, 2022

Décryptage de la réglementation DORA

Le règlement européen DORA (Digital Operational Resilience Act), adopté le 14 décembre 2022, entrera en vigueur le 17 janvier 2025. Son but est de renforcer la résilience opérationnelle numérique du secteur financier face aux risques croissants liés à la digitalisation et à la cybercriminalité. **Ce règlement est obligatoire** pour tous les établissements financiers, et vise à unifier, harmoniser et renforcer les réglementations nationales en vigueur des pays membres grâce à un cadre détaillé, et complet sur la gestion des risques liés aux technologies de l'information et de la communication (TIC) et à la sécurité des réseaux et des systèmes d'information au niveau de l'UE.

DORA impose aux établissements financiers européens de mettre en place une résilience constante et efficace face à toutes les évolutions du secteur (digitalisation, automatisation, SaaS, IA generative, etc.).

> **L'objectif est de passer d'une gestion des risques IT à une approche globale sur la résilience numérique.**

Pour répondre aux obligations édictées par la réglementation, les institutions financières et leurs tiers doivent mettre en place une série de mesures autour de leurs SI et des technologies utilisées, et les documenter.

Les 5 grands chapitres de DORA

Chapitre 2

Gestion des risques liés aux TIC

Chapitre 3

Gestion, classification & notification des incidents liés aux TIC

Chapitre 4

Test de résilience opérationnelle numérique

Chapitre 5

Gestion des risques liés aux prestataires tiers de services TIC

Chapitre 6

Dispositifs de partage d'informations

Durant le débat, nous nous sommes concentrés sur le chapitre 5 dont une des mesures est l'identification et la maîtrise des prestataires de services TIC. Ces derniers seront soumis à une supervision directe et renforcée des autorités européenne.

Dans cette perspective, les établissements financiers sont obligés de tenir un registre exhaustif de tous les prestataires tiers, y compris ceux jugés non-risqués afin pouvoir les déclarer proactivement, et à tout moment au régulateur. Ce registre doit également être industrialisé, via des processus pérennes en interne :

- Tenir un registre annuel et à jour répertoriant tous les prestataires TIC, incluant contrats, due diligences, audits et stratégies de sortie, en distinguant ceux qui couvrent des fonctions critiques des autres.
- Définir une stratégie en matière de risques liés aux prestataires tiers.
- Etablir un cadre de surveillance renforcé pour les prestataires critiques, incluant des dispositions contractuelles supplémentaires, des tests de performance et de pénétration, ainsi que l'identification précise de la chaîne de sous-traitance.

Ce pilier central "Gestion des risques liés aux fournisseurs tiers", rend donc obligatoire le recensement, la classification et la déclaration de tous les fournisseurs. En tant que fournisseurs de services tiers, les SaaS sont particulièrement concernés et devront faire l'objet d'un suivi et d'un référencement à l'échelle de l'entreprise.

> **Avec Dora, la pression s'accentue, il faut tout référencer, tout connaitre, tout déclarer.**

Il devient impératif pour les institutions financières d'agir maintenant et de mettre en place un plan d'action pour assurer la conformité à DORA d'ici 2025. C'est un défi particulièrement urgent pour les organismes financiers, car la plupart ne disposent pas d'une visibilité complète de leur parc IT et surtout des applications SaaS utilisées. L'ACPR a d'ailleurs mis en évidence la "gestion lacunaire du Shadow IT" au sein du secteur.

L'ACPR pointe « une gestion du Shadow IT toujours lacunaire »

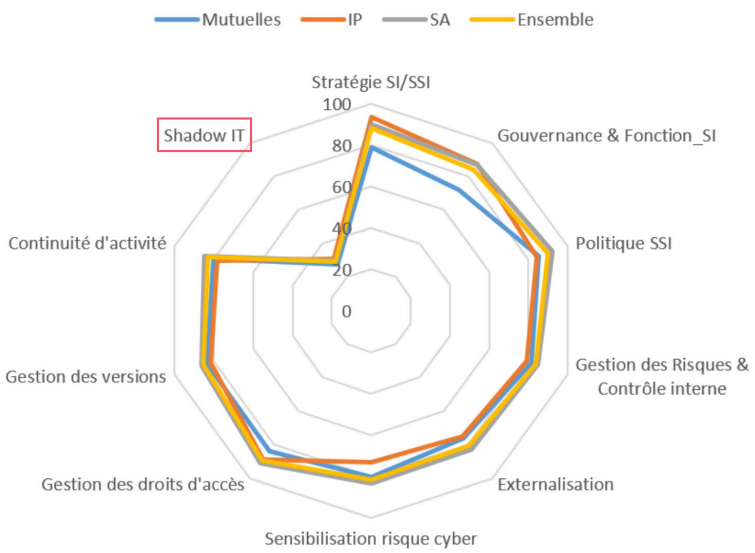
Le rapport de l'ACPR de 2022 sur la gestion de la sécurité des systèmes d'information des organismes d'assurance en France déplore que le référencement des outils non déclarés n'a pas progressé chez les assureurs depuis l'étude de 2019 (voir schéma page 5).

