Projets et Cybersécurité

-

« Ecosystème et Gouvernance de la Sécurité de l'Information »

Un Livre Blanc du Cercle des Entreprises du PMI®

Une initiative du chapitre **PMI-France**

Avec la collaboration du **Clusif**

Project Management Institute. France	CLUSIF
Date de publication : Septembre 2025	Version : Finale

Avertissement

Ce livre blanc est le fruit des échanges et des contributions de professionnels sur un certain nombre de bonnes pratiques liées aux projets de transition énergétique, basées sur leur expérience. En aucun cas il n'a la prétention de couvrir l'exhaustivité des sujets ou des types de projet, pas plus qu'il ne représente la position officielle des entreprises des contributeurs.

Table des matières

Table des figures

1 Executive Summary

Ce Livre Blanc de PMI-France, écrit en collaboration avec le Clusif, explore les liens entre Gestion de Projet et Sécurité de l'Information. Il aborde comment la sécurité et la protection de la donnée doivent être pensées en amont du projet et en quoi une bonne approche de gestion de projet favorise la mise en place d'une cybersécurité pertinente et efficace au sein de votre organisation.

En effet, la Cybersécurité est devenue ces dernières années une préoccupation majeure des organisations de toutes tailles. Omniprésent, le numérique a pris une dimension fondamentale dans la société et stratégique dans nos organisations.

Les risques numériques engendrent d'autres menaces, bien souvent elles-mêmes à l'origine de nouveaux risques. Il est essentiel que le Comité Exécutif de chaque entreprise en tienne compte au même titre que les autres problématiques auxquelles l'organisation doit faire face.

Toutes les organisations doivent pleinement mesurer ce changement de paradigme ainsi que les niveaux de responsabilité et d'implication attendus. Cette exposition, aux conséquences très graves et aux impacts imprévisibles, est dans une large mesure imputable à la gouvernance. Cette gouvernance, en charge de l'organisation, de la stratégie, de l'arbitrage des moyens et des priorités, ne s'est pas encore systématiquement saisie de cette nouvelle dimension du risque, qu'elle perçoit encore trop souvent avec un **biais cognitif persistant** : le prisme technique.

« Security is a process, not a product » explique Bruce Scheiner[1], chercheur en cryptologie. Bref, à nous de prendre nos propres responsabilités, sans nous tourner vers les marchands du temple.

Les directions métiers, les donneurs d'ordres, les maîtrises d'ouvrage se doivent d'exprimer leurs besoins métiers de sécurité afin de pouvoir y répondre d'un point de vue organisationnel et technique dans les projets numériques présents et à venir.

C'est pour cette raison que PMI-France a décidé de lancer une série de Livres Blancs autour du thème « Projets et Cybersécurité ». Ils traitent naturellement de l'intégration de la sécurité dans les projets en se focalisant sur les points suivants :

- L'écosystème de la Cybersécurité que doit **absolument connaître** le Chef de Projet ;
- La gouvernance qui porte la **responsabilité des risques numériques** et des moyens pour y répondre ;
- Les directions Métiers qui identifient les risques à travers une démarche d'**intégration de la sécurité** dans les projets ;
- les experts techniques avec une **vision transversale du risque** « technique-métier-sectoriel ».

Ce périmètre est très vaste et nous avons fait le choix de nous concentrer dans ce premier ouvrage sur **l'écosystème et la gouvernance de la Sécurité de l'Information**.

Une fois ce socle posé, nous aborderons les autres points dans les Livres Blancs ultérieurs.

Cet ouvrage prône la rencontre effective entre deux populations qui, trop souvent, se connaissent mal, les acteurs des Projets d'une part et les acteurs de la Sécurité de l'Information d'autre part.

Après avoir posé des définitions clés, nous présenterons en détail, le contexte actuel, les enjeux et surtout l'écosystème - les normes et les référentiels – de la sécurité de l'information français, européen et international.

Par la suite, nous passerons en revue la gouvernance nécessaire à la bonne intégration de la sécurité dans les projets. Ainsi, la direction de l'entreprise doit se saisir de la sécurité, la porter et l'imposer sans oublier de vérifier que les objectifs en matière de sécurité sont bien atteints et répondent aux besoins.

[1]The Process of Security (Schneier, 2000)

2 Présentation générale de ce Livre Blanc

2.1 Pourquoi un Livre Blanc sur Projets et Cybersecurite ?

La cybersécurité s'impose à tous et à toutes les organisations et elle se déploie partout, naturellement de manière spécifique à chaque organisation :

- Elle se déploie à tous les niveaux et toutes les activités de l'entreprise, de façon adaptée à son contexte ;
- Elle entraîne de profondes transformations dans les entreprises, en particulier par son approche globale et transversale.

En revanche elle n'a, pour l'instant, pas réellement été étudiée sous l'aspect de la gestion de projet.

L'objectif de ce Livre Blanc est donc de présenter l'impact de la cybersécurité sur la transformation des entreprises et en particulier sur leur manière de mener à bien leurs différents projets, afin d'identifier des bonnes pratiques de management de projet permettant de remplir ses obligations en matière de cybersécurité.

En revanche ce premier Livre Blanc n'est pas destiné à traiter **en profondeur un point spécifique** de la cybersécurité.

2.2 Les destinataires de ce Livre Blanc

2.2.1 Les acteurs projets

Le PMI-France est à la pointe du management de projet et a vocation à animer la communauté des chefs de projets dont les membres du PMI® et naturellement les certifiés PMP® et autres certifications du PMI®.

Cette population est naturellement sensibilisée ou formée aux bonnes pratiques de gestion de projet. En revanche, elle n'est pas nécessairement au fait des enjeux, des contraintes et des impacts de la sécurité des systèmes d'information et plus globalement de la cybersécurité.

En conséquence, la cible principale de ce Livre Blanc est **le chef ou directeur de projet**, ou encore **les responsables de programme** ou de **portefeuille**. En effet, à travers ce Livre Blanc, nous souhaitons permettre à ces porteurs de projet d'acquérir le **socle de base minimal en matière de sécurité des systèmes d'information**, ainsi que son écosystème spécifique de cybersécurité, afin d'être capable de mener avec succès des projets en intégrant la sécurité de l'information dans toutes ses phases.

Ce guide sera par ailleurs utile pour **tous les acteurs** du système d'information au sens large : la DSI, la gouvernance, la cellule de crise, la direction qualité, la/le Data Protection Officer (DPO), la/le Responsable de la Sécurité des Systèmes d'Information (RSSI) / Conseiller à la Sécurité Numérique (CSN), la direction/responsable intelligence économique, les directions (métiers, financières, RH, juridique et SI), la sous-traitance, les fournisseurs, les partenaires, ...

2.2.2 Les acteurs de la cybersécurité

Dans le même temps, il nous parait également essentiel d'intégrer à ce Livre Blanc les acteurs systémiques de la cybersécurité : Directeur cybersécurité, RSSI/CSN, DPO, les fournisseurs de solutions, les hébergeurs, les autorités (l'ANSSI, la CNIL, l'ENISA ou European Union Agency for Cybersecurity etc…).

Ceci afin de pouvoir présenter l'articulation entre intégration de la cybersécurité et gestion de projet, mais également des acteurs plus éloignés du sujets. Ces acteurs sont par exemple :

- Les directions de l'entreprise (générale, juridique, RH, achats, des directions non spécialistes de la sécurité informatique) ;
- Les experts techniques de la cybersécurité.

Tous ces acteurs peuvent s'appuyer sur son contenu comme un levier culturel de départ et un langage commun dans l'organisation, pour faire avancer leurs propres chantiers.

2.3 DEFINITIONS : SURETE, SECURITE ET CYBERSECURITE

2.3.1 Sûreté

Selon le Larousse, la sûreté :

- Est l'état de quelqu'un ou de quelque chose qui est à l'abri, n'a rien à craindre : par exemple, prendre des précautions pour sa sûreté ;
- Est un caractère précis, efficace de quelqu'un ou de quelque chose, sur lequel on peut compter de façon certaine : par exemple, mémoire d'une sûreté absolue ;
- Est un dispositif de protection : il a mis deux sûretés à sa porte, un verrou et une chaîne.

2.3.2 Qu'est-ce que la sécurité

La sécurité en entreprise est l'ensemble des mesures, procédures et moyens visant à **protéger les actifs matériels et humains de l'organisation** contre toute forme de menace, qu'elle soit **physique, organisationnelle, humaine ou technologique**.

Exemples de domaines couverts :

- Sécurité physique des bâtiments (accès, vidéosurveillance, contrôle d'entrée, badges) ;
- Protection du personnel (plan de sécurité, gestion de crise, sûreté des collaborateurs) ;
- Prévention des actes de malveillance (vols, intrusions, sabotage, espionnage industriel) ;
- Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA) ;
- Gestion des incidents non numériques (incendie, panne électrique, catastrophe naturelle, …).

Normes associées :

ISO 22301 (PCA), ISO 45001 (santé/sécurité au travail)

La sécurité des systèmes d'information (SSI) [2] : « Ensemble des moyens techniques et non-techniques de protection permettant à un système d'information d'assurer la Disponibilité, l'Intégrité et la Confidentialité des données, traitées ou transmises, et des services connexes que ces systèmes offrent ou rendent accessibles. »

[2] CyberDico (ANSSI)

Exemples de domaines couverts :

- Protection contre les cyberattaques (phishing, ransomware, DDoS…) ;
- Sécurisation des réseaux, systèmes, applications, cloud, endpoints ;
- Chiffrement, authentification, gestion des identités et des accès ;
- Gouvernance de la sécurité de l'information (ISO/IEC 27001) ;
- Conformité réglementaire (RGPD, NIS2, DORA, IA Act…).

2.3.3 Notre définition de la Cybersécurité

Cybersécurité[3] :
Niveau de maturité organisationnelle, humaine, physique et technologique recherché pour permettre à un système d'information de résister à des événements malveillants (externe/interne) ou accidentels issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises, ainsi que des services associés.

La cybersécurité mobilise des **techniques issues de la sécurité des systèmes d'information**, contribue à la **lutte contre la cybercriminalité**, et s'exerce dans le **cyberespace** — c'est-à-dire l'espace numérique constitué de réseaux interconnectés, dans lequel circulent les données et s'exécutent les services numériques.

Elle n'est pas fondée sur la cyberdéfense, mais la précède dans l'échelle d'intensité des réponses : la cyberdéfense intervient en complément dans des contextes critiques, stratégiques ou souverains, notamment face à des menaces étatiques ou de haute intensité.

Enfin, la cybersécurité s'étend également à la protection de certains **actifs immatériels** dans l'environnement numérique, tels que **les idées, la propriété intellectuelle**, ou les modèles sensibles des organisations.

Une façon de gérer le développement et la maturité de cette cybersécurité[4] est présentée ci-dessous :

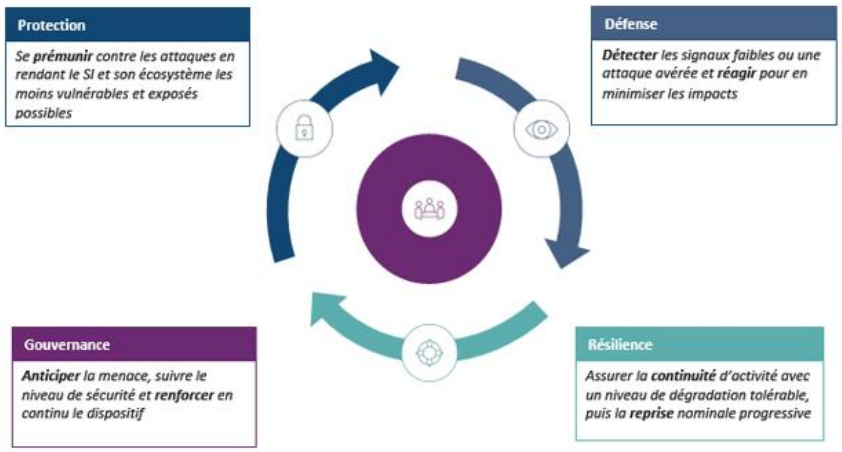


Figure 1- Structurer ses mesures de sécurité (ANSSI)

[3] CyberDico (ANSSI)
[4] Cybersécurité : des pistes pour la protection des entreprises (Ministère de l'économie et des finances, s.d.)

2.3.4 Qu'est-ce que le Risque Cyber

Le risque cyber[5] représente le risque lié à l'usage des technologies numériques, et défini comme un impact opérationnel potentiel portant sur 4 (parfois 5 selon les sources) critères de sécurité : la confidentialité, l'intégrité, la disponibilité, la traçabilité et parfois l'identité des données et des systèmes d'informations.

En 2025, **la grande majorité des sinistres cyber** (incidents ayant un impact financier ou opérationnel pour les organisations) sont **liés à des cyberattaques**, et cette tendance est **en forte hausse depuis 2019**.

2.3.5 Cyberdéfense et Cyber espace

D'après l'ANSSI, la cyberdéfense[6] est « l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.»
Le cyberespace est « l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numériques. »

2.4 LES SUJETS ABORDES DANS CE PREMIER LIVRE BLANC

Ce livre blanc va traiter des points suivants :

- L'**écosystème** de la **Cybersécurité** au sens large, y compris le contexte, le cadre réglementaire ainsi que les enjeux de la Cybersécurité ;
- La **gouvernance de l'entreprise**, en particulier sur la partie Cybersécurité, qui doit porter la **responsabilité des risques numériques.**

Dans un second temps, nous aborderons dans les prochains Livres Blancs :

- Comment les directions Métiers identifient les risques par une démarche d'**intégration de la sécurité** dans les projets ;
- Comment les équipes d'experts en analyse de risque (EBIOS, …) qualifient les risques avec une **vision transversale** "technique-métier-sectoriel ».

[5] CyberDico (ANSSI)
[6] CyberDico (ANSSI)

3 Contexte de la cybersécurité

3.1 CONTEXTE GLOBAL

Traiter de la Cybersécurité réclame tout d'abord un constat : le monde est de plus en plus connecté et les risques s'intensifient, d'une part du fait de cette multiplication des interfaces, mais aussi en raison de la sophistication croissante des menaces.

Cet exposé décrira le jeu mondial des influences et attractions d'un nouvel ordre politique, tout comme l'apparition de nouvelles technologies.

Face aux risques qu'entraîne ce nouvel ordre, des solutions de plusieurs natures existent et commencent à se déployer, avec la considération fondamentale que le facteur humain reste toujours le maillon faible.

Aussi l'enjeu majeur est de mettre en place une organisation adaptée, agile et efficace pour accompagner le changement et l'amélioration des pratiques.

3.1.1 Quelques chiffres

Allianz Risk Barometer 2025 [7] :

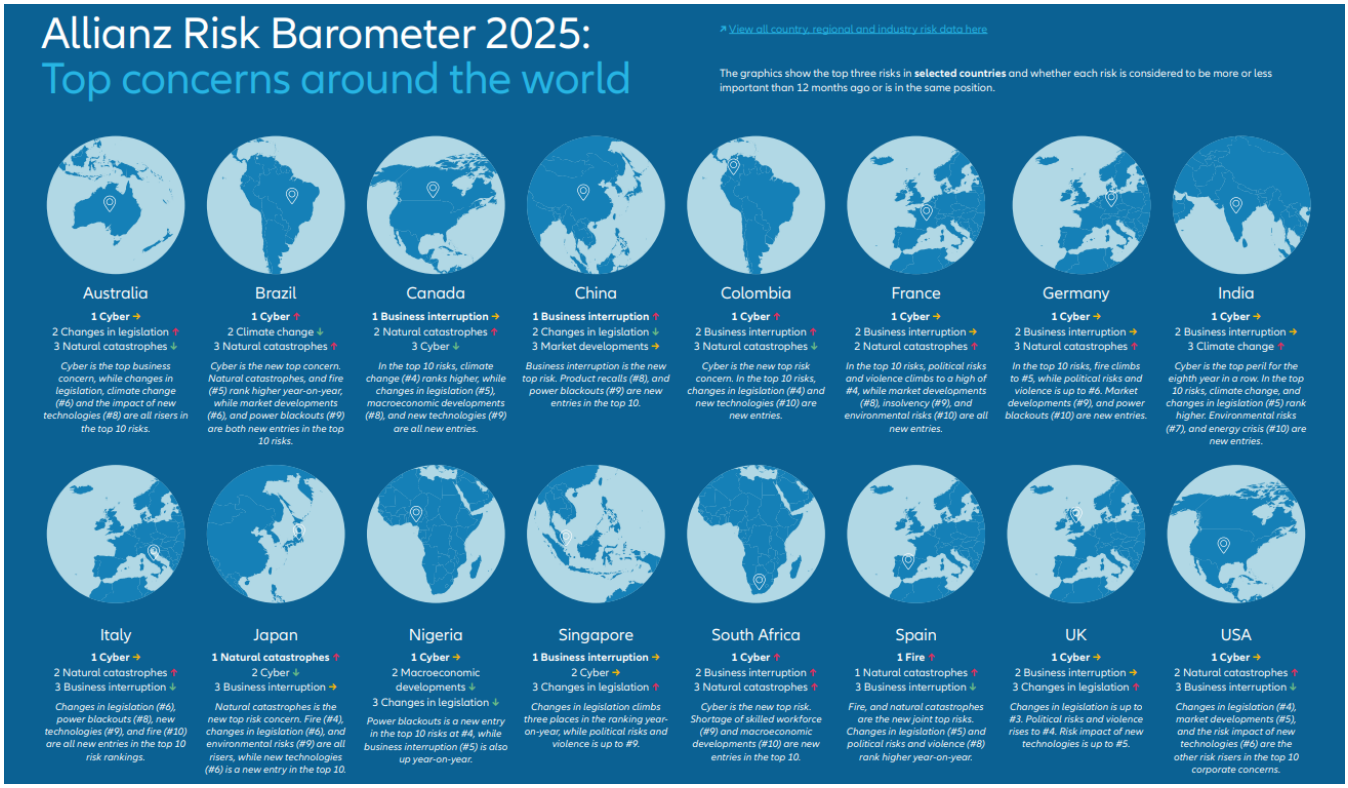


Figure 2- Cyber parmi les principaux risques (Allianz)

Cette image peut être récupérée sur le lien :
https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

Le risque le plus important que chaque pays remonte, apparaît sous le nom du pays. Sur 16 pays, 11 considèrent le risque Cyber comme le plus important.

[7] Baromètre Allianz sur les risques (Allianz, 2025)

Principaux risques pour les entreprises en 2025, en France

Classement		Pourcentage	Classement 2024	Tendance
1	Incidents cyber *(ex : cyber crimes, interruptions de service et réseau IT, logiciels malveillants/ransomware, violation de données, amendes et sanctions)*	44%	*1 (44%)*	→
2	Interruptions d'activités *(y compris les perturbations de la chaîne logistique)*	31%	*2 (40%)*	→
2	Catastrophes naturelles *(ex : tempête, inondation, tremblement de terre, feu de forêt, événements climatiques extrêmes)*	31%	*5 (22%)*	↑
4	Risques politiques *(ex : instabilité politique, guerre, terrorisme, coup d'état, conflits sociaux, grèves, émeutes, pillages)*	27%	*6 (21%)*	↑
5	Incendie, explosion	22%	*3 (25%)*	↓
6	Changement climatique *(ex : risques physiques, opérationnels et financiers résultant du réchauffement climatique)*	18%	*4 (23%)*	↓
7	Évolutions législatives et réglementaires *(ex : nouvelles directives, protectionnisme, les exigences RSE et en matière de durabilité)*	16%	*7 (16%)*	→
8	Évolutions de marché *(ex : concurrence accrue/nouveaux entrants, fusions/acquisitions, stagnation ou fluctuation de marchés)*	12%	NOUVEAU	↑
9	Insolvabilité	11%	NOUVEAU	↑
10	Risques environnementaux *(ex : pollution, enjeux liés à la biodiversité, pénurie)*	10%	NOUVEAU	↑

Figure 3 - Le Top10 des risques en France (Allianz)

L'évolution des cyberattaques reflète une sophistication croissante des techniques utilisées par les attaquants, par exemple des rançongiciels (logiciels malveillants pouvant bloquer tout ou partie du système d'information et réclamant une rançon) toujours plus ciblés, grâce à des campagnes complexes d'ingénierie sociale[8].

Ces menaces, de plus en plus fréquentes et diversifiées, obligent les organisations à s'adapter en permanence. La rapidité d'innovation des cybercriminels oblige à repenser tout aussi vite les stratégies de défense, en s'appuyant sur différents moteurs d'innovation, tels que l'IA.

3.1.2 Contexte géopolitique

Le cyberespace est une création de l'homme et est devenu l'extension de notre société qui inclut nos réalités politiques, économiques, culturelles... Si nous devions en donner une définition simple, il s'agit de l'ensemble des infrastructures numériques et des données mis en réseaux, que l'on va communément apparenter à l'Internet.

La **Loi de Programmation Militaire** 2024-2030 publiée en avril 2024 continue de reconnaitre le **cyber** comme un champ de conflictualité au même niveau que les champs traditionnels (terre, mer, air et espace). Elle prévoit ainsi un budget de **4 milliards d'euros** (contre **1,6 milliards** pour la LPM 2019-2025) autour de trois axes d'effort : la cyber protection, la lutte informatique défensive et la diversification des moyens d'action. Cette dernière vise à augmenter les efforts d'investissement en matière d'Intelligence Artificielle (IA), de lutte informatique offensive et de lutte informationnelle et d'influence. L'effort du gouvernement français en matière d'investissement en cyber est notable, mais reste à relativiser alors même que le budget américain pour l'année 2025 en matière de cyber s'élève à **13 milliards de dollars**.

[8] Voir en glossaire la signification de l'ingénierie sociale

Le cyber devient alors une priorité stratégique pour toute organisation :

Au niveau national : afin de répondre aux cybermenaces, les Etats vont militariser les structures numériques en redéfinissant leur stratégie de défense. Dès 2011, les Etats-Unis publient leur stratégie internationale pour le cyberespace. Deux ans plus tard, la France va mettre à jour son Livre Blanc sur la Défense et la Sécurité National et fait entrer la cyberdéfense au même titre que la dissuasion nucléaire au rang des priorités nationales. L'augmentation des attaques envers les états et le tissu économique nécessitent un renforcement de la sécurité des systèmes d'information d'importance vitale.

Au niveau de l'Union Européenne : à partir de 2020, elle présente sa stratégie pour la cybersécurité dans l'objectif de renforcer la résilience européenne face aux cybermenaces. Les directives en matière de sécurité des systèmes d'information visent à établir des obligations en matière de sécurité pour opérateurs de services essentiels (énergie, transport, santé...). La définition d'un cadre réglementaire commun européen ainsi que la promotion d'une coopération entre les états membres s'inscrivent dans la volonté d'une autonomie stratégique en matière de cybersécurité.

Dans le secteur privé : une récente étude de la société Ivanti interroge plus de 7 000 dirigeants et professionnels de la cybersécurité. Dans son rapport, **91% disent que la cybersécurité est considérée comme une question stratégique majeure dans leur entreprise**. L'attention donnée à la sécurité des entreprises répond au fait que le risque cyber n'est pas uniquement un risque technologique mais également un risque majeur qui pourrait avoir des impacts organisationnels, juridiques, règlementaires, et financiers. C'est pourquoi la cybersécurité n'est plus ignorée des agendas des conseils d'administration.

3.1.3 Contexte technologique en constante évolution

L'évolution des nouvelles technologies profitera à tous, y compris aux cybercriminels. Elle est autant porteuse d'opportunités (travail hybride, l'approche Zero Trust ou encore les services liés au Cloud) que de défis pour les organisations. Il est important de mettre en lumière qu'une rupture technologique signifie également une non-sécurisation des systèmes et une incapacité à résister à des attaques toujours plus sophistiquées au plan organisationnel, physique, humain et technologique. C'est pourquoi il est important de favoriser les investissements dans ces domaines pour suffisamment rester à jour dans la protection dynamique des SI.

Quelles sont les nouvelles technologies qui façonneront la sécurité de demain ?

Chaque nouvelle technologie apporte son lot de nouvelles menaces. Simultanément, il est à noter que ces technologies émergentes auront également un impact sur le marché du travail et l'éducation. Elles orienteront les politiques en matière d'éducation à la cybersécurité, de formation, de parcours de carrière, d'apprentissages et de reconversion professionnelle.

Une complexification technologique porteuse de solutions mais également de risques nouveaux.

3.1.4 Risques induits pour les organisations

La cybersécurité désigne l'ensemble des mesures techniques, humaines et organisationnelles visant à protéger les systèmes d'information, les réseaux — qu'ils soient connectés ou non à Internet —, ainsi que les données qu'ils traitent, contre les menaces issues du cyberespace. Elle va au-delà de la seule sécurité informatique (notion plus ancienne et centrée sur les systèmes internes) en intégrant la gestion des risques numériques, la conformité réglementaire, la protection de la vie privée et la résilience face aux cyberattaques. La cybersécurité ne se limite pas aux réseaux connectés à Internet. Elle englobe aussi les réseaux privés, les systèmes industriels (OT/ICS), les équipements non connectés en permanence, etc.

Par nature ces environnements plus ou moins accessibles depuis Internet peuvent être vulnérables et donc victimes de cyber-attaques qui utilisent ces vulnérabilités organisationnelles, physiques, humaines ou technologiques. Dans un monde de plus en plus connecté, le risque d'attaque est exponentiel, les sources de menace sont protéiformes et les impacts sur les infrastructures, les données et les individus augmentent en conséquence.

Le **risque cyber** devient alors un **risque global** car il est au cœur de toutes les activités humaines devenues dépendantes des technologies de l'information et de communication. Il touche autant le secteur privé que le secteur public. La professionnalisation de la cybercriminalité et l'évolution des technologies complexifient la maîtrise et la protection des systèmes d'information.

Néanmoins, voici une liste non exhaustive des risques cyber, caractérisé soit par des menaces, soit par les impacts engendrés :

- Menaces : espionnage industriel et économique, atteinte à la propriété intellectuelle, attaques concurrentielles, attaques sémantiques ;
- Impacts : atteinte à l'image, incapacité à produire, infection des ressources informatiques, non-conformité aux lois et aux réglementations...

Dans son dernier Panorama de la cybermenace en 2023 l'ANSSI relève **3 modes d'action des récentes attaques marquées par de fortes tensions géopolitiques** : **l'espionnage** (augmentation du ciblage sur des individus ou structures traitant des données sensibles), **l'extorsion** (augmentation de 30% des attaques par rançongiciel) **et la désinformation** (recrudescence des opérations de déstabilisation visant à promouvoir un discours politique ou porter atteinte à l'image d'une organisation). Le sabotage peut également provenir d'acteurs internes (vengeance d'un salarié licencié ou d'un prestataire non reconduit dans son contrat de maintenance ou d'administration informatique, par exemple).

Afin de réduire le risque cyber, il est donc primordial de prendre en compte la sécurité dès la phase de conception des systèmes, donc notamment dès l'initialisation des projets, en plus de continuer à mettre en place des politiques, procédures, modes opératoires et technologies adaptés à l'évolution des technologies et des menaces. Le maintien en condition opérationnelle de la sécurité de l'information et des systèmes (réseaux inclus) est donc une condition *sine qua non* d'une organisation résiliente face aux menaces cyber.

Ce sujet sera présenté au §5.4, avant d'être détaillé dans un futur Livre Blanc.

3.2 CADRE REGLEMENTAIRE EN 2024

3.2.1 Européen : plusieurs réglementations

L'Union Européenne a pris les devants en encadrant l'usage du numérique et des données [9] :

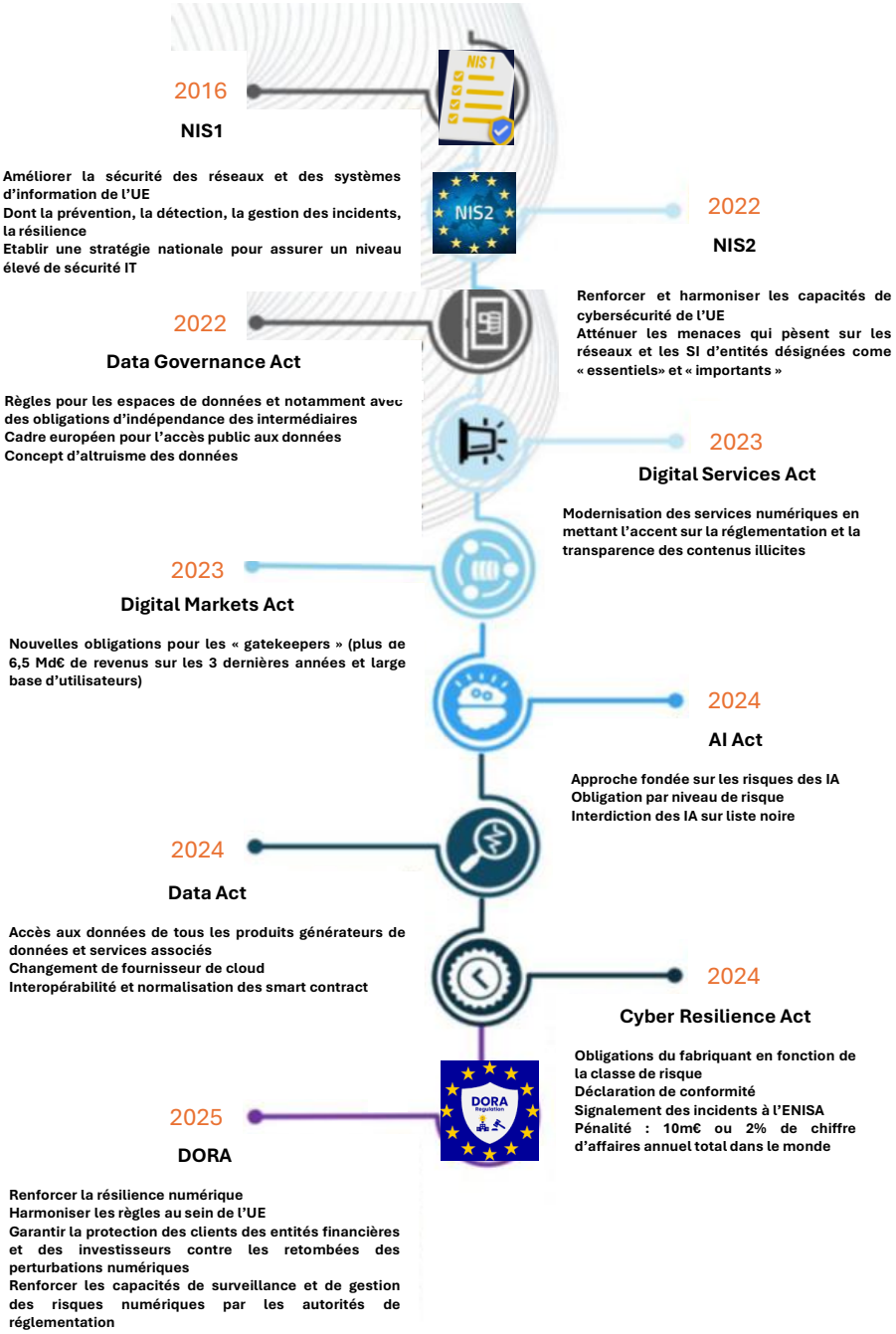


Figure 4 - Législation sur le numérique dans l'UE (non-exhaustif)

[9] Selon forum-des-competences.org (cybersécurité)

Ci-après sont présentées brièvement quelques directives structurantes pour vos projets.

Nom	Secteur	Objectif	Exigence clé	Risques
NIS1 Détail Site Web	SI, infrastructures critiques et services essentiels	Améliorer la sécurité des réseaux et des SI au sein de l'UE pour protéger les infrastructures critiques et les services essentiels contre les cyberattaques et autres incidents de sécurité.	Elaborer une stratégie nationale de sécurité, créer une équipe de réponse aux incidents de sécurité informatique (CSIRT), échanger avec les autres membres de l'UE en vue de se coordonner.	Attaques et menaces contre les infrastructures critiques et les biens essentiels concernés par les SI.
NIS2 Détail Site Web	SI, services publics et d'intérêt général	Renforcer et harmoniser les capacités de cybersécurité au sein de l'UE, atténuer les risques de menaces.	Impliquer davantage la responsabilité d'acteurs désignés (opérateurs OIV d'importance vitale et OSE de services essentiels), à cet effet un manquement aux obligations NIS, en particulier de reporting, est sanctionné par des amendes conséquentes.	Attaques et menaces contre des infrastructures critiques plus étendues : réseaux de distribution de l'eau, services de communication électroniques ou certifiant les transactions numériques, entreprises de recherche scientifique.
RGPD Détail Site Web	Tout secteur ~~concerné par~~ traitant des données personnelles	Etablir des règles sur la collecte et l'utilisation des données, afin de renforcer les droits des personnes, responsabiliser les acteurs traitant des données, crédibiliser la régulation exercée par les autorités de protection des données.	Le traitement des données personnelles est encadré, de sorte à soumettre son utilisation à l'accord de la personne concernée, ainsi qu'à restreindre cet usage sur le territoire de l'UE et de pays (« adéquats ») disposant d'une réglementation équivalente (pas de transmission extérieure à ce périmètre).	Non-respect et violation des droits de données personnelles, en particulier dans des pays ne disposant pas de telles réglementations.
DORA Détail Site Web	Finances	Renforcer la résilience opérationnelle numérique des entités financières face aux cybermenaces et aux risques liés aux Technologies de l'Information et de la Communication.	Harmoniser les règles au sein de l'UE, garantir la protection des clients des entités financières et des investisseurs contre les retombées des perturbations numériques et renforcer les capacités de surveillance et de gestion des risques numériques par les autorités de réglementation.	Menaces issues des TIC (*), incidents insuffisamment gérés et aboutissant à des pannes, contrôle insuffisant des prestataires tiers de TIC, échanges d'information non conformes.
CRA : Cyber Resilience Act Détail Site Web	Produits numériques	Renforcer les normes de cybersécurité des produits qui contiennent un composant numérique, exigeant des fabricants et des détaillants qu'ils garantissent la cybersécurité tout au long du cycle de vie de leurs produits.	Protéger les consommateurs et les entreprises qui achètent des produits logiciels ou matériels comportant un composant numérique.	Vulnérabilités présentes sur des produits matériels et logiciels mis sur le marché ; Absence de conformité ou de transparence sur le respect de normes de sécurité des composants numériques.
CSA: Cyber Security Act Détail Site Web	Produits numériques	Certifier la cybersécurité des technologies de l'information et des communications.	Evaluer les produits TIC(*) (rôle de l'ANSI en France) selon les schémas et les méthodologies de certification définis par l'ENISA, et délivrer les certifications associées.	Non-conformité de produits TIC en cybersécurité.
IA Act Détail Site Web	IA	Encadrer le développement, la commercialisation et l'utilisation de l'IA.	Elever le niveau d'exigence des systèmes utilisant de l'IA traitant des données à caractère personnel. En particulier réaliser une **AIDP** (Analyse d'Impact sur les Droits Fondamentaux).	Impact sur les droits fondamentaux, contraire aux valeurs de l'UE ; Atteinte à la sécurité des personnes ou de leurs droits fondamentaux ; Absence de transparence, par exemple sur les chatbots.

(*) TIC : Technologies de l'Information et de la Communication

Se reporter en annexe §7.1.1 pour en connaître le détail.

3.2.2 Cadre réglementaire non européen

Liste des réglementations non européennes

Nom	Secteur	Objectif	Exigence clé	Portée	Risques
LPM Détail Site Web	SAIV (Importance vitale)	Garantir la sécurité nationale.	20 règles LPM de gouvernance, maîtrise des risques, maîtrise des SI, gestion des incidents et protection des systèmes.	France	Cyberattaques
Protection de la vie privée[10] Détail Site Web	Tous secteurs	Fournir un cadre réglementaire pour la protection des données personnelles.	Protéger la vie privée et les données personnelles des citoyens.	Plusieurs réglementations : nationales, régionales…	Risques sur la violation de la vie privée, les fuites de données ; Amendes liées aux non-conformités.
Homologation de sécurité Détail Site Web	Services de l'état	Fournir un cadre réglementaire pour la sécurité numérique du système d'information et de communications de l'Etat et de ses établissements publics.	Homologuer les systèmes d'information et de communication de l'Etat et de ses établissements publics : infrastructures et services logiciels informatiques.	France	Cyberattaques, pannes.

Se reporter en annexe §7.1.1 pour en connaître le détail.

3.3 NORMES INTERNATIONALES APPLICABLES EN 2024

Le tableau qui suit vous présente succinctement les principales normes **internationales** liées à la Cybersécurité applicables en 2024.

Nom	Secteur	Objectif	Exigence clé	Risques
ISO/IEC 2700x Détail Site Web	Tous secteurs	Fournir des lignes directrices et des bonnes pratiques pour la gestion de la sécurité de l'information.	27001 : mettre en place un SMSI ; 27002 : définir les contrôles de sécurité ; 27005 : gérer les risques.	Risques sur la sécurité des systèmes d'information.
ISO/IEC 22301 Détail	Tous secteurs	Fournir des lignes directrices et des bonnes pratiques pour la continuité d'activité et la gestion de crise.	Accroître la résilience de l'organisation face à différentes perturbations, et gérer une situation de crise	Absence de protection contre des perturbations majeures, pas ou peu d'anticipation, gestion de crise défaillante
ISO/IEC 31000 Détail Site web	Tous secteurs	Fournir des lignes directrices et des bonnes pratiques pour le management des risques	Détecter et réagir avec une approche globale, face à des menaces et aussi des opportunités	Risque de mauvaise compréhension ou d'absence de détection d'un risque, trop tardivement, perte de confiance
IEC 62443 Détail Site Web	Secteur industriel	Fournir des lignes directrices sur la sécurité des systèmes d'automatisation et de contrôle industriel (IACS).	Sécuriser les environnements industriels (systèmes, composants, produits).	Risques sur les infrastructures critiques, sabotages industriels.
Standards PCI Détail Site Web	Systèmes de paiement	Fournir des lignes directrices aux organisations opérant sur les systèmes de paiement, et aux fournisseurs de solutions de ces systèmes.	Protéger les données de paiement tout au long du cycle de vie du paiement.	Risques sur les fraudes et attaques relatives aux systèmes de paiement.

L'annexe **§7.1.2** indique le détail de ces normes, accessible en cliquant ci-dessus sur « détail ».

Le lien vers ces organisations est accessible en cliquant sur « Site Web ».