> **« Les risques relatifs aux "Shadow SaaS" applications non gérées par la DSI sont toujours aussi peu pris en compte (37 % des répondants seulement) dans la gestion des risques opérationnels » mentionne l'ACPR.**

Les assureurs doivent donc mettre en place rapidement des mesures pour se conformer aux obligations du règlement DORA.

ACPR BANQUE DE FRANCE La sécurité des SI des assureurs en France en 2022

Notation des principaux processus impliqués dans la gestion de la SSI



7. Une gestion du *Shadow IT* toujours lacunaire

Le *Shadow IT* recouvre les outils informatiques sous toutes leurs formes (appareils personnels, logiciels, applications, services web, programmes, …) qui sont développés, achetés ou utilisés par des utilisateurs appartenant à l'organisme d'assurance, sans que la direction des systèmes d'information en soit informée et donc sans supervision ni sécurisation de sa part.

La thématique « *Shadow IT* » a été abordée lors de la précédente enquête en 2019. Cette dernière a notamment révélé des lacunes dans la gestion des « EUC » (*End-User Computing* – programmes ou services non gérés par la DSI) qui représentent une des formes du *Shadow IT*. En 2022, le référencement des EUC n'a pas progressé par rapport à 2019 (22 % des organismes, de façon uniforme quelle que soit leur taille), ce qui, en dehors des aspects de supervision et de sécurisation mentionnés *supra*, est particulièrement dommageable en cas d'usage de « *Shadow SaaS*[13] », solution pouvant être contractualisée par un utilisateur sans qu'aucune analyse de risque ne soit effectuée par le RSSI. De la même façon, les risques relatifs aux applications non gérées par la DSI sont toujours aussi peu pris en compte (37 % des répondants seulement) dans la gestion des risques opérationnels.

La croissance du SaaS/AI bouleverse le SI : il est plus que jamais nécessaire de mettre un plan d'action

S'attaquer au Shadow IT n'est donc plus une option, mais un impératif pour les équipes IT. La DSI doit mettre en place une politique plus souple et agile pour référencer toutes les applications présentes au sein de l'organisation, en favorisant une collaboration renforcée avec les différentes entités métiers. Il est crucial de détenir et maintenir une liste structurée, organisée et continue de tous les fournisseurs. En parallèle, il est nécessaire de réguler l'adoption de nouveaux outils dès leur apparition, afin de prévenir le recours aux solutions en Shadow. La mise en place d'un cadre de gouvernance devient alors l'une des principales priorités pour permettre aux métiers de continuer à innover tout en préservant la sécurité du SI et la conformité vis-à-vis des différentes régulations.

Gouvernance IT : trouver la bonne balance entre innovation, agilité et sécurité des actifs ?

Les métiers sont, plus que jamais, en quête d'agilité et d'innovation pour rester compétitifs dans un environnement en perpétuelle évolution. Les solutions SaaS se distinguent comme des atouts indispensables de performance, grâce à leur disponibilité, leur diversité et leur facilité d'implémentation sur le marché. Toutefois, cela engendre d'importants défis en matière de sécurité et de conformité, du fait du volume de données que ces solutions peuvent intégrer et traiter.

Malgré ces risques, de nombreux employés ont tendance à contourner les processus IT établis, les jugeant trop longs, complexes et fastidieux.

> **Il est compréhensible qu'un métier ne souhaite pas attendre quatre mois pour conclure un contrat avec une solution SaaS, notamment si celle-ci ne contient aucune donnée personnelle.**

Cette digitalisation des métiers est une tendance qui n'est pas prête de s'arrêter ; au contraire celle-ci ne fait que s'accélérer, notamment avec l'émergence de solutions basées sur l'intelligence artificielle générative (IA gen). Pour en savoir plus sur les risques associés au Shadow IT/AI, cliquez ici.