[10] Dont protection des données de santé : HIPAA aux USA, HDS en France (voir détail)

3.4 LES PRINCIPAUX REFERENTIELS

3.4.1 Différence normes vs cadres référentiels/framework

Les normes sont des exigences établies pour garantir la qualité, la sécurité ou la compatibilité des produits ou des processus. Elles sont généralement définies par des organismes de normalisation.

En revanche, les cadres référentiels appelés aussi couramment frameworks (en système d'information) sont des structures ou des plateformes qui fournissent des directives, des bibliothèques et des outils pour développer des applications. Ils offrent un ensemble de concepts et de pratiques pour guider le développement :

- Un guide à implémenter en fonction du contexte de l'entreprise ;
- Une implémentation plus ou moins complète d'une norme spécifique.

Se conformer à une norme et/ou s'appuyer sur un cadre référentiel est un avantage pour une entreprise. Du point de vue opérationnel, cela aide à anticiper et à gérer les risques de sécurité de l'information de manière systématique et proactive. En outre, c'est un atout pour réduire la probabilité et l'impact des incidents de sécurité grâce à des contrôles et des processus de gestion des risques efficaces.

Du point de vue stratégique, cela renforce la confiance des clients, partenaires et régulateurs en démontrant un engagement envers la sécurité de l'information. Par ailleurs, cela constitue un avantage concurrentiel en améliorant la réputation de l'organisation et en répondant aux attentes des parties prenantes en matière de sécurité de l'information. Enfin cela permet aussi de pouvoir négocier son assurance cyber à la baisse, soit un gain pour l'entreprise.

3.4.2 Référentiels de sécurité

Le tableau qui suit vous présente succinctement les principaux **référentiels de sécurité**.

Nom	Secteur	Objectif	Exigence clé	Risques
NIST Cybersecurity Framework Détail Site Web	Tout secteur	Ensemble de lignes directrices adoptées pour gérer les risques de cybersécurité.	Framework décliné en 5 fonctions : identifier, protéger, détecter, répondre, récupérer.	Cybersécurité
CIS Détail Site Web	Tout secteur	CIS produit des benchmarks qui permettent à une organisation de s'améliorer.	Recommande une sécurisation de configuration descriptive pour plus de 25 familles de produits.	Cybersécurité
OWASP Détail Site Web	Tout secteur	Améliorer la sécurité des logiciels.	OWASP Top Ten : liste des 10 vulnérabilités les plus courantes, actualisées.	Cybersécurité
MITRE Att&ck Détail Site Web	Tout secteur	Sa base de connaissance permet de modéliser, détecter, anticiper et lutter contre les menaces de cybersécurité basées sur les comportements adverses connus des cybercriminels.	3 angles d'attaques sont prévus : entreprise, mobile, systèmes de contrôle industriel.	Cybersécurité
SafeCode Détail Site Web	Tout secteur	Forum industriel mondial, où chefs d'entreprise et experts échangent des idées sur la création, l'amélioration et la promotion de programmes de sécurité logicielle évolutifs et efficaces.	Le développement de logiciels sécurisés ne peut être réalisé qu'avec un engagement organisationnel dans l'exécution d'un processus d'assurance holistique.	Cybersécurité
SecNumCloud Détail Site Web	Tout secteur	Propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique.	D'une part, les prestataires proposant une offre d'informatique en nuage (cloud) doivent présenter une bonne hygiène informatique, d'autre part, les données doivent être protégées en conformité avec le droit européen.	Cybersécurité

L'annexe **§7.1.3** indique le détail de ces référentiels, accessible en cliquant ci-dessus sur « détail ».
Il peut être consulté le site web de ces référentiels, en cliquant sur « Site Web ».

3.5 LES ORGANISATIONS DE LA SECURITE DE LA DONNEE NUMERIQUE

Les tableaux qui suivent vous présente succinctement les principales organisations de la sécurité de la donnée numérique.

Dans ces tableaux vous accéderez directement à l'objectif poursuivi par l'organisation, ainsi que son Site Web Officiel.

3.5.1 Les organisations européennes et nationales de cybersécurité

Elles sont détaillées dans l'annexe **§7.1.4** de ce document.

Description	Secteur	Objectif	Rattachement
ENISA Détail Site web	SSI	L'Agence de l'Union européenne pour la cybersécurité est l'agence de l'Union qui se consacre à la réalisation d'un niveau commun élevé de cybersécurité dans toute l'Europe. Créée en 2004, l'ENISA renforce la fiabilité des produits, services et processus TIC (*) avec des systèmes de certification en matière de cybersécurité, coopère avec les États membres et les organismes de l'UE et aide l'Europe à se préparer aux cyber-déficits de demain.	Europe
ANSSI Détail Site web	SSI	Déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle. Cette politique s'attache à défendre les infrastructures numériques publiques et privées les plus critiques.	SGDSN/PM
CEPD Détail Site web	RGPD	Le Comité européen de la protection des données est le successeur du G29. Les membres sont : les chefs des autorités de contrôle de chaque État membre (CNIL pour la France) plus le contrôleur européen de la protection des données	Europe
CNIL Détail Site web	RGPD	Autorité de contrôle, elle est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.	Autorité administrative indépendant (AAI)
CERT-FR France Détail Site Web	Incident SSI	Le CERT-FR traite sur le plan technique les incidents concernant l'administration et les Opérateurs d'Importance Vitale (OIV), et les entités essentielles et importantes (EE, EI)	ANSSI
COMCYBER France Détail Site web	Militaire	Le COMCYBER rassemble l'ensemble des forces de cyberdéfense du **ministère des Armées**. Il a pour mission la défense des systèmes d'information – dont les systèmes d'armes, ainsi que la conception, la planification et la conduite des opérations militaires dans le cyberespace.	Ministère des Armées
COMCYBER-MI France Détail Site web	Maintien de l'ordre	Le COMCYBER-MI rassemble l'ensemble des forces de cyberdéfense du **ministère de l'Intérieur**. Il a pour mission la lutte contre la cybercriminalité, que ce soit par le renseignement sur les structures cybercriminelles, et aussi sur les moyens d'action juridiques et judiciaires	Ministère de l'Intérieur

(*) TIC : Technologies de l'Information et de la Communication

3.5.2 Les associations françaises à but non lucratif dédiées à la cybersécurité

Nom	Secteur	Activités
InterCERT Détail Site Web	CERT	Association loi 1901 qui constitue la première communauté des CERTs en France. L'objectif de cette communauté de CERT est de renforcer la capacité de chaque membre à détecter et à répondre aux incidents de sécurité impactant son périmètre. Le partage d'expériences et l'échange d'informations concourent ainsi à la réalisation de cet objectif.
Club EBIOS Détail Site Web	Risque	Créé en 2006, le Club EBIOS est une association indépendante à but non lucratif (Loi 1901), composée d'experts individuels et d'organismes. Il supporte et enrichit le référentiel de gestion des risques français depuis 2003. Il promeut et développe EBIOS, tous ses usages et ses dérivés.
CLUSIF Détail Site Web	Sécurité de l'information et de la gestion des risques	Le Club de la Sécurité de l'Information Français (CLUSIF) est une association française à but non lucratif créée en 1982, dédiée à la sécurité de l'information et à la gestion des risques. Son objectif principal est de promouvoir les bonnes pratiques en matière de sécurité des systèmes d'information et de favoriser l'échange de connaissances entre professionnels du domaine.
CESIN Détail Site Web	SSI	Le Club des Experts de la Sécurité de l'Information et du Numérique réunit des responsables de la cybersécurité venant d'entreprises de tous secteurs d'activités et d'administrations, ayant pour principal objectif de contribuer collectivement à la montée en maturité des organisations en cybersécurité.
AFCDP Détail Site Web	RGPD	L'Association française des correspondants à la protection des données à caractère personnel (AFCDP) est une association loi de 1901, créée en 2004, dans le contexte de la modification de la Loi informatique et libertés qui a officialisé une nouvelle fonction, celle de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant informatique et libertés). L'association se focalise sur le métier devenu celui de Délégué à la protection des données, ou DPO (pour Data Protection Officer ou Data Privacy Officer), dans le cadre du Règlement général sur la protection des données (RGPD).

L'annexe **§7.1.5** indique le détail de ces référentiels, accessible en cliquant ci-dessus sur « détail ».
Le lien vers ces organisations est accessible en cliquant sur « Site Web ».

3.6 CONCLUSION DU CONTEXTE ? DIFFERENTES VISIONS SELON CONTEXTE NATIONAL, EUROPEEN ET MONDIAL.

En fonction du périmètre d'activité de votre entreprise, les cadres et réglementations vont varier.

Les politiques et réglementations en matière de cybersécurité se manifestent de différentes manières, à différents échelons.

Il existe par exemple des pactes de sécurité régionaux, des cadres réglementaires nationaux et des exigences sectorielles.

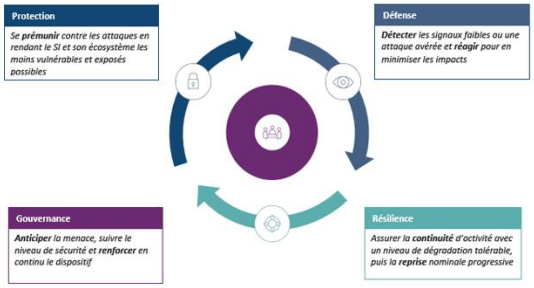
En particulier, nous notons une tendance croissante parmi ces politiques, à l'obligation pour les entreprises de certains secteurs de signaler aux agences gouvernementales compétentes les cyberattaques confirmées contre leurs systèmes, tant en Europe, qu'en Amérique du Nord et enfin dans la région Asie-Pacifique.

Le risque est décuplé quand on opère mondialement. À une ère de retour de la conflictualité, où chacun cherche à se renforcer et se protéger, les prérequis et les attentes ne sont pas les mêmes et nécessitent de mettre en place des approches ad hoc.

Même dans une zone en apparence unifiée telle que l'Union européenne, il est nécessaire de suivre les 27 transpositions de la directive **NIS2** dans les législations nationales. Ce qui confirme la complexité pour les entreprises internationales agissant en Europe de mener à bien une cybersécurité efficace.

4 Les enjeux de la Cybersécurité et de la Transformation Numérique

Ce paragraphe part du rappel inscrit dans les définitions de la cybersécurité, suivant.

Rappel : gérer le développement et la maturité de la cybersécurité	
	Se traduit en - Protection - Défense - Gouvernance - Résilience

Cela nous amène à proposer les enjeux suivants qui se ramènent aux questions du chef de projet :

- Sécurité des informations et des données sensibles
- Sécurité des infrastructures critiques dont le SI
- Sécurité dans les transformations numériques
- Adaptation de l'organisation permettant l'implication de tous les échelons dont le Comex
- Sensibilisation et formation des collaborateurs
- Gestion des risques de sécurité liés aux projets

En revanche, même si ces enjeux sont tous importants, ils ne sont pas tous de la responsabilité du Chef de projet. Par exemple la **Sécurité du SI** ou la **Sensibilisation et Formation des collaborateurs** n'est pas de sa responsabilité, sauf dans le cas très spécifique par exemple d'un projet de mise en place d'un SMSI, ou PCA.

Sous réserve des spécificités des activités de l'organisation considérée, il en est de même pour les points suivants qui peuvent être vus comme des objectifs à plus long terme :

- Lutte contre la cybercriminalité et les menaces pouvant affecter l'entreprise
- Innovation et adaptation
- Sécurité des objets connectés
- Résilience et continuité des activités
- Etc

La conformité avec la réglementation est également un enjeu majeur. Suivre les normes est un aspect fondamental de la gestion de projet, et la description des normes applicables a été faite en §3.2. Le chef de projet, à l'aide d'experts qui l'entourent, devra confirmer quelles normes s'appliquent à son projet.

4.1 SECURITE DE L'INFORMATION ET DES DONNEES DE L'ENTREPRISE

Le constat est sans appel, l'actualité regorge d'incidents de sécurité sur des données de toutes sortes et de tous niveaux de sensibilité. Longtemps difficilement audible par la grande majorité, la question est maintenant : « quand serons-nous à notre tour frappés et avec quelle gravité ? ».

L'un des risques majeurs d'exposition des données face à différentes menaces cyber, est la dégradation de contrôles liés à l'hébergement cloud des données, ou à l'hybridation massive de cet hébergement que vivent les entreprises depuis 2020.

Dernièrement, plusieurs évaluations sans qu'il soit possible de les citer, considèrent que les coordonnées de plus de la moitié des Français sont en vente dans des espaces liés à la cybercriminalité. Les fuites de données se multiplient. Le coupable tout désigné est un cybercriminel encore improprement et médiatiquement désigné de "hacker" pour faire le "buzz". En fait, ceci est le fruit d'un enchaînement de négligences, techniques certes, mais aussi organisationnelles, humaines et réglementaires d'organisations publiques et privées de toute taille : Hôpitaux, Centres hospitaliers, universités, écoles, collectivités territoriales, organismes de retraites, organismes de santé, mutuelles, services de l'Etat, etc.

Il est impératif de protéger la donnée et ses traitements contre toute compromission de sa sécurité en confidentialité, intégrité et disponibilité.

Exposer sans précautions élémentaires une donnée de l'organisation et/ou des individus qui y sont rattachés peut engendrer un **risque** dit « **numérique** » et ce risque numérique est à l'origine de nombreux autres risques (image, légal, financier, usurpation, etc.)

De façon similaire aux processus de production qui sécurisent l'usage de l'automobile, du train ou de l'avion, le numérique se doit de penser sa sécurité dès la conception.

4.2 LA SECURITE DANS LES PROCESSUS METIER ET LES PROJETS

Prenons l'exemple d'un outil sujet à une transformation numérique. Notre nouvel outil numérique s'inscrit dans une **infrastructure logique existante**, potentiellement un mélange de systèmes locaux et hébergés.

Il s'insère dans un SI beaucoup plus large, dans lequel il va établir de nouvelles communications en interne, vers l'internet ou dans la zone intermédiaire appelée DMZ, en engendrant de nouveaux risques, à la fois par contamination potentielle, mais également par augmentation de la surface d'attaque.

N'oublions pas que la protection du SI demeure un enjeu de cybersécurité. Le chef de projet est moins impliqué que les acteurs DSI, sauf exception (projet SI). Se reporter à l'Annexe A de la norme ISO27001, si besoin.

4.2.1 Penser la sécurité dès la conception

La **sécurité** est partie prenante du fonctionnel et doit être **pensée avec lui** et non comme un pansement que la norme nous oblige à coller.

La technologie a tendance à s'auto-légitimer (on doit la mettre en œuvre parce que c'est possible et que d'autres vont le faire). Qui prendrait un avion dont la sécurité a été rajoutée après la conception par laquelle le fonctionnel aura été poussé aux limites du possible ? Le fonctionnel doit être pensé avec **la sécurité comme arbitre.**

Penser la sécurité dès la conception permet également d'identifier et de traiter les vulnérabilités potentielles avant qu'elles ne deviennent des failles coûteuses à corriger. Par exemple, selon une étude[11] du NIST, corriger une vulnérabilité découverte après la mise en production peut coûter jusqu'à 30 fois plus cher que si elle avait été traitée lors de la phase de conception. Intégrer la sécurité dès le départ permet donc de réduire les risques, les coûts et les délais liés à d'éventuelles remédiations ultérieures.

4.2.2 Sécuriser les processus et les projets

La gestion de projet, répondant aux besoins fonctionnels et aux besoins de sécurité, s'inscrit dans une vision plus large de mise en cohérence dont il faut tenir compte en amont en termes de schéma directeur et d'arbitrage de l'exécutif.

Rappelons brièvement que le numérique, dans son développement enthousiaste et frénétique, n'a pas de légitimité *de facto*. Une organisation se doit d'avoir une stratégie et des axes de développement.

Le numérique est un outil d'automatisation de tout ou partie des processus métiers de cette organisation. L'outil numérique est avant tout une machine, un amplificateur, un accélérateur. Le processus aux étapes plus ou moins manuelles fonctionne à son optimum grâce à des corrections discrètes de ses opérateurs. Aucune organisation n'a de visibilité totale sur ses processus. Avant de les automatiser, il est fort nécessaire de les remettre à plat afin d'identifier des risques qui ne sont pas d'origine numérique mais fonctionnelle, dû à la conception et aux évolutions dans le temps.

Il faut **sécuriser le processus** d'un point de vue fonctionnel avant d'envisager de l'automatiser (« run ») et de répondre aux nouveaux besoins fonctionnels (« build »).

[11] Se référer à « Evolution du coût des corrections » (NIST, s.d.)

La sécurité de l'ensemble peut aussi être compromise par des besoins fonctionnels non couverts des directions métiers, non pensés, occultés, dans un angle mort faute d'un recensement des besoins fonctionnels et d'un schéma directeur.

Tout se passe comme si le développement de l'organisation pouvait se réaliser au travers des activités des directions sans vision transversale, sans stratégie, dans lequel chaque direction lutte de manière frénétique et managériale, avec son agenda et son budget, pour avoir accès aux ressources informatiques de son organisation ou d'un fournisseur, comme elle irait acquérir de simples « fournitures ».

L'émergence de nouveaux outils non maîtrisés pour répondre à ces besoins pourrait se faire en dehors de tout cadre porté par l'organisation. Pour les directions métiers, la tentation est grande et encouragée de faire appel à de l'hébergement *nuageux* (cloud) rempli de promesses. Une autre tentation est celle de la sous-traitance aux allures d'électro-ménager numérique, sans réelle maitrise des coûts futurs, des aspects réglementaires ou des conséquences juridiques, en cas d'incident, de compromission aux impacts graves sur les usagers, clients ou partenaires.

Les évolutions du SI avec la mutation de ses sous-parties et le développement de nouveaux projets numériques, doivent se faire en cohérence avec un schéma de développement d'ensemble. Même si des éléments de ce SI sont parfois non maîtrisés voir tout simplement inconnus de la DSI (« Shadow-IT »). Et il faudra le faire avec une architecture et des technologies choisies et mises en œuvre pour répondre à ses besoins de sécurité en conformité avec la réglementation, incluant les standards internes de l'entreprise (PSSI, …). La sécurité est intimement liée au contrôle du processus (cf. §5.2.1 Introduction à la maîtrise du risque numérique).

Ce constat factuel appelle à une vision d'ensemble permettant de piloter le SI.

De même que la culture de gestion de projet est héritée de l'industrie aéronautique, il a fallu trouver de nouvelles et nécessaires méthodologies pour maitriser le SI dans son ensemble avec sa complexité informatique toujours grandissante, toujours en mutation :

- Cartographie[12] – identifie les sous-parties, les processus métiers, les directions, les parties prenantes, les flux, la sensibilité des données, les sous-couches techniques, etc. ;
- Urbanisation – méthode s'appuyant sur la cartographie aidant au développement et à l'évolution harmonieuse et planifiée du SI, c'est un outil de pilotage du SI et de dialogue entre les directions ;
- Méthode ITIL – « Information Technology Infrastructure Library » a été créée afin d'améliorer la gestion des services informatiques. Son but est d'aligner les services informatiques avec les besoins des directions et de dispenser des services informatiques de qualité. Cette qualité dans le rendu fonctionnel est le gage d'une sécurité maîtrisée.

[12] Exemple donné plus loin en §5.2.7 Système de Management de la Sécurité

4.3 ADAPTATION DU CADRE ORGANISATIONNEL AUX ENJEUX

4.3.1 Quelle organisation pour maîtriser le risque de Cybersécurité ?

Quel acteur semble le plus pertinent pour gérer le risque Cybersécurité ?

- Le chef de projet ?
- La DSI ?
- La Direction Générale ?

Encore faut-il que les acteurs concernés se coordonnent pour gérer ce risque et que l'organisation le permette et le facilite.

Il est important que le risque cyber soit adressé au bon niveau, et en particulier que les comités exécutifs prennent leur responsabilité entière et complète sur le sujet.

Dans le même temps il est important qu'il soit également géré au niveau opérationnel.

La gestion du risque projet est un processus spécifique de la gestion de projet. Permet-il la gestion du risque de cybersécurité ou bien faut-il penser une organisation spécifique ?

4.3.2 L'engagement managérial

Le cercle vertueux de la sécurité ne peut s'activer que par un fort engagement managérial au plus haut niveau.

À la manière du virage engagé par Bill Gates en 2002 avec son célèbre mail "Trustworthy Computing" : "So now, when we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve". (Source : Bill Gates).

C'est en effet le nerf de la guerre puisqu'il en découle ensuite le sens et une stratégie déclinée au sein de l'entreprise. Bien entendu, selon les priorités de l'entreprise sur les différentes lignes de produits, les moyens financiers peuvent être bien différents. En conséquence, les moyens sécurité aussi, et il faudra choisir de manière la plus pragmatique possible ce qu'il sera envisageable d'atteindre avec les moyens donnés.

Ne nous leurrons pas, l'objectif est de **faire mieux avec moins**. Et dans ce cadre-là, l'automatisation (avec ses doses d'intelligence artificielle) est systématiquement une carte à jouer puisqu'elle est censée réduire les efforts à terme sur des sujets atteignables (ne nécessitant pas d'analyse humaine pointue) à condition toutefois de mettre les moyens pour construire ces processus/outils d'automatisation, ce qui est clairement un défi.

4.3.3 Le changement de culture des responsables et équipes produits

Dans un monde Agile, les « Business/Product/Service Owners » sont pleinement responsables de la feuille de route de leur produit ou service. En conséquence, ils sont aussi garants des aspects sécurité sur leur produit ou service. La mise en responsabilité est bien entendu vertueuse et une belle cible à atteindre, ce qui résonne à ce qu'affirme Werner Vogels (Amazon CTO, 2018) « security is everyone's job now, not just the security team's. » repris de concert par Dino Dai Zovi dans sa présentation d'introduction à BlackHat USA 2019 « Every Security Team is a Software Team Now », mais elle ne peut réussir que si les prérequis sont en place.

Il ne s'agit pas d'un modèle de mise en responsabilité sans en donner les leviers et moyens associés. Une organisation des forces sécurité au service de la conception des produits doit être mise en place en parallèle d'une organisation / responsabilité sécurité au sein de l'équipe produit en elle-même.

En effet, l'expertise en cybersécurité, au fait des dernières évolutions technologiques, se doit d'être déployée dans toute l'entreprise. Mais ce modèle de mise en responsabilité, pour qu'il soit fonctionnel en pratique, doit prendre en compte plusieurs aspects :

- Un rôle de correspondant sécurité doit être identifié au sein de l'équipe produit, ce rôle pourra être l'interface entre l'équipe produit et les acteurs sécurité (correspondants sécurité ou équipes sécurité) ;
- L'équipe produit ne peut construire de zéro tous les processus/services sécurité transverses, elle doit se reposer sur l'existant au niveau de l'organisation ;
- L'équipe produit ne gère pas forcément les recrutements de la force au travail, un alignement avec les lignes managériales est nécessaire pour disposer des ressources avec des compétences sécurité ;
- En ce sens, le mindset de securité by design et la responsabilisation de l'ensemble des acteurs de l'entreprise sont à renforcer avec pour vocation de protéger le business de l'entreprise.

4.3.4 Impact sur les ressources humaines : les compétences

Ceci n'est pas un enjeu propre à la **Cybersécurité**, mais est bien entendu général.

L'enjeu de ressources humaines est colossal et est relié directement aux stratégies d'entreprise, comme par exemple, "faire faire" ou "savoir-faire". Il est évident que les deux stratégies ont des avantages et des inconvénients, mais si nous nous projetons sur la Cybersécurité, la maîtrise technologique des actifs construits ou opérés est essentielle pour assurer un niveau élevé de maîtrise et donc des risques sécurité associés.

Dans ce cadre-là, la politique des ressources humaines est déclinée directement de la stratégie d'entreprise, elle peut parfois être infléchie "localement" à des entités selon le degré de liberté qui leur aura été accordée. Toujours est-il que des invariants apparaissent : les entités ayant l'habitude de construire par elles-mêmes des lignes de produit sont souvent en maîtrise de l'ensemble des composants qui les composent, et la qualité de service et la Cybersécurité en font partie.

A contrario, la gestion de la Cybersécurité uniquement par une relation contractuelle client/fournisseur, n'apporte pas un développement des compétences Cybersécurité au sein des entités habituées à ce mode de fonctionnement : la Cybersécurité devient externalisée, et la culture avec.

Malgré ces constats, il est cependant nécessaire de développer une **culture cybersécurité minimale**, pour toutes les lignes de collaborateurs, quelles que soient les entités et les métiers. Ceci est à la main des politiques de ressources humaines, où des prérequis en termes de connaissance de culture d'entreprise seraient attendus puis mis en œuvre, tout comme cela est fait pour l'accessibilité, l'égalité professionnelle ou la Responsabilité Sociétale de l'Entreprise. La Cybersécurité doit obligatoirement en faire partie pour légitimer cette nécessité au plus haut niveau et la décliner ensuite.

5 Comprendre l'écosystème de la sécurité de l'information

5.1 Importance de la Gouvernance pour le Chef de projet

La gouvernance doit être **partie prenante** dans la prise en compte des risques sur le système d'information. Elle doit être responsabilisée dans la couverture des risques en y allouant les moyens humains et financiers nécessaires, ainsi que dans l'acceptation des risques résiduels qu'elle choisit de ne pas couvrir.

La gouvernance est donc associée au lancement de chaque nouveau projet, cadré par une identification des besoins de sécurité, porteuse d'une conduite du changement dont celui lié à la sécurité.

Elle est sollicitée à la clôture de chaque projet en tant qu'autorité d'homologation de sécurité, où le comité d'homologation déterminera si le système d'information est apte à être mis en production et la durée de cette homologation.

Les usagers d'un SI sont ainsi informés que l'autorité de l'organisation a connaissance des risques qui pèsent sur ce SI. Il s'agit d'un arbitrage autour du risque que porte l'organisation. Il faut rappeler que le risque numérique est à l'origine de nombreux autres risques, pour l'organisation, ses usagers et dans le temps.

C'est dans cette optique que **la gouvernance prend en considération le risque numérique** de chaque nouveau projet ou évolution du système d'information.

Par cet engagement, la gouvernance contribue pleinement à l'intégration de la sécurité dans les nouveaux projets comme dans la mise à jour des systèmes d'information existants. Les nouveaux SI font partie d'un schéma directeur des systèmes d'information ou du numérique, schéma directeur au service de l'organisation, que la gouvernance a validé stratégiquement.

L'ensemble constitue pour la gouvernance un ensemble cohérent avec des objectifs stratégiques pour l'organisation, des outils informatiques et numériques au service de ses objectifs cadré par un schéma directeur validé, avec une approche de la sécurité par la connaissance, la maîtrise et la réduction des risques.

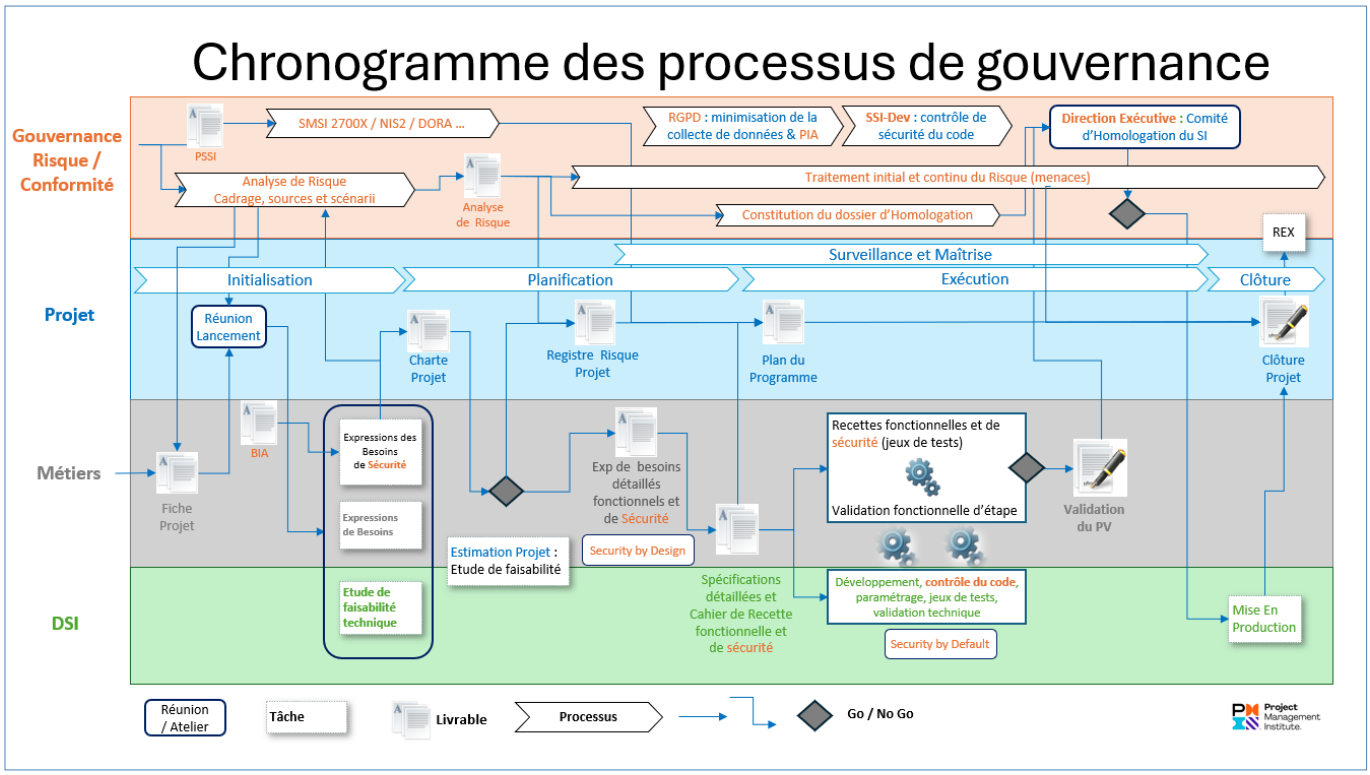


Figure 5 - Chronogramme des processus de gouvernance liée à la sécurité dans les projets (source : PMI)

Ce schéma souhaite donner une **vision globale** des différents processus de gouvernance impliqués dans l'intégration de la sécurité dans les projets.

Elle est construite sur l'interaction de **4 couloirs de nage ou échelons** différents composés d'acteurs spécifiques :

- l'échelon **Gouvernance Risque Conformité** intègre un **RSSI GRC** (ou le directeur de la sécurité) en liaison étroite avec la **Direction Générale** ou le **Comex** qui validera les grandes étapes du projet en particulier la partie **Homologation** du SI ;
- l'échelon **Projet** intègre un **Chef de Projet**, un Directeur de Projet ou de Programme en charge du Pilotage du Projet ;
- l'échelon **Métier** intègre un **Responsable Métier** à l'origine de la **demande projet**, des **exigences** et qui aura la charge du produit final généré ;
- l'échelon **DSI** qui intègre un **Responsable DSI**, en charge de la réalisation.

Ces **différents échelons** sont tous essentiels. Le **Chef de projet** se doit de bien les connaître afin de piloter au mieux le projet dans le respect des intérêts mutuels.

Pour que le projet soit un succès partagé, il est important que **tous les acteurs** puissent jouer pleinement leur rôle.

Le **Métier** doit exprimer ses besoins, en particulier en matière de sécurité, et s'impliquer fortement dans les arbitrages financiers, la co-construction et la recette du produit.

La **DSI** devra être à l'écoute et réaliser le produit demandé dans le cadre contraint qui est le sien (Architecture technique, contexte financier).

L'échelon **Gouvernance** nous apparaît **primordial** parce qu'il n'est pas toujours bien compris et qu'il peut faire courir le risque d'un manque d'implication de la **Direction Générale**, le Chef de projet étant parfois trop éloigné de cet échelon.

C'est la raison qui nous a incité à mettre l'accent sur la partie Gouvernance qui est largement détaillée dans ce premier Livre Blanc.

D'autres Livres Blancs traiteront en profondeur de « l'Intégration de la sécurité dans les projets » ainsi que des « analyses de risques liés à la cybersécurité ».

Ainsi le chapitre 5 de ce premier Livre blanc traite des points suivants :

- Gouvernance et Management de la sécurité de l'information et du SI ;
- Présentation de l'Intégration de la sécurité dans les projets (point détaillé ultérieurement) ;
- Présentation de l'Analyse des risques de Cybersécurité (point détaillé ultérieurement).

Illustration de la relation entre la gouvernance et le Pilotage de Projet à travers l'outil RACI (« Responsible » (réalisateur), Accountable (approbateur), Consulted (consulté), Informed (informé)).

La responsabilité pleine et entière du **pilotage des projets** demeure attribuée aux acteurs terrains : les directeurs et chefs de projet. Cependant la sécurité doit s'exercer avec un dispositif à la fois terrain et d'accompagnement.

Par exemple dans une ESN (Entreprise de Services Numériques), les projets sont organisés au sein de **Centres de Services (CDS),** et placés sous la responsabilité de Directeurs de Projet et de Chefs de projets. Pas de DSI dans cet exemple, l'équipe projet réalise le logiciel. Un **chargé de sécurité opérationnelle** est affecté à chaque projet. Les responsabilités RACI sont indicatives, elles s'appliquent à cet exemple précis.

Le déploiement de la sécurité dans l'entreprise est assuré par une équipe **centrale sécurité,** dirigée par un **RSSI** et placée sous la responsabilité d'un Directeur de la Conformité (membre du COMEX). Cette équipe se compose de spécialistes et experts en veille sécurité, de gestionnaires d'incident et d'auditeurs internes.

L'équipe centrale sécurité accompagne les projets au côté des **chargés de sécurité opérationnelle**, en réalisant par exemple des analyses de risques ou des études spécifiques, des audits, de l'accompagnement au suivi des vulnérabilités et de la sensibilisation (voir plus loin). Cette équipe et son responsable, le **RSSI**, assurent ainsi la gouvernance sécurité, dont l'animation de la communauté des acteurs sécurité affectés sur le terrain des différents métiers de l'entreprise (dont les projets). Voir schéma ci-dessous.

R = Réalise
A = Approuve
C = Consulté
I = Informé

Activités SSI	Sous-activités	Directeur Conformité	RSSI	Expert Veille	Auditeur interne	Resp. Gestion Incidents	Equipe Sécurité	Responsables CDS	Chargé Sécu. Opérationnelle	DP, CP	Autres collaborateurs CDS
A7 - Accompagner les centres de services	A7.1 - Insérer la sécurité dans les projets	I	A	I	I	I	C	R	C	C	C
	A7.2 - Accompagner les responsables CDS, DP, CP	I	A	I	I	I	R	C	C	C	I
	A7.3 - Suivre les chantiers et plans d'action CDS	I	A	C	I	C	R	C	R	R	C

Figure 6 - RACI pour accompagner les projets

Insérer la sécurité dans les projets, pour le RSSI, c'est convaincre les patrons de projet (responsables CDS) de sensibiliser les directeurs et chefs de projet à la sécurité, et de nommer des correspondants sécurité dans leurs équipes. L'équipe sécurité aide ces acteurs à maîtriser leur responsabilité en sécurité.
Note : les acteurs projets figurent ci-dessus sur fond bleu, l'équipe sécurité représentée en fond saumon.

5.2 GOUVERNANCE ET MANAGEMENT DE LA SECURITE DE L'INFORMATION ET DU SI

La gouvernance de la sécurité consiste en l'organisation des acteurs jouant un rôle dans la sécurité de ces systèmes afin d'atteindre les objectifs définis par la stratégie de cybersécurité. Cette stratégie est définie par un ensemble de facteurs dont notamment les besoins métiers et standards internes, les risques de cybersécurité ou encore les exigences définies par les réglementations.

5.2.1 Introduction à la Maîtrise du risque numérique et gouvernance [13] par l'ANSSI

« Le risque numérique est devenu un risque stratégique pour les organisations : il est potentiellement « mortel », non évitable et son pilotage n'est pas externalisable. Pour déjouer les cyberattaques, il est indispensable d'inscrire la sécurité numérique dans l'ADN des organisations. Les responsables métiers et les décideurs doivent ainsi s'approprier ces enjeux à leur niveau. »

« La transformation numérique s'est accompagnée d'une interconnexion croissante de l'ensemble des acteurs de la société, faisant en même temps évoluer le risque numérique du champ purement technique vers un risque pesant de plus en plus fortement sur l'activité des organisations. Ce nouveau paradigme oblige dorénavant les dirigeants à reconsidérer leur modèle de gestion des risques de telle sorte que le risque numérique rejoigne les préoccupations stratégiques, économiques ou juridiques des organisations. »

La sécurité doit être pilotée au sein des **instances de management de l'organisation** pilotant les différents métiers de l'entreprise.

Ainsi, le **chef de projet**, au sein du processus métier auquel il appartient, doit y contribuer à son niveau en intégrant la sécurité dès le **lancement** de ses projets.

5.2.2 Stratégie pour une maîtrise de sécurité du numérique

Elaboré par l'ANSSI et l'AMRAE, le guide « Maîtrise du risque numérique – L'atout confiance »[14] propose une démarche pragmatique issue de l'expérience des principaux acteurs de la maitrise du risque numérique. Cet ouvrage de référence s'adresse notamment aux dirigeants, CISO groupe et directeurs en charge de la sûreté, la sécurité ou la gestion de crise. Il concerne les organisations de toute taille.

La démarche proposée s'articule autour de 4 axes :

- PRENDRE LA MESURE DU RISQUE NUMÉRIQUE de manière proportionnée aux enjeux de transformation et de compétition économique ;
- COMPRENDRE LE RISQUE NUMÉRIQUE ET S'ORGANISER pour élaborer une stratégie de sécurité numérique adaptée au seuil d'acceptation de la menace ;
- BÂTIR SON SOCLE DE SÉCURITÉ en agissant sur **3 activités spécifiques** : protéger vos actifs, surveiller et anticiper la menace, faire preuve de résilience en cas de cyberattaque ;
- PILOTER SON RISQUE NUMÉRIQUE ET VALORISER SA CYBERSÉCURITÉ pour générer de la confiance auprès de vos clients et partenaires, et en faire un atout de compétitivité.

Là encore, le Chef de projet interviendra sur le pilotage du risque numérique dans le cadre de son projet.

[13] L'atout confiance (ANSSI, 2019)

5.2.3 Cadre de gouvernance du risque numérique [14]

Une bonne gouvernance du risque numérique passe par la mise en place d'un comité dédié et adapté aux réalités de l'organisation. Son rôle est de définir la stratégie de sécurité numérique de l'organisation, de s'assurer de sa mise en œuvre, de piloter la performance et de valoriser les investissements réalisés.