75% des SaaS ne sont pas gérés par l'IT.

Source : échantillon de 40 clients Beamy +1000 employés

Il incombe donc à la DSI de revoir sa stratégie pour remplir pleinement son rôle fondamental : répondre aux besoins de ses clients - ici ses clients internes : les métiers. Il ne s'agit plus de se cantonner à la gestion des infrastructures IT classiques et traditionnelles, mais de viser bien plus que le simple pilotage de l' "IT core". L'objectif est d'accompagner les différents départements métiers vers l'autonomie tout en maintenant une maîtrise du Système d'Information.
Cela passe d'abord par une meilleure compréhension des enjeux et besoins métiers pour anticiper l'adoption technologique et limiter le Shadow IT. Cela implique **la formation des métiers aux enjeux de la 'New Tech'** (SaaS, IA, Low-code/No-code...) **et la sensibilisation aux risques associés** (RGPD, cyber, opérationnel, et continuité...).

Mettre en place la bonne gouvernance IT

Il devient donc impératif de redéfinir la gouvernance des applications SaaS afin de favoriser l'innovation tout en garantissant un niveau de sécurité robuste.

La première étape consiste à établir une distinction claire entre les SaaS critiques intégrés au SI et traitant des données sensibles, et ceux moins critiques, non connectés au SI et ne manipulant peu/pas de données personnelles. Ainsi, la DSI devra revoir ses processus et son rôle : être impliquée de manière significative dans le déploiement des solutions dites critiques, et en tant que consultante pour les applications moins sensibles, laissant ainsi aux métiers la liberté d'utiliser le SaaS de leur choix.

Cette première phase de gouvernance permettra à la DSI de passer d'une approche binaire où l'autonomie et l'agilité des métiers semblent s'opposer à la protection du SI, à une approche vertueuse où agilité et protection se complètent mutuellement. Toutefois, cela ne sera possible qu'avec une collaboration renforcée entre les équipes IT et les métiers de l'entreprise.

Cette relation renforcée et ces processus simplifiés offriront une vision globale du parc IT, stimulant ainsi l'innovation au sein de l'entreprise. De plus, cela contribuera à maintenir la compétitivité, tout en atténuant les risques liés aux attaques et aux fuites de données, des enjeux cruciaux dans l'environnement actuel.

Dans une seconde phase, la DSI pourra évoluer vers le rôle de fournisseur et de concentrateur de solutions SaaS pour les différents métiers. Cette transition

repose sur la volonté d'adopter un catalogue de solutions SaaS, permettant aux métiers d'accéder aisément aux solutions approuvées par l'IT via un portail d'applications d'entreprise, tout en imposant des conditions et des règles spécifiques pour atténuer les risques.

Pour parvenir à cette autonomie, il est crucial d'établir un référentiel de solutions SaaS à jour et d'avoir un contrôle effectif sur le parc applicatif, avec une gouvernance clairement définie.

La DSI doit rester au cœur de cette transformation, en étant à la fois le moteur de l'innovation et gardienne des bonnes pratiques.

Conclusion

La résilience de l'entreprise et la résistance de son SI deviennent des enjeux stratégiques majeurs, qui nécessitent l'implication immédiate du comité de direction, sous la responsabilité du DSI. Ce dernier vise à être au cœur de la technologie, en adoptant une approche à la fois rigoureuse et pragmatique pour favoriser l'innovation tout en garantissant la sécurité. À ce titre, il doit être capable d'établir un cadre de communication exhaustif et industriel pour gérer efficacement tous les prestataires de services TIC.

Cette transformation vise à établir la DSI en tant que concentrateur de SaaS et partenaire des métiers, favorisant une collaboration étroite et proactive pour une digitalisation efficace. Dès lors, il est crucial de se préparer en amont pour répondre aux exigences imposées au secteur financier prévues pour janvier 2025.

Rejoignez notre communauté de leaders IT pour relever les enjeux liés au SaaS

Beamy organise régulièrement des événements (tables rondes, networking, webinars) **autour de sujets stratégiques liés aux SaaS et aux défis qu'ils impliquent pour les grandes entreprises.** Pour plus d'infos sur nos prochains évènements, contactez-nous »

beamy.io