La gouvernance du risque numérique s'inscrit dans une démarche de long terme et doit pouvoir trouver sa place dans le fonctionnement habituel de l'organisation, ce qu'apporte la solution du **Système de Management de la Sécurité du Système d'Information** (SMSI). Un exemple est donné plus loin en §5.2.7 .

Elle s'appuie sur trois « lignes de maîtrise » fréquemment appelées **les trois lignes de défense** :

- Les fonctions opérationnelles et les responsables métiers ;
- Les spécialistes des risques (y compris numériques) à même d'assister les fonctions opérationnelles dans l'identification et l'évaluation de leurs risques ;
- La fonction d'audit (interne ou externe selon la taille de l'organisation) indépendante et liée au plus haut niveau de l'organisation.

5.2.4 Organisation du numérique et de sa sécurité

Le **schéma directeur du numérique** et celui de la sécurité du numérique sont des instruments du schéma directeur stratégique de l'organisation.

Le Comité stratégique de la SSI (Sécurité du Système d'Information) porte la responsabilité de définir la stratégie de sécurité numérique de l'organisation, de s'assurer de sa mise en œuvre, de piloter la performance et de valoriser les investissements réalisés. Il définira une organisation de la SSI et s'appuiera sur un schéma directeur ou un ensemble de chantiers de sécurisation permettant à l'organisation de monter en compétences, en maturité et en conformité, d'appliquer les mesures issues des analyses de risque réalisées en amont des projets numériques issus du schéma directeur du numérique et de prendre les mesures découlant de l'analyse des incidents.

Les projets et leur sécurisation s'inscrivent dans :

- Schéma directeur du numérique structurant un ensemble de projet ou portefeuille des projets ;
- Cartographie du SI maintenue par les directions[15] ;
- Urbanisation du SI maintenue par la direction technique du SI[10].

5.2.5 Rôles liés à la sécurité de l'information au sein de l'organisation

5.2.5.1 Rôle du ou des RSSI

Moyennant solide formation, un candidat au poste de RSSI doit faire preuve d'aisance orale et écrite ainsi que d'aptitude à structurer sa pensée dans un environnement changeant constamment. Ces compétences lui permettront de jongler entre : contact à haut niveau (CODIR/COMEX), animation, orchestration, organisation de collectifs, négociation, management d'équipe, prise de temps pour comprendre/aider et fluidifier.

[14] Gouvernance de sécurité numérique (ANSSI, 2025)
[15] Cartographie du système d'information (ANSSI, 2018)

Le RSSI devra construire le socle sécurité, sous le parrainage de la DG, et avec l'aide d'acteurs déjà familiers des processus de l'entreprise :

- Création ou mieux, adaptation du système de management de l'entreprise,
- Mise en place des instances appropriées pour le pilotage de ses processus,
- Définition/enrichissement d'indicateurs, de tableaux de bord,
- Mise en place des bases incidents, d'audits multi-sectoriels, du suivi d'analyse des risques, d'un plan de continuité d'activité et d'organisation de cellules de crise
- Définition et suivi d'un programme de sensibilisation à la sécurité
- Alimentation et animation d'un réseau de correspondants sécurité parmi les métiers de l'entreprise

En termes de cyber sécurité comme de projets, une **équipe sécurité dédiée s'avère indispensable**. L''équipe centrale de sécurité peut être composée d'experts en cybersécurité, d'auditeurs, d'analystes, de risk managers, ainsi que d'acteurs sécurité responsables de la gouvernance et est souvent sous la responsabilité d'un RSSI ou d'un RSSI délégué.

Elle est garante de la gouvernance globale de sécurité à appliquer à l'ensemble de l'entreprise. Pour les organisations les plus complexes, elle peut être divisée en plusieurs équipes par périmètre, et alors sous la responsabilité d'un RSSI délégué à ce périmètre.

Elle est également responsable de l'animation de la communauté des acteurs sécurité, notamment des acteurs les plus proches des projets tels que les chargés de sécurité opérationnelle ou les Security Champion.

Cela inclut la gestion et mise à jour d'un référentiel documentaire, d'indicateurs… à jour.

5.2.5.2 Positionnement du ou des RSSI

Une question se pose de manière récurrente au sujet du RSSI : la dénomination anglo-saxonne CISO représente-t-elle la même chose que la dénomination française de RSSI ?

Rappel :

- **RSSI** = **R**esponsable de la **S**écurité du **S**ystème d'**I**nformation
- **CISO** = **C**hief **I**nformation **S**ecurity **O**fficer

Aux États-Unis, la responsabilité pénale s'applique au CISO, alors qu'en France elle sera appliquée au niveau le plus haut, à savoir la Direction Générale.

D'autre part, le CISO fait partie des CxO et du COMEX.

En France, ce rôle est, généralement, rattaché à un directeur conformité (et risque), donc ne suivra pas le risque opérationnellement.

Cette lacune peut être comblée, si le RSSI propose une organisation adaptée sous forme :

- D'instance de supervision des patrons métiers sur le thème SSI ;
- De relais ou correspondants dans les différentes entités métiers.
- Dans ce cas, sans responsabilité hiérarchique directe, car il est en mesure d'animer cette communauté de correspondants, de sorte à faire passer les informations, les directives…
- Avec cependant la possibilité de manager une équipe conséquente, d'acteurs sécurité spécialisés par thème. Dans ce cas, cette animation pourra être facilitée car démultipliée (voir plus loin)

Dans le cas où le RSSI est rattaché à un DSI le positionnement du RSSI est sujet à caution : doit-il régler des problèmes de sécurité, ou des problèmes de la DSI ?

Une autre formulation, pour écarter cette situation hasardeuse, est de séparer les domaines d'intervention du RSSI :

- **RSSI G**ouvernance **R**isque **C**onformité (RSSI GRC) : au cœur des organisations stratégiques, un conseiller du Comex définit la politique de sécurité à haut niveau et travaille étroitement avec le RSSI opérationnel.
- **RSSI Opérationnel** : a pour mission de maintenir la sécurité des SI. En tant qu'assistance à maîtrise d'œuvre, il apporte son expertise et propose des mesures de sécurité en termes d'architectures, de produits et de paramétrages. L'objectif est de se conformer aux bonnes pratiques, à la PSSI de l'organisation et aux mesures arbitrées lors des analyses de risque. Ainsi la direction et son RSSI GRC bénéficient de la sécurité des éléments techniques du système d'informations de l'organisation.

Les experts en sécurité sont des acteurs de l'équipe sécurité centrale qui jouent un rôle d'accompagnement transverse sur le périmètre de l'équipe sécurité centrale.

5.2.5.3 Autres fonctions SSI

Les **Correspondants SSI (ou CSSI)** assurent l'accompagnement, la sensibilisation adaptée et la communication de leur entité organisationnelle (direction, service, atelier, laboratoire, etc.) et le/les RSSI de l'organisation. Ils forment avec les RSSI une chaîne fonctionnelle de la sécurité des SI, qui collecte depuis la base incidents, faiblesses, dysfonctionnements, permettant d'alimenter la base de connaissance des risques numériques de l'organisation, et diffuse les postures réglementaires et/ou issues d'analyses de risque depuis la direction opérationnelle vers les organes de l'organisation.

En cas d'incident, cette chaîne fonctionnelle travaille en étroite collaboration avec les équipes opérationnelles, qu'elles soient techniques ou de sécurité.

Par ailleurs, ces correspondants peuvent agir comme conseiller, tant en terme de recommandations de sécurité que de soutien dans leur implémentation.

Les **chargés de sécurité opérationnelle** (cf 5.1) sont des acteurs dont le périmètre d'activité est limité au projet. Ils possèdent l'expertise technique spécifique au projet et ont pour mission de veiller qu'à son démarrage, les décisions prises respectent la gouvernance sécurité. Si nécessité d'étude ou d'analyse spécifique, ou lorsqu'un audit est planifié, ils peuvent faire appel à l'équipe centrale de sécurité.

5.2.6 Ressources, conformité, responsabilités et déploiement

Suivant l'explication des acteurs projets concernés par la sécurité, du **§5.1**, la gouvernance sécurité étend son périmètre hors des seules activités projet. Comme mentionné en **§5.2.4**, d'autres **sujets de sécurité** sont traités avec la mise en place d'une **équipe centrale**, rassemblant plusieurs acteurs sécurité. Ces sujets sont :

- Gérer les incidents de sécurité, la veille sur les menaces et vulnérabilités
- Repérer les risques et gérer les changements appropriés à les réduire,
- Maintenir un haut niveau de fiabilité et de résilience de l'organisation.
- Maintenir la conformité

Il est décrit ci-dessous l'exemple d'une ESN, dont les activités de sécurité sont gérées selon le RACI suivant :

R = Réalise
A = Approuve
C = Consulté
I = Informé

Activités SSI	Sous-activités	Directeur Conformité	RSSI	Expert Veille	Auditeur interne	Resp. Gestion Incidents	Equipe Sécurité	Responsables CDS	Chargé Sécu. Opérationnelle	DP, CP	Autres collaborateurs CDS
A1 - Gérer le Système de Management Sécurité	A1.1 - Organiser les comités et les revues	C	A	I	C	C	R		C		
	A1.2 - Gérer les référentiels et les documents	I	A	C	I		R	I	I	I	I
	A1.3 - Gérer les indicateurs, constats et plans	C	A	C	C	C	R				
	A1.4 - Gérer l'équipe	A	R	I	I	I	I				
A2 - Organiser les audits	A2.1 - Audits externes	C	A	C	C	C	C	C	C	C	C
	A2.2 - Audits internes	C	A		R			C		C	
	A2.3 - Audits Réflexes	C	A				R	C	C	C	C
	A2.4 - Audits Fournisseurs	C	A				R				
	A2.5 - Audits CDS	C	A		R			C	C	C	C
A3 - Gérer les actifs et les risques	A3.1 - Identifier les risques	I	A	R			R	I	C	I	
	A3.2 - Analyser les risques	I	A	R			R	I	C	I	
	A3.3 - Gérer les changements	I	A	I			C	I	C	I	
A4 - Gérer la veille, les menaces et les vulnérabilités	A4.1 - Collecter	I	A	R		I	C	I	C	I	I
	A4.2 - Analyser	I	A	R		I	C	I	C	I	I
	A4.1 - Traiter	I	A	R		I	C	I	C	I	I
	A4.1 - Contrôler	I	A	R		I	C	I	C	I	I
A5 - Gérer les situations de danger	A5.1 - Gérer les incidents de sécurité	I	A	I	I	R	I	C	R	C	C
	A5.2 - Gérer les Plans de Continuité d'Activité	I	A	I	I	C	C	C	C	C	I
	A5.3 - Gérer les crises	I	A	I	I	R	C	C	C	C	I
A6 - Conduire le changement	A6.1 - Communiquer	I	A	C		I	R	I	I	I	I
	A6.2 - Former	I	A	C		I	R	I	I	I	I
	A6.3 - Sensibiliser	I	A	C		I	R	I	I	I	I
A7 - Accompagner les centres de services	A7.1 - Insérer la sécurité dans les projets	I	A	I	I	I	C	R	C	C	C
	A7.2 - Accompagner les responsables CDS, DP, CP	I	A	I	I	I	R	C	C	C	I
	A7.3 - Suivre les chantiers et plans d'action CDS	I	A	C	I	C	R	C	R	R	C
A8 - Accompagner les métiers	A8.1 - Identifier les actifs et les risques métier	I	A	I	I	I	R				
	A8.2 - Accompagner le processus métier	I	A	I	I	I	R				
	A8.3 - Suivre les chantiers et plans d'action métier	I	A	C	I	C	R				

Figure 7 - RACI des Activités de sécurité dans une ESN

A noter que cet exemple d'une ESN de taille intermédiaire, simplifie l'attribution des responsabilités (notamment A et R). Le chef de projet devra vérifier ces attributions, dans son entreprise ou chez son client.

5.2.7 Le Système de Management de la Sécurité de l'information

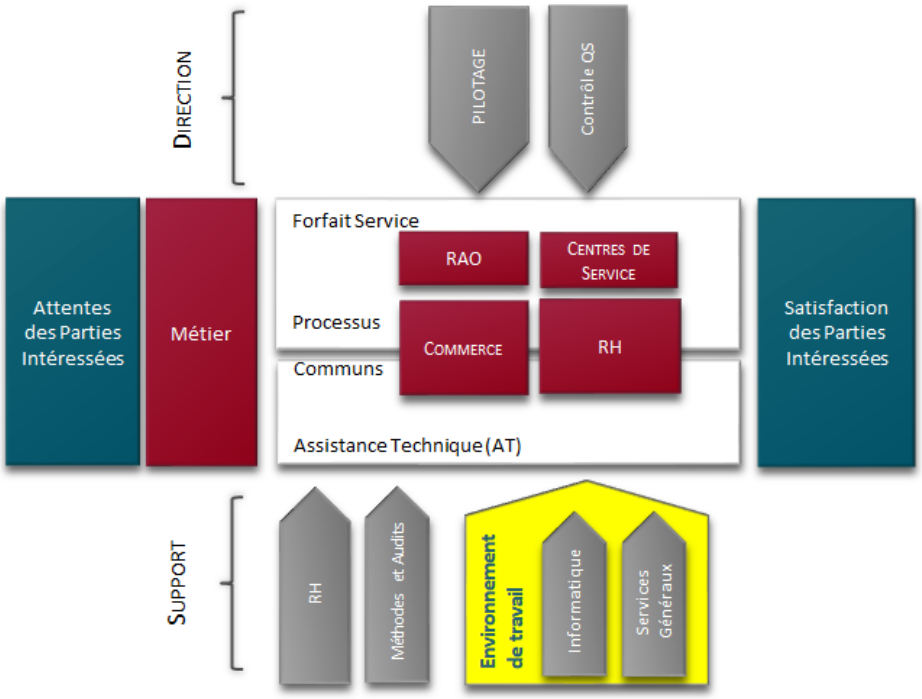
Pour bien comprendre comment la gouvernance sécurité s'applique à l'ensemble des activités métiers de l'entreprise (et des projets qui en sont issus), approfondissons la notion de système de management.

Le **Système de Management de la Sécurité de l'Information**, est fréquemment construit dans les grandes entreprises et les ETI, selon un Système de Management de la Qualité, préexistant au contexte plus récent de la Cybersécurité. Il permet de visualiser et présenter les processus de l'entreprise selon les attentes et satisfaction des parties prenantes.

Dans la quête de performances, l'entreprise doit s'améliorer en permanence (principe de l'amélioration continue / PDCA). Ce que permet le système de management de la qualité, piloté par la DG.

De la même façon, l'exposition aux risques et conséquences de sécurité, doit être visualisée par un système de management de la sécurité. Pour ne pas créer de dispositif organisationnel spécifique qui surchargerait le pilotage, un système de management mixte (qualité et sécurité) permet d'être facilement maîtrisé par les différents responsables métiers et la DG, car déjà utilisé.

Par exemple, ce système commun est présenté ci-dessous pour une ETI de nature ESN :



Processus	Direction	Métier	Support
Pilotage	✓		
Contrôle QS	✓		
Commerce		✓	
RAO		✓	
Centres de Service		✓	
RH		✓	✓
Informatique			✓
Méthodes et Audits			✓
Services Généraux			✓

Figure 8 - Exemple d'un Système de management d'une ESN

Note 1 : le processus RH est dédoublé, en tant que processus métier (recrutement et suivi des consultants) et processus support (recrutement et suivi personnel en structure).

Note 2 : le processus « Contrôle QS » exerce un contrôle sur le système de management, selon deux familles d'exigences adossées à des normes : qualité, sécurité (ISO9001, ISO27001).

- Ainsi dans les instances périodiques que le Système de Management prévoit, chaque responsable métier en charge d'un processus indiqué ci-dessus, est tenu de présenter des indicateurs bi-référentiel à la DG.
- De la sorte, l'exposition aux risques et la conformité de sécurité est supervisée au plus haut niveau (DG) par l'acteur métier responsable, chargé de faire appliquer moyennant aide de l'équipe centrale sécurité, les règles de gouvernance sécurité.

En termes de système de management de sécurité, il est exposé ci-dessous, la description du RACI de cette même ESN, englobant cette fois-ci tous les processus métiers, en plus des acteurs projets.

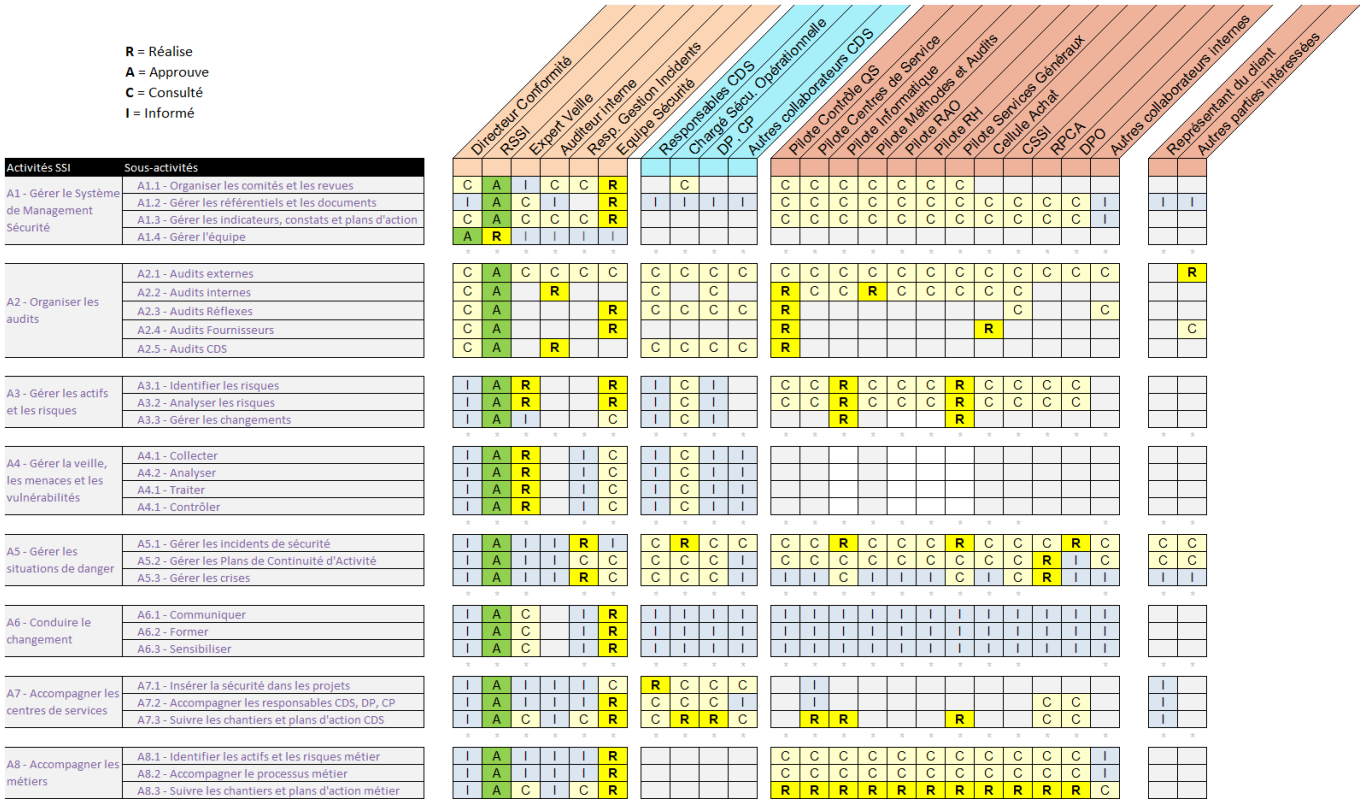


Figure 9 - RACI sécurité sur tous les métiers d'une ESN

A côté des processus identifiés par le système de management de la qualité (figure précédente), ce RACI décrit le rôle sécurité d'autres entités :

- En charge d'aspects comptables et financiers,
- Sous-traitance de consultants (cellule achat) et représentants clients couverts par le processus Commerce,
- Autres acteurs spécifiques sécurité : DPO ou Data Protection Officer, RPCA ou responsable des Plans de Continuité d'Activité, CSSI ou correspondants SSI…)

5.2.8 Engagement et sensibilisation des Parties Prenantes et des dirigeants

La sécurité implique toute l'entreprise :

- En conséquence elle exige une implication à la hauteur des rôles et responsabilités de chacun
- Néanmoins, une équipe spécialisée, apportant expertise et activités de sécurité précises, est souhaitable

5.2.8.1 L'homologation (proposée par l'ANSSI)

Cette instance est obligatoire dans le cadre des services de l'état, sur son système d'information. Cette étape est obligatoire pour les SI des services de l'État.

Elle est recommandée pour d'autres organisations, en vue d'un pilotage des risques par les dirigeants.

Son objectif est de trouver un équilibre entre le risque acceptable et les coûts de sécurisation, puis de faire arbitrer cet équilibre, de manière formelle, par un responsable ou un comité (voir plus loin) qui a autorité pour le faire. L'homologation de sécurité permet à un responsable, en s'appuyant sur l'avis des experts, de s'informer et d'attester aux utilisateurs d'un système d'information que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés.

L'homologation est délivrée par une autorité d'homologation pour un système d'information avant sa mise en service opérationnel. L'homologation permet d'identifier, d'atteindre puis de maintenir un niveau de risque de sécurité acceptable pour le système d'information considéré.

L'homologation peut aussi être initiée et avoir lieu après la mise en fonctionnement du SI.

Se référer à l'annexe en §7.1.1.10 présentant cette disposition

Attention : l'homologation n'est pas conduite par le chef de projet, cependant il doit en comprendre la finalité.

5.2.8.2 Engagement des dirigeants et des métiers

Dans cette logique, il est important de préserver le quotidien des acteurs ne disposant pas de compétences particulières en sécurité, et cependant de les sensibiliser avec l'accord de la direction qui se doit de montrer l'exemple : lors de directives qui peuvent revêtir un caractère impopulaire.

Seul **un engagement au plus haut niveau** garantit la cohérence de ce dispositif et organisation de sécurité.

L'intervention de directions commerciales voire de la direction générale, est focalisée sur la relation client. Cette dernière réclame de traiter avec diligence, tout incident sécurité survenant dans leur périmètre business. Leur participation de suivi sera demandée, tout comme identifier les risques de mécontentement client et suivre les plans d'actions correctifs et d'anticipation proposés à cette fin.

Dans la conduite du changement pour chacun des projets, les dirigeants doivent s'engager en tant que porteur politique dans la mise en place des mesures de sécurité. Cet engagement se met en place naturellement avec la connaissance par le dirigeant des risques au travers de leur pilotage (cf. Homologation), du suivi des incidents avec l'éventuel dépôt de plainte et de la conduite de la stratégie de la sécurité du SI par l'allocation des moyens et le suivi des chantiers de sécurité et de mise en conformité.

Exemple de formalisation de cet engagement : le Comité Stratégique de la SSI porté par l'Autorité Qualifiée (Dirigeant exécutif)

- La stratégie, l'organisation et les moyens financiers et humains sont arbitrés en CoStraSSI en présence des membres de la direction qui sont les commanditaires des projets numériques.
- Il y est présenté les risques, menaces et incidents permettant une acculturation des dirigeants ainsi que la feuille de route des homologations, limitant ainsi le lancement de projet sans la prise en compte de leur sécurisation en amont.
- CoStraSSI, Bureau des projets et homologation permettent de garantir une mise en œuvre structurée, cohérente d'une stratégie numérique garantissant la sécurité, la réduction des risques et donc une mise en qualité, une garantie à mettre en avant lors des partenariats futurs.

5.2.8.3 Sensibilisation des parties prenantes métiers

Ces opérations de sensibilisation ont la particularité d'aller dans les 2 sens : top down + bottom up. Le programme de sensibilisation doit être crédible et convaincant (pas seulement discursif), il s'agit d'un véritable projet (de sensibilisation) mené avec :

- ses attendus, pour lesquels les acteurs ont des leviers, couverture,
- ses KPI : couverture, sensibilité au risque, capacité à agir,
- des enquêtes de compréhension des participants

Voici un exemple de sensibilisation au Système de Management Sécurité, en l'occurrence le plan de la séance de sensibilisation, aligné sur le référentiel ISO27001 :

- Les enjeux d'un SMSI
- L'approche processus
- Les référentiels d'un SMSI
- Le rôle des objectifs, indicateurs, constats, plan d'actions
- Les instances du SMSI et la revue des risques
- Les parties intéressées
- RGPD, Analyse des risques, Déclaration d'applicabilité

Quelques exemples d'utilisateurs Métiers, particulièrement sensibles pour la sécurité :

- Les trésoriers et acteurs comptables

Rappelons la tentative de « fraude au président », qui doit donner lieu à une sensibilisation particulière

- La DSI Maitrise d'œuvre

Une particularité demeure concernant les métiers des systèmes d'information : ils doivent accompagner par leur maîtrise du sujet, tous les acteurs métiers dans la prise en compte des mesures essentielles de sécurité sur la mise en œuvre des nouveaux processus digitaux.

5.2.9 Le cas des prestataires et des fournisseurs

Une catégorie à part concerne les prestataires et les fournisseurs :

- Le processus de sélection et agrément fournisseur doit être particulièrement renforcé en matière de sécurité, dans leur référencement ;
- Un audit sécurité s'avère indispensable à cet effet.

Cet audit doit tout autant s'attacher aux procédures de contrôle sur les produits et services acquis par l'entreprise, que sur le recrutement des prestataires et leur sensibilisation à la sécurité. Effort que l'entreprise ne pourrait consacrer seule à cet effet, en dehors d'un programme global de ses salariés et traitant à la marge ses prestataires.

La gestion des fournisseurs (ou Supplier Management en anglais) doit permettre à l'organisation de pouvoir contractualiser avec ses partenaires dans un contexte transparent en matière de sécurité de l'Information. C'est un élément critique pour les parties prenantes car toute faille peut impacter l'autre et avoir des conséquences business, financières, et/ou réglementaires majeurs. On ne compte plus le nombre d'exemples d'attaques causées par une mauvaise gestion des fournisseurs ces dernières années : **SolarWinds**, **Target** ou **NotPetya**.

- SolarWinds est l'éditeur de logiciel américain proposant des solutions de supervision de réseau informatique, dont la plateforme Orion. En 2020, une mise à jour logicielle de cette plateforme a intégré un code malveillant, susceptible d'accéder aux données échangées sur les réseaux. La cyberattaque semble avoir été une opération d'espionnage, reposant sur ce code malveillant (« backdoor »), qui par ricochet a touché des tiers.
- Target est un groupe de distribution américain, important car le tiers des américains en sont client. En 2013 son système de paiement, provenant d'un prestataire, a fait l'objet d'un piratage (récupération de droits d'administration) causant le vol de données sensibles de plusieurs millions de clients.
- NotPetya : s'il ne s'agit pas d'un exemple de "mauvaise gestion fournisseurs", il s'agissait d'un des vecteurs d'infection en Ukraine. Mais NotPetya est connu pour d'autres vecteurs de propagation et on la retient comme une cyberattaque mondiale (2017), sur la base d'un logiciel malveillant provoquant la destruction de données informatiques.
  https://fr.wikipedia.org/wiki/Cyberattaque_NotPetya

Il est indispensable de prendre en compte que la sous-traitance augmente la surface d'attaque et les fournisseurs deviennent donc une porte d'entrée privilégiée si tous les moyens ne sont pas mis en œuvre pour réduire le risque. Par conséquent, il est primordial de renforcer la gestion des risques liés aux tiers au travers d'audits, de mise en place de clauses de sécurité dans les contrats, ainsi que de réaliser des tests réguliers.

Compte tenu des évolutions technologiques et des attaques les règlementations deviennent de plus en plus exigeantes en matière de gestion des fournisseurs. Ainsi pour renforcer les entreprises et infrastructures critiques européennes **NIS2** et **DORA** vont introduire un cadre règlementaire visant à réduire les risques liés aux tiers et sécuriser la chaine d'approvisionnement. En cas de manquement, les amendes pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial (NIS2), tandis qu'avec DORA le régulateur peut même aller jusqu'à interdire la collaboration avec un fournisseur non conforme.

5.3 INTEGRATION DE LA SECURITE DANS LES PROJETS

5.3.1 Synthèse

Dans la conduite de projet, la prise en compte de la sécurité se fait à **chaque étape du projet et ce dès le début du projet**.

Ainsi elle s'effectue, lors de l'*Expression de besoin*, l'*identification des besoins de sécurité* par les directions métiers, l'*analyse de risque* et l'*application de* ***nouvelles mesures de sécurité*** qui viendront s'additionner à celles déjà en place.

Cette expression de besoin de sécurité permet de **responsabiliser les directions métiers** en termes de risques, de coûts humains et financiers des mesures pour les réduire, l'exposition excessive due à certains choix fonctionnels.

Un équilibre est alors possible entre **objectif métier** et **objectif de sécurité** par le prisme des éventuels impacts d'incidents de cyber sécurité et des risques engendrés, évalués en concertation avec ses directions.

L'expression des besoins et l'identification des objectifs de sécurité pourront être conduites pendant les différentes phases de la conduite de projet en utilisant une méthodologie d'analyse de risques. Ces méthodes d'analyse de risques ont déjà été présentées succinctement dans le chapitre 3. La méthodologie **EBIOS Risk Manager** sera présentée en détail dans un prochain Livre Blanc.

Ainsi, l'intégration de la sécurité en amont des projets[16] se réalise à travers les points suivants :

- Expression de **besoins de sécurité** pendant l'expression de besoins fonctionnels
- **Analyses de risque** adaptées à la sensibilité des données et des traitements[17]
- **Homologation des SI** les plus sensibles, se référer à l'annexe §7.1.1.10

L'organisation de la SSI doit permettre, au travers de spécialistes, la mise en œuvre et son contrôle d'une **politique de sécurité** et d'un ensemble de **mesures de sécurité**. Structurellement transverse, elle s'appuie aussi sur un réseau de **correspondants** dans les directions métiers et les directions techniques.

Elle se dote d'une **chaîne fonctionnelle de la sécurité**. La chaîne fonctionnelle SSI est le lien entre spécialistes de la sécurité et opérationnels techniques ou fonctionnels du SI. Elle permet la **remontée des incidents**, leur qualification et analyse pouvant alimenter une éventuelle cellule de crise ou des tutelles de l'organisation.

Elle permet également l'**application** et le **contrôle des mesures de sécurité** opérationnelles techniques. Elle réalise des audits internes et fait appel à des prestataires qualifiés (PASSI) pour réaliser des audits externes.

Le signalement, la qualification et le traitement des incidents doit permettre d'alimenter la base de connaissances de l'organisation en *scénarii* de menaces, pour les envisager dans les analyses de risque, établir les plans de remédiation, et effectuer les mises à jour pertinentes des analyses de risque déjà réalisées. L'organisation pourra, entre autres, se référer et s'appuyer sur le référentiel **MITRE ATT&CK** comme base de connaissance initiale à destination de ses analyses de risques dans le cadre de ses projets numériques. EBIOS-RM présente un intérêt complémentaire, de haut niveau, qui sera détaillé dans un prochain Livre Blanc.

In fine, la connaissance des risques, de leurs impacts et gravités pour l'ensemble des porteurs de risques, organisations et usagers, les plans de remédiation qui en découlent sont nécessaires à la future gestion de crise pour réduire la **gravité des impacts**. Rappelons que c'est l'objet de l'**Analyse d'Impact relative à la Protection des Données** (AIPD - loi Informatique et libertés - RGPD).

[16] Intégrer la sécurité dans les projets (ANSSI, 2025)
[17] La méthode EBIOS Risk Manager (ANSSI, 2024)

5.3.2 Echelon Projet lors de l'intégration de la sécurité dans les projets

L'échelon **Projet** permet de suivre les groupes de Processus et les principaux Livrables projets préconisés par le PMI®

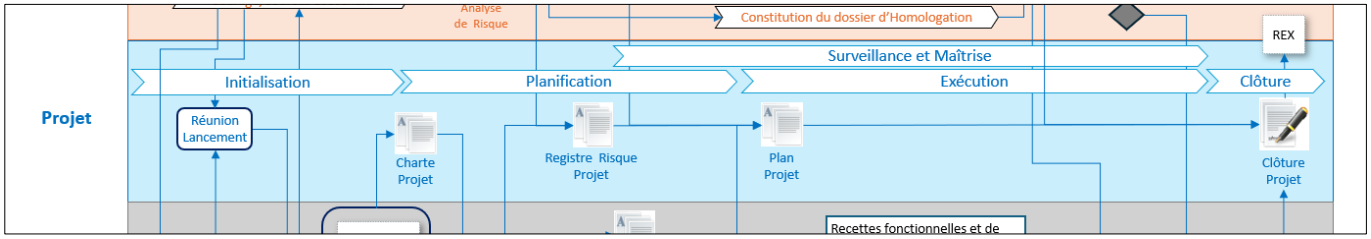


Figure 10 - Processus et livrables PMI

Nous pouvons citer les 5 groupes de processus habituels du PMI® :

1. **Initialisation :** cadrage du projet, en lien avec le cadrage et socle de sécurité de l'analyse de Risque ;
2. **Planification** : dès les premières phases, il est crucial d'intégrer la gestion des risques cyber. Cela comprend l'identification des actifs critiques, l'analyse des menaces potentielles et la définition des exigences de sécurité ;
3. **Exécution** : pendant la mise en œuvre du projet, des mesures de sécurité doivent être appliquées pour protéger les systèmes et les données. Des audits réguliers et des tests de vulnérabilité permettent de s'assurer de l'efficacité des contrôles de sécurité ;
4. **Surveillance et Maîtrise** : une fois le projet opérationnel, la surveillance continue des systèmes et la détection des incidents de sécurité sont essentielles. Des plans de réponse aux incidents doivent être mis en place pour gérer efficacement les situations critiques ;
5. **Clôture** : à la fin du projet, il est important de prendre des mesures pour assurer la sécurité des données et des systèmes, même après la fin de leur utilisation. Cela peut inclure la suppression sécurisée des données, la désactivation des systèmes et la mise à jour des politiques de sécurité.

Et également les principaux livrables Projet :

- La charte de projet ;
- Le registre des risques ;
- Le plan de management de projet ;
- La clôture de projet.

Cette liste n'est bien évidemment pas exhaustive, on pourrait y ajouter les **parties prenantes** par exemple.

Dans un contexte de projet agile, on s'appuiera sur des notions d'EPIC et d'itérations.

5.3.3 Guide de l'ANSSI

Le guide de l'ANSSI "AGILITE & SECURITE NUMERIQUES - Méthode et outils à l'usage des équipes projet"[18] est une autre source complémentaire et très pertinente.

Compte tenu de la nécessité de sécuriser le système d'information, il est aujourd'hui impératif de s'orienter vers l'intégration de la Sécurité dans les Projets (ISP) pour toute nouvelle initiative projet.

L'intégration de la sécurité dans les projets permet la prise en compte des contraintes liées à la cybersécurité durant tout le cycle de vie du projet.

[18] Agilité & Sécurité Numériques (ANSSI, 2018)

5.4 ANALYSES DES RISQUES DE CYBERSECURITE

Dans les phases d'analyses techniques des éventuels *scenarii* d'attaque du SI considéré, le chef de projet devra s'appuyer sur des experts en cybersécurité et sur la connaissance fine du RSSI des vulnérabilités et des incidents de l'ensemble du système d'information de l'organisation. La connaissance et le traitement des incidents sont centraux à l'évolution des mesures de sécurité.

On comprend naturellement, comme pour n'importe quelle technologie, d'énergie ou de transport, au service et impliquant des personnes et des organisations, qu'intégrer la sécurité dans les projets implique la gouvernance, les directions métiers, la direction technologique et les experts en sécurité de l'organisation. Cela vaut donc également pour le numérique et les systèmes d'information.

5.4.1 La gestion des risques

Le chef de projet est le garant de l'intégration de la sécurité dans les projets. C'est à lui de s'assurer que tous les acteurs de la sécurité connaissent leurs rôles et leurs responsabilités dans toutes les phases du projet. Il doit pouvoir faire appliquer les processus liés à la sécurité et alerter en cas de déviation, en interaction avec les acteurs de la sécurité. Un de ces processus est notamment la démarche de gestion des risques.

Ce qui réclame une sensibilisation du chef de projet aux risques cyber.

Ces aspects seront développés ultérieurement dans un prochain Livre Blanc.

5.4.2 De l'identification à l'évaluation du risque

Dans le cadre d'un projet, l'analyse de risques doit arriver en amont afin de pouvoir cibler au plus tôt les risques liés à la sécurité et proposer un plan de traitement des risques actionnable aux décideurs. Cette démarche s'inscrit parfois dans ce que l'ANSSI appelle l'homologation de sécurité d'un système d'information. Elle met en lumière les risques liés à l'exploitation d'un SI et décline les mesures de sécurité à mettre en place avant son déploiement. Plus l'appréciation du risque se fait tôt, plus les exigences de sécurité vont être ciblées dans le cahier des charges du projet et des phases de développement.

Selon l'ISO27005, l'appréciation d'un risque se découpe en 3 phases :

- L'identification du risque ;
- L'analyse du risque ;
- L'évaluation du risque.

L'identification du risque démarre avant tout par le ciblage du ou des objets de risque. Moyennant l'attribution de sa responsabilité, qui n'est probablement pas le chef de projet, le gestionnaire du risque devra se poser la question de ce que l'on cherche à protéger ? En fonction des 4 critères de sécurité DICP (ou DICT):

- Disponibilité ;
- Intégrité ;
- Confidentialité ;
- Preuve (Traçabilité).

Qu'elle soit quantitative ou qualitative, l'évaluation du risque consiste à étudier l'impact et la probabilité d'un risque qui donnera lieu à un niveau de criticité. Le niveau d'impact et de probabilité d'occurrence sera évalué par les sachants en fonction des besoins de sécurité et du contexte associé à l'objet de risque.

Dans cette étape, il s'agira de lister les scénarios pertinents couplés aux menaces, vulnérabilités et actifs associés et donner un niveau d'impact puis évaluer la probabilité que ce scénario ait lieu.

Les scénarios de risques qui présentent la criticité la plus élevée seront à prioriser. Le niveau de risque (ou criticité) est évalué à partir de la probabilité qu'un incident ne se déclenche et les impacts liés à cet incident. Les risques sont alors présentés dans une matrice de risques. La classification des risques se fait par ordre d'importance afin d'accompagner la prise de décision dans la phase de traitement des risques.

Dans tous les cas il s'agira d'identifier les risques les plus pertinents, leur vraisemblance et les conséquences associées à un impact élevé

A l'issue, il est important de s'assurer de la pertinence des risques ainsi que de la conformité vis-à-vis des exigences organisationnelles, réglementaires/légales ou contractuelles.

Rôle du Chef de Projet :

- S'assurer que les risques sont identifiés en amont ;
- Revue de sécurité et réévaluation du risque à chaque étape du projet.

5.4.3 Traiter et répondre aux risques

Le traitement d'un risque reste lié à l'appétence au risque des individus et des parties prenantes, ainsi qu'à la culture de l'organisation.

Traiter le risque signifie tout simplement agir ou non sur celui-ci. Il existe 4 grandes catégories de traitement du risque :

- La réduction ;
- L'évitement ;
- L'acceptation ou le maintien ;
- Le transfert ou le partage.

Celles-ci vont permettre de définir ensuite un plan d'action ainsi que l'identification de risques résiduels.

La mise en œuvre du traitement d'un risque passe par l'élaboration d'un plan de traitement. Ce dernier priorise l'ensemble des actions à mener dans le cadre du traitement des risques en identifiant les responsables de chaque action et suggère une planification claire.

Une fois traité le risque devient résiduel et doit être accepté par les décideurs. En cas de rejet, un retour à l'étape d'évaluation et de traitement est nécessaire. Il est conseillé ici de redéfinir les besoins et objectifs en matière de sécurité afin d'assurer un plan de traitement des risques en phase avec les objectifs de l'organisation.

La direction, en tant que sponsor des projets, doit disposer d'une vision claire des risques résiduels et de la feuille de route qui en découle afin de pouvoir décider dans un environnement dont les risques sont connus et maitrisés.

Rôle du Chef de Projet :

- Suivi du plan d'action et de la feuille de route ;
- Définition et suivi des KPIs pour s'assurer que les objectifs de sécurité soient atteints ;
- Sensibilisation sécurité des collaborateurs du projet ;
- Prise en compte de l'impact sur le Cadre Juridique ;
- Supervision sécurité (vérification de cette tâche)

.

6 Conclusion

Ce premier Livre Blanc sur les « Projets et la Cybersécurité » avait pour ambition, pour le chef de projet, de dresser à la fois le panorama de l'Ecosystème à connaitre et de détailler la Gouvernance de la sécurité de l'information.

En effet, il est crucial pour le Chef de Projet de pouvoir se situer au sein de l'entreprise et d'identifier les acteurs de la Sécurité avec qui il sera en interaction afin de mener à bien ses différents projets.

La Gouvernance de la sécurité de l'information doit être bien comprise par tous les acteurs et bien sûr par le COMEX afin que la responsabilité du risque de sécurité de l'information soit effectivement portée au bon niveau.

Ultérieurement, nous vous donnons rendez-vous pour des nouveaux Livres Blancs sur le thème « Projets et Cybersécurité » afin d'explorer ensemble, à minima, les points suivants :

- Comment les directions Métiers identifient les risques par une démarche d'**intégration de la sécurité** dans les projets ;
- Comment les experts techniques qualifient les risques avec une **vision transversale** "technique-métier-sectoriel».

Le rôle du Chef de Projet sera, là encore, très important. Il sera naturellement une Partie Prenante clé de ces deux approches.

7 Annexes

7.1 DETAIL DES REGLEMENTATIONS, NORMES, REFERENTIELS ET ORGANISATIONS

Ces parties descriptives sont utiles à connaître selon le projet que vous menez. Leur descriptif a été évoqué sommairement dans le corps du livre blanc.

7.1.1 Réglementations

Cette partie reprend le détail des réglementations, résumées dans deux tableaux en §3.2

7.1.1.1 NIS1

La **directive NIS1** (Network and Information Systems Directive) de l'Union Européenne (UE), adoptée en juillet 2016, marque une étape importante dans l'amélioration de la cybersécurité à travers l'UE. Elle vise à établir un cadre commun pour les États membres afin de garantir un niveau élevé de sécurité des réseaux et des systèmes d'information.

L'objectif principal de la directive NIS1 est d'améliorer la sécurité des réseaux et des systèmes d'information au sein de l'Union européenne pour protéger les infrastructures critiques et les services essentiels contre les cyberattaques et autres incidents de sécurité. Cela comprend la prévention, la détection, la gestion des incidents, et la résilience face aux cybermenaces.

Cette norme européenne contraint les États membres à suivre et appliquer diverses obligations. D'abord, ils doivent élaborer une stratégie nationale pour assurer un niveau élevé de sécurité des réseaux et des systèmes d'information. De plus, ils ont l'obligation de créer des équipes de **réponse aux incidents de sécurité informatique** (Computer Security Incident Response Teams) pour surveiller, détecter et répondre aux incidents de sécurité.

Enfin, d'un point de vue stratégique, un groupe de personnes est établi pour soutenir et faciliter la coopération stratégique et l'échange d'informations entre les États membres. Et d'un point de vue opérationnel un réseau de **CSIRT**[19] est créé pour promouvoir une coopération opérationnelle rapide et efficace.

7.1.1.2 NIS2

La **directive NIS2** s'appuie sur la directive de 2016 sur les réseaux et les systèmes d'information (NIS) et en élargit le champ d'application. Adoptée en **2022**, elle vise à renforcer et à harmoniser les capacités de cybersécurité dans l'UE et à atténuer les menaces qui pèsent sur les réseaux et les systèmes d'information utilisés pour certaines entités désignées : les OIV (opérateur d'importance vitale), OSE (opérateur de services essentiels) et les entités concernées auraient dû être conforme à NIS2 depuis le 17 octobre 2024 [20].

Le non-respect de la directive NIS2 peut avoir de graves conséquences, notamment des sanctions financières et une atteinte à la réputation.

NIS2 vise à protéger un plus grand nombre d'organisations et d'infrastructures critiques de l'UE contre les cybermenaces. En plus des secteurs déjà couverts par la NIS1, la NIS2 inclut les services publics, pour couvrir plus d'infrastructures critiques comme les réseaux de distribution de l'eau, les services de communication électroniques, les entités offrant des services de certification pour les transactions numériques et les entreprises de recherche scientifique.

[19] CSIRT: Computer Security Incident Response Team

[20] il s'agissait de la date limite donnée par l'UE pour la transposition du texte ; le texte n'est pas encore voté au Parlement ; de plus, l'ANSSI a déclaré lors des auditions qu'elle accordera 3 années aux entreprises pour se mettre en conformité.

Elle comprend des mesures telles qu'un nouveau régime de surveillance et d'application, un nouveau cadre de divulgation des vulnérabilités, des dispositions relatives à la sécurité de la chaîne d'approvisionnement des technologies de l'information et de la communication (TIC), ainsi que des obligations en matière de gestion des risques et de rapports pour plusieurs secteurs, notamment l'énergie, les transports et les télécommunications.

Pour améliorer le niveau actuel de la cybersécurité, des pratiques et politiques cybernétiques sont mises en place, dont la nécessité de signaler, aux autorités compétentes, les cybers incidents importants dans les 24 heures suivant leur découverte.

La NIS2 introduit des responsabilités spécifiques pour le personnel décisionnaire des entités couvertes, y compris des sanctions en cas de manquement. De plus, elle met l'accent sur la coopération et l'échange d'informations *via* le groupe de coopération et le réseau CSIRT.

Pour garantir une conformité stricte dans son organisation, il faudra adapter un suivi interne de la transposition dans chaque pays européen.

NIS1	versus	NIS2
Comment la nouvelle directive NIS étend sa couverture		

Directive (UE) 2016/1148 Directive sur la sécurité des réseaux et systèmes d'information		versus	Directive NIS2	
	Ne couvrait que les services essentiels et les fournisseurs de services numériques		Couvre de façon significative davantage de secteurs, de taille d'entreprise, et d'industries	
2016	Sanctions variables appliquées par les autorités nationales compétentes et les équipes de réponse aux incidents de sécurité informatique (CSIRT)		Des amendes peuvent aller de 10 millions d'euro, à 2% du chiffre d'affaire mondial annuel. La responsabilité juridique des cadres dirigeants peut être engagée.	2024
	Règles générales en matière de déclaration		Attentes strictes et spécifiques en matière de reporting	

Figure 11 - NIS1 vs NIS2

7.1.1.3 RGPD, le règlement général sur la protection des données

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne (UE). Il est entré en application le 25 mai 2018[21].

Le RGPD s'inscrit dans la continuité de la loi française « Informatique et Libertés » de 1978, modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles, établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Il a été conçu autour de trois objectifs :

- Renforcer les droits des personnes ;
- Responsabiliser les acteurs traitant des données ;
- **Crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données.

[21] RGPD (Ministère de l'Economie et des Finances, 2023)

Données personnelles : de quoi parle-t-on ?

Une **donnée à caractère personnel (ou « donnée personnelle »)** est décrite par la Commission nationale de l'informatique et des libertés (CNIL) comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Il existe deux types d'identification :

- Identification **directe** (nom, prénom, etc.) ;
- Identification **indirecte** (identifiant, numéro, etc.).

Lorsqu'une opération ou un ensemble d'opérations portant sur des données personnelles sont effectuées, on considère qu'il s'agit de **traitement de données personnelles**. La CNIL donne les actions suivantes à titre d'exemple du traitement des données :

- Tenue d'un fichier de ses clients ;
- Collecte de coordonnées de prospects via un questionnaire ;
- Mise à jour d'un fichier de fournisseurs.

La commission européenne a pris plusieurs décisions d'adéquation qui permet d'échanger les données vers un pays tiers « adéquat » alors considéré comme offrant un niveau de protection approprié et donc assimilé comme un échange au sein de l'UE.

À ce jour, 14 pays bénéficient d'une décision d'adéquation ou adéquation partielle :

- Andorre ;
- Argentine ;
- Canada uniquement pour autrement dit les traitements "commerciaux" ;
- Les îles Féroé ;
- Guernesey ;
- Israël ;
- L'île de Man ;
- Japon ;
- Jersey ;
- Nouvelle-Zélande ;
- Suisse ;
- Uruguay ;
- Corée du Sud ;
- Royaume-Uni.

Les États-Unis restent un cas particulier, même si en juillet 2024 la commission européenne a validé un nouveau système sous condition que le prestataire se trouve dans la liste du site du Département du Commerce des Etats-Unis. Cet accord limite l'accès aux données des européens par les renseignements US et permet de former un recours auprès du "**Civil Liberties Protection Officer**" (CLPO) en cas de préjudice. L'impact du RGPD sur les projets sera plus étoffé dans notre prochain livre blanc.

7.1.1.4 DORA

La loi **DORA** (**Digital Operational Resilience Act**) est une réglementation **européenne** adoptée pour renforcer la résilience opérationnelle numérique des **entités financières** dans l'Union européenne (AMF, 2024). DORA est en partie un règlement d'application directe (fait le **17 janvier 2025)**, et en partie une directive, à transposer en droit national (fait par le parlement français dans le même texte que NIS2).

DORA vise à garantir que les institutions financières disposent de capacités suffisantes pour gérer et surmonter les cyberattaques et autres perturbations numériques. Grâce à un cadre de gouvernance et de contrôle interne spécifique, elle vient renforcer l'existant : **ISO27001,** ou encore **NIS2**.

L'objectif de renforcement de la résilience opérationnelle numérique est réalisé grâce aux cinq principaux piliers de DORA :

Gestion des risques liés aux TIC	Ensemble de principes et d'exigences clés concernant le cadre de gestion des risques liés aux TIC	Chapitre II, Articles 5 à 16
Gestion, classification et déclaration des incidents liés aux TIC	Harmoniser et rationaliser la notification, étendre les obligations de notification à toutes les entités financières et élargie le champ des incidents à notifier	Chapitre III, Articles 17 à 23
Tests de résilience opérationnelle numérique	Soumettre les entités financières à des tets de base ou à des tests avancés (par exemple TLPT)	Chapitre IV, Articles 24 à 27
Gestion des risques liés aux prestataires tiers de services TIC	Règles pour la surveillance des risques liés aux prestataires tiers, dispositions contractuelles essentielles et cadre de surveillance pour les prestataires tiers critiques de services TIC (CTTP)	Chapitre V, Articles 28 à 44
Echange d'informations	Echange volontaire d'informations et de renseignements sur les cybermenaces	Chapitre VI, Article 45

Figure 12 - les 5 piliers de DORA

À l'image de **NIS2**, ses objectifs principaux sont de **renforcer la résilience numérique**, harmoniser les règles au sein de l'UE, garantir la protection des clients des entités financières et des investisseurs contre les retombées des perturbations numériques et renforcer les capacités de surveillance et de gestion des risques numériques par les autorités de réglementation.

7.1.1.5 Cyber Resilience Act

Le règlement sur la cyber-résilience (**CRA**) renforce les normes de cybersécurité des produits qui contiennent un composant numérique, exigeant des fabricants et des détaillants qu'ils garantissent la cybersécurité tout au long du cycle de vie de leurs produits.

Le CRA vise à protéger les consommateurs et les entreprises qui achètent des produits logiciels ou matériels comportant un composant numérique.

Deux objectifs principaux ont été identifiés pour assurer le bon fonctionnement du marché intérieur :

1. Créer les conditions pour le développement de produits sécurisés avec des éléments numériques en veillant à ce que les produits matériel/logiciel soient mis sur le marché avec moins de vulnérabilités et en veillant à ce que les fabricants prennent la sécurité au sérieux tout au long du cycle de vie d'un produit ;
2. Créer les conditions permettant aux utilisateurs de prendre en compte la cybersécurité lors de la sélection et de l'utilisation de produits comportant des éléments numériques.

Quatre objectifs spécifiques ont été fixés :

1. Veiller à ce que les fabricants améliorent la sécurité des produits comportant des éléments numériques dès la phase de conception et de développement et tout au long du cycle de vie ;
2. Assurer un cadre de cybersécurité cohérent facilitant la conformité des producteurs de matériel et de logiciel ;
3. Améliorer la transparence des propriétés de sécurité des produits avec des éléments numériques ;
4. Permettre aux entreprises et aux consommateurs d'utiliser des produits comportant des éléments numériques en toute sécurité.

L'amélioration du niveau de cybersécurité des produits comportant des éléments numériques faciliterait le respect des obligations par les entités relevant du champ d'application de la directive NIS 2 et renforcerait la sécurité de l'ensemble de la chaîne d'approvisionnement.

Le règlement sur la cyber-résilience est entré en vigueur le **10 décembre 2024**. Les principales obligations introduites par le CRA s'appliqueront à partir du 11 décembre 2027.

7.1.1.6 Cybersecurity Act

Règlement européen « Cybersecurity Act » relatif à l'**ENISA** (**European Union Agency for Cybersecurity)** et à la certification de cybersécurité des technologies de l'information et des communications.

Publié en juin 2019, le **Cyber security Act** donne à l'ENISA un mandat permanent et fixe ses rôles et responsabilités d'acteur majeur de la sécurité pour les Etats membres de l'UE. Cet acte juridique va imposer un cadre européen de certification en cybersécurité en établissant la gouvernance et les règles pour la certification à l'échelle de l'UE des produits, processus et services des technologies de l'information et de la communication (TIC).

L'ANCC (Agence Nationale de Certification de Cybersécurité) va voir le jour dans chaque Etat membre – en France c'est l'**ANSSI** qui sera désignée comme telle. L'ENISA définit les schémas et les méthodologies de certifications des produits TIC, à charge aux ANCC d'évaluer ces produits et de délivrer les certifications associées.

7.1.1.7 IA Act

Le règlement européen sur l'IA (RIA) est entré en vigueur le 1er août 2024 et encadre le développement, la commercialisation et l'utilisation de l'IA.

Suivant une approche par les risques, le RIA va classer les IA en 4 niveaux :

- Risque inacceptable – interdiction totale car ayant un fort impact sur les droits fondamentaux et est contraire aux valeurs de l'UE ;
- Haut risque – si l'IA porte atteinte à la sécurité des personnes ou à leurs droits fondamentaux, des exigences renforcées seront attendues (Le RIA propose une liste de ces systèmes dans ses annexes I et III. Ex : systèmes biométriques) ;
- Risque spécifique en matière de transparence – en cas de manipulation des populations (Ex: chatbots) ;
- Risque minimal – aucune obligation supplémentaire.

L'entrée en application est prévue de manière échelonnée :

- 2 février 2025 : interdiction des IA évaluée à un niveau de risque inacceptable ;
- 2 août 2025 : application des règles pour les modèles d'IA à usage général et nomination des autorités compétentes ;
- 2 août 2026 : les dispositions du RIA deviennent applicables.

Ce nouvel Act va également augmenter le niveau d'exigence des systèmes utilisant de l'IA traitant des données à caractère personnel. En effet, il faudra appliquer les obligations du RGPD (réalisation d'une AIPD) mais aussi l'analyse d'impact sur les droits fondamentaux comme le suggère le RIA.

7.1.1.8 National : la LPM

La Loi de Programmation Militaire (LPM) en France est un cadre législatif qui détermine les orientations[22], les priorités et les budgets des forces armées françaises sur une période pluriannuelle. Son objectif principal est de garantir la sécurité nationale et de préparer les forces armées aux défis futurs.

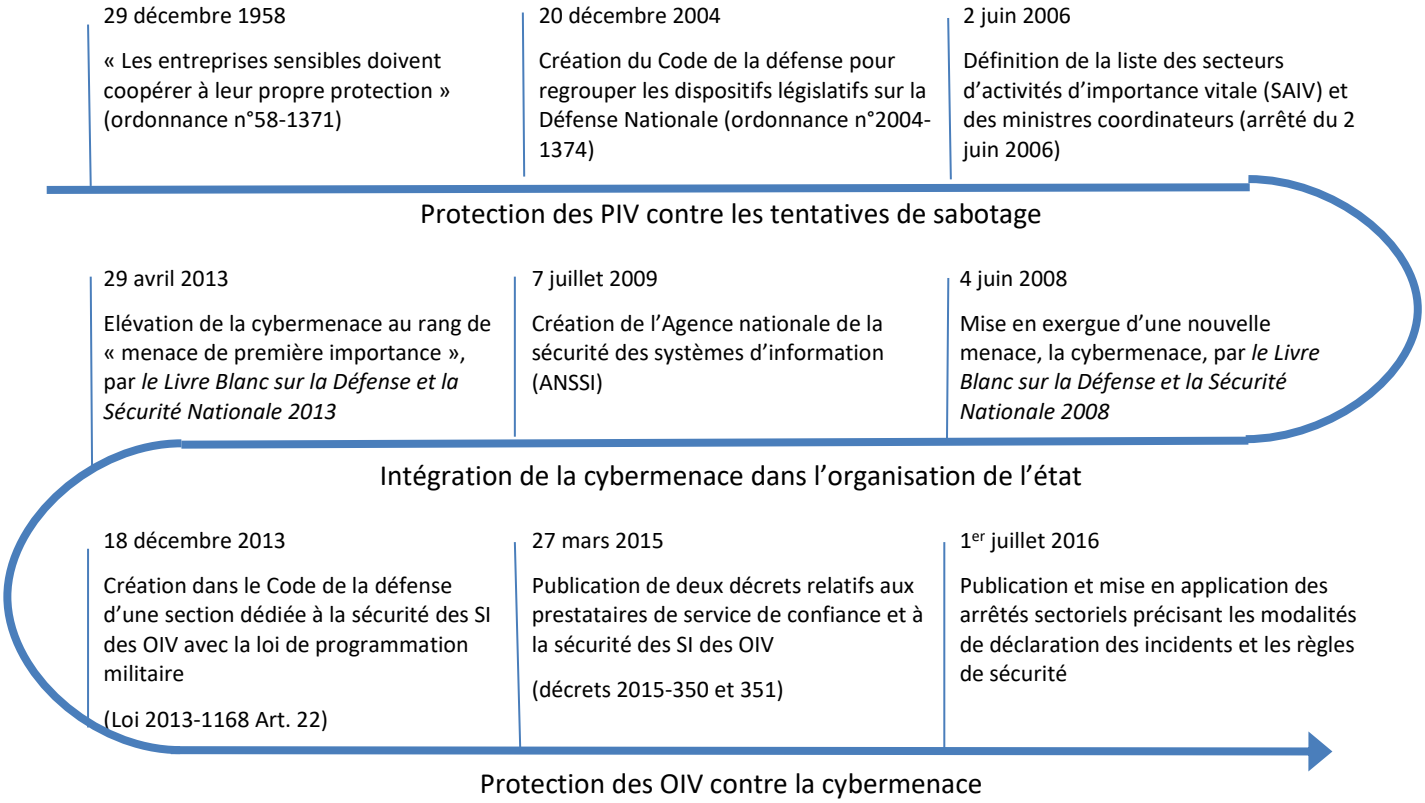


Figure 13 - la LPM

La LPM vise à renforcer la défense nationale pour protéger le territoire national, ses citoyens et ses intérêts. Le législateur vote cette LPM et attribue les fonds qui permettront, sur une période de 10 ans, à moderniser les équipements militaires, améliorer la préparation des forces et renforcer la cybersécurité en intégrant des mesures pour protéger les infrastructures critiques et les systèmes d'information contre les cyberattaques.

Du point de vue cybersécurité et cyberdéfense, la LPM renforce la protection des infrastructures numériques et développe des capacités offensives et défensives en matière de cyberdéfense.

Le volet cyber de cette loi décline des stratégies et des postures de cyberdéfense présentées largement dans le livre Blanc de Défense et de la Sécurité 2013, déjà bien présentes dans celui de 2008.

La continuité et résilience des services « essentiels et indispensables » (se référer à la définition de la cyberdéfense en §2.3) au fonctionnement de notre pays sont donc au cœur de la loi.

La notion d'**O**pérateur d'**I**mportance **V**itale déjà existante dans cet enjeu de continuité des services pourrait être assimilée à la « cyber continuité » de l'état.

[22] Orientation de la LPM (Ministère des Armées, 2023)

12 secteurs d'activités d'importance vitale **(SAIV)** ont été définis pour protéger les opérateurs jugés indispensables à la survie de la nation contre les actes malveillants. Ces opérateurs (publics ou privés) identifiés sont nommés des « opérateurs d'importance vitale » (**OIV**). La liste est couverte par le secret de la défense nationale.

Charges ensuite aux OIV de déclarer leurs systèmes d'information d'importante vitale (SIIV), c'est-à-dire les systèmes les plus critiques pour lesquels une attaque avérée aurait une conséquence grave sur la nation.

L'ANSSI a définit les règles techniques et organisationnelles de sécurité des systèmes d'information devant être appliquées par l'opérateur à ses SIIV. Elles sont au nombre de 20 déclinées en 5 thématiques [23]. Les exigences sont définies dans des arrêtés sectoriels.

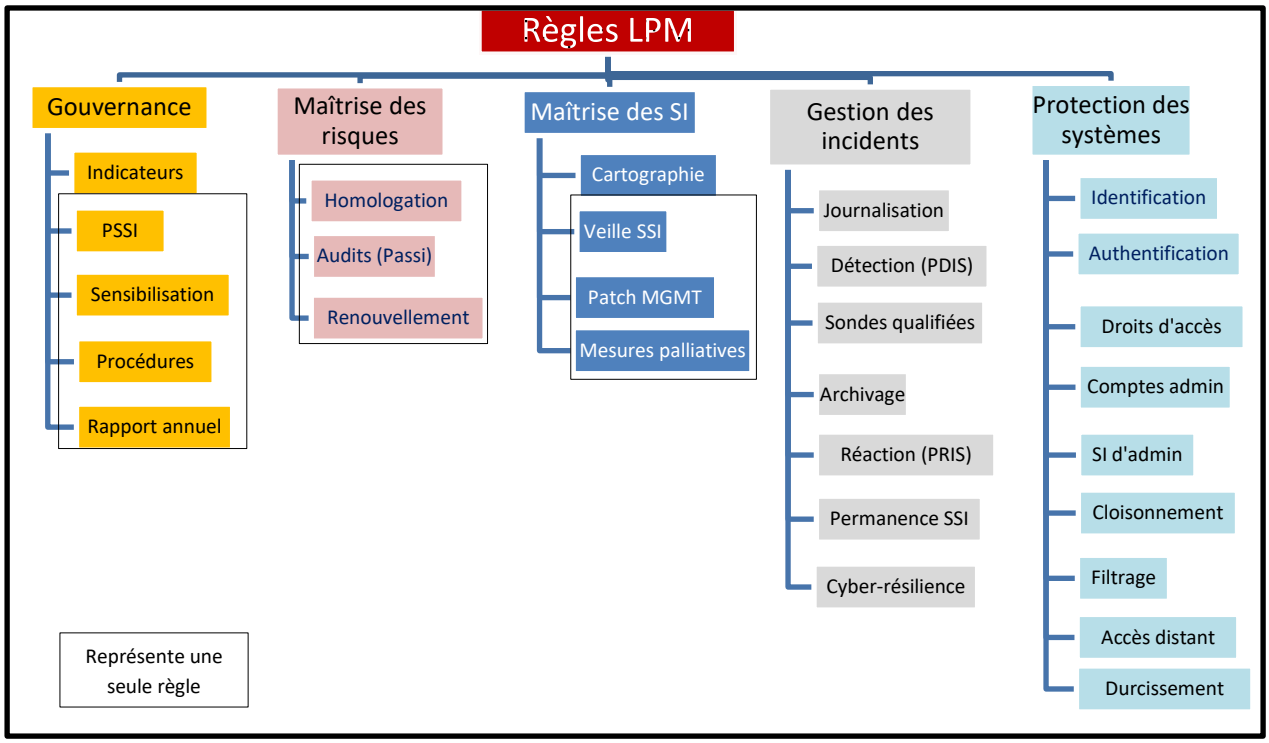


Figure 14 - Les 20 règles applicables aux SIIV

À noter que les prestataires qui participent à la sécurité ou au fonctionnement des systèmes d'information d'importance vitale seront soumis aux obligations prévues par la LPM à travers leurs contrats avec les opérateurs d'importance vitale.

L'ANSSI peut déclencher des contrôles de sécurité pour évaluer le niveau de sécurité des OIV et en cas de non-conformité, outre l'exposition aux menaces des SIIV, peut entrainer en dernier recours des sanctions financières pour l'organisme et son dirigeant.

La Loi de Programmation Militaire est essentielle pour assurer la planification à long terme des forces armées françaises. En définissant des priorités claires, en allouant des ressources appropriées et en mettant en place des mécanismes de suivi rigoureux, la LPM permet à la France de maintenir une force militaire capable de répondre aux menaces actuelles et futures[24].

[23] Règles de sécurité sur SIIV (ANSSI, 2022)
[24] Code de la cybersécurité, publié chez Dalloz (ANSSI, 2024)

7.1.1.9 Protection de la vie privée

La protection de la vie privée est un droit humain fondamental, de plus en plus protégé par des obligations de conformité dans le monde entier, et notamment par des réglementations relatives à la confidentialité des données dans le domaine de la cybersécurité.

Il a déjà été abordé dans les réglementations européenne le RGPD relative aux DPI (données personnelles d'identification – PII en anglais) mais il en existe plusieurs dans le monde[25].

Fin 2020, 106 pays disposaient d'une réglementation nationale (dont beaucoup s'inspirent du RGPD qui reste une norme d'excellence et une des plus stricte) sur la protection des données personnelles s'appliquant à tous les secteurs d'activité.

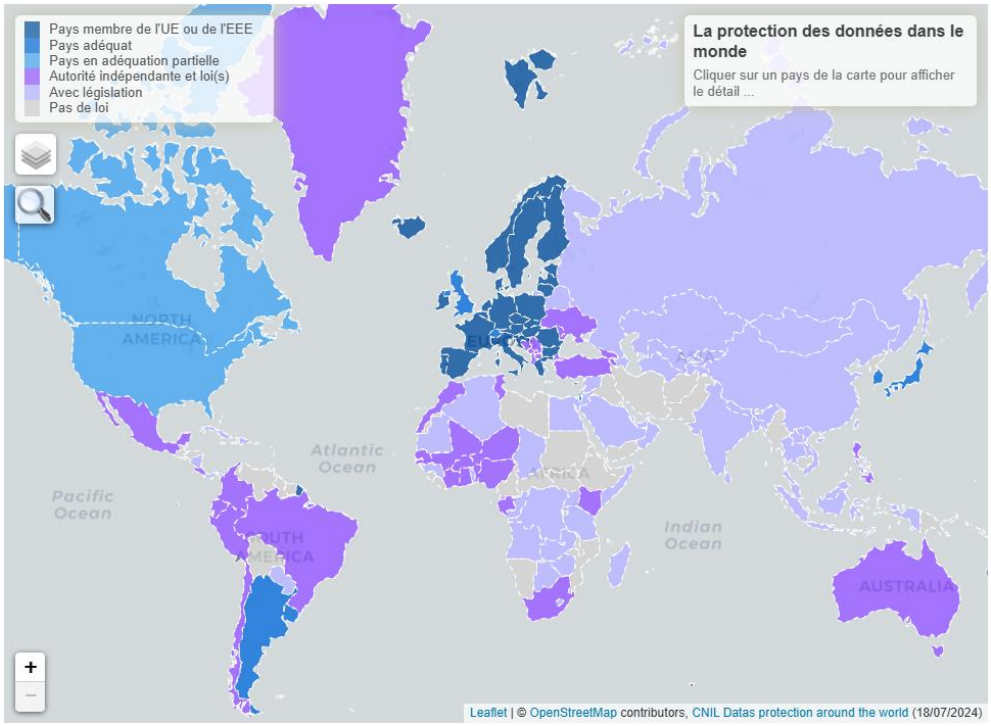


Figure 15 - Planisphère des législations spécifiques de protection des données personnelles.

Source carte : CNIL : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Les entreprises et les plateformes doivent se conformer aux réglementations nationales et locales en matière de confidentialité (notamment la CCPA aux États-Unis et la PDPA en Australie) partout où leurs produits et services sont accessibles aux utilisateurs.

[25] La protection des données dans le monde (CNIL, s.d.)

Figure 16 - Panorama des réglementations de protection de la vie privée (non exhaustif)

Il existe également des réglementations sectorielles de protection des données personnelles, notamment pour les données de santé.

Pour exemple, la loi américaine HIPAA (***Health Insurance Portability and Accountability Act***) de 1996 qui établit les exigences de sécurité et de confidentialité des données pour les organismes chargés de sauvegarder les données de santé protégées des patients.

En France, il existe également la certification **HDS**[26], pour les hébergeurs de données de santé, qui s'appuie sur la certification ISO/IEC 27001 pour répondre aux enjeux de sécurité des données et est agrémentée d'exigences additionnelles en lien avec le Règlement Général sur la Protection des Données personnelles (RGPD) et le domaine de la santé. Les exigences issues de la norme ISO/IEC 27001 représentent environ 80% des exigences applicables de la certification HDS. Cette certification donne lieu à l'émission de 2 certificats : un certificat ISO/IEC 27001 et un certificat HDS.

[26] HDS : Hébergeurs de Données de Santé (Agence du Numérique en Santé , 2024)

7.1.1.10 Homologation de sécurité des SI de l'état

Une réglementation a été instaurée pour harmoniser la protection des systèmes d'information publics.

Il s'agit du Décret **n° 2022-513 du 8 avril 2022** relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics, les infrastructures et services logiciels informatiques qui, à la date d'entrée en vigueur du présent décret, composent le système d'information et de communication de l'Etat [...] font l'objet de l'homologation de sécurité prévue à l'article 4-3 du même décret **dans un délai de deux ans** à compter de cette date.

Elle s'appuie sur les travaux de l'ANSSI[27], présentés dans le document suivant :

Figure 17 - Homologation selon ANSSI

7.1.2 Détail des normes internationales applicables en 2024-2025

Cette partie reprend le détail des normes, dont la description est résumée dans un tableau en §3.3

[27] Homologation de sécurité (ANSSI, 2025)

7.1.2.1 Norme IT: ISO/IEC 2700x

Les normes ISO (Organisation internationale de normalisation) relatives à la sécurité de l'information forment une suite sous le nom ISO/IEC 27000. Ces normes fournissent des lignes directrices et des bonnes pratiques pour la gestion de la sécurité de l'information au sein des organisations. La suite ISO/IEC 27000 est utilisée pour protéger les informations sensibles, garantir la confidentialité, l'intégrité et la disponibilité des données.

ISO/IEC 27001:2022

- Sécurité de l'information, cybersécurité et protection de la vie privée
- Systèmes de management de la sécurité de l'information
- **Exigences**

ISO/IEC 27001:2022 /Amd1:2024

- Sécurité de l'information, cybersécurité et protection de la vie privée
- Systèmes de management de la sécurité de l'information
- **Exigences**
- Amendement 1 : actions relatives aux changements climatiques

ISO/IEC 27005:2022

- Sécurité de l'information, cybersécurité et protection de la vie privée
- Préconisations pour la gestion des risques liés à la sécurité de l'information

Voici quelques composantes clés de la suite ISO/IEC 27000 :

1. La norme ISO/IEC 27001 :2022 spécifie les **exigences** pour établir, mettre en œuvre, maintenir et améliorer un **Système de Management de la Sécurité de l'Information** (SMSI). Elle inclut des exigences pour l'évaluation et le traitement des risques sécurité de l'information adaptés aux besoins de l'organisation ;
    - Elle vise à aider les organisations à protéger leurs informations de manière systématique et rentable, grâce à l'adoption d'un système de gestion de la sécurité de l'information (SGSI),
    - Cette certification est un parcours et non une destination : elle est valable trois ans et le SMSI doit être géré et maintenu pendant toute cette période,
    - La norme ISO27001 vise à protéger la confidentialité, l'intégrité et la disponibilité des informations au sein de l'entreprise, en tenant compte des personnes, des processus et de la technologie,
2. La norme ISO/IEC 27002 fournit des **lignes directrices** pour les mesures de sécurité de l'information basées sur les meilleures pratiques de gestion des risques. Elle couvre des domaines tels que les politiques de sécurité, la sécurité des ressources humaines, la gestion des actifs, le contrôle d'accès, la cryptographie, et la sécurité des opérations ;
3. La norme ISO/IEC 27005 fournit des **lignes directrices** pour la gestion des risques de sécurité de l'information. Elle propose une méthodologie pour identifier les actifs, les menaces, les vulnérabilités et les impacts potentiels afin de traiter les risques de manière efficace.

Enfin, la suite ISO/IEC 27000[28] est un cadre essentiel pour la gestion de la sécurité de l'information, offrant des **normes** et des **lignes directrices** complètes pour protéger les informations sensibles.

Tableau 1 : Famille des normes ISO/IEC 27000

Vocabulaire	**ISO/IEC 27000** Vue d'ensemble et vocabulaire				
Exigences	**ISO/IEC 27006** Organismes d'audit et de certification des SMSI		**ISO/IEC 27001** Système de management de la sécurité de l'information		**ISO/IEC 27701** Système de management de la protection de la vie privée
Lignes directrices	**ISO/IEC 27002** Mesures de sécurité de l'information	**ISO/IEC 27003** Orientations du SMSI	**ISO/IEC 27004** Surveillance, mesurage, analyse et évaluation	**ISO/IEC 27005** Gestion des risques liés à la sécurité de l'information	**Directives d'audit des normes ISO/IEC 27007 et ISO/IEC 2708x** Lignes directrices pour l'audit du SMSI et évaluation des mesures de sécurité de l'information
Lignes directrices propres à chaque secteur d'activité	**ISO/IEC 27011** Organismes de télécommunication		**ISO/IEC 27799** Systèmes informatiques pour la santé		Autres normes de la famille ISO/IEC 27000

La mise en œuvre de la norme ISO/IEC 27001 aborde l'article 32 du RGPD. En outre la norme ISO/IEC 27001 et le RGPD se recoupent dans plusieurs domaines, tels que la confidentialité, la disponibilité et l'intégrité des données, ainsi que l'évaluation du risque, etc.

7.1.2.2 Norme IT: ISO/IEC 22301

ISO 22301 est la Norme internationale pour les systèmes de management de la continuité d'activité (SMCA). Elle fournit aux organisations un cadre de référence pour planifier, établir, mettre en œuvre, exploiter, surveiller, passer en revue, maintenir et améliorer en continu un système de management documenté afin de leur permettre de se protéger contre les perturbations, d'en réduire la probabilité et de s'assurer qu'elles sont en mesure de se rétablir.

7.1.2.3 Norme IT: ISO/IEC 31000

ISO 31000 est une Norme internationale qui fournit des principes et des lignes directrices pour le **management du risque**. Elle propose une approche globale pour identifier, analyser, évaluer, traiter et surveiller les risques au sein d'un organisme et communiquer sur ces derniers.

7.1.2.4 Norme OT : IEC 62443

La norme IEC 62443 est un ensemble de standards élaboré par la Commission électrotechnique internationale (IEC) pour la sécurité des systèmes d'automatisation et de contrôle industriel (IACS). Ces normes fournissent des lignes directrices pour la sécurisation des environnements industriels contre les menaces cyber, en couvrant l'ensemble des aspects de la sécurité, depuis la gestion des risques jusqu'à la mise en œuvre de contrôles techniques.

La série IEC 62443 offre une gamme complète de critères pour les divers niveaux d'un environnement OT, allant des mesures de sécurité **Security Development Lifecycle** (SDL) et produit aux exigences organisationnelles.

[28] ISO/IEC 27000 (ISO, s.d.)

La norme IEC 62443 est divisée en plusieurs parties, regroupées en quatre catégories principales :

1. Politiques et procédures générales (62443-1-x) ;
2. Systèmes (62443-2-x) ;
3. Composants (62443-3-x) ;
4. Produits (62443-4-x).

7.1.2.5 Standards de sécurité PCI

Les standards de sécurité PCI (Payment Card Industry) sont élaborés et maintenus par le PCI Security Standards Council pour protéger les données de paiement tout au long du cycle de vie du paiement. Les différentes normes PCI prennent en charge différents acteurs et fonctions au sein du secteur des paiements[29].

Ces standards s'appliquent à tous les organismes qui stockent, traitent ou transmettent des données relatives aux titulaires de cartes et/ou les données d'authentification sensibles ; ainsi qu'aux développeurs de logiciels et aux fabricants d'applications et d'appareils utilisés dans le cadre de ces transactions.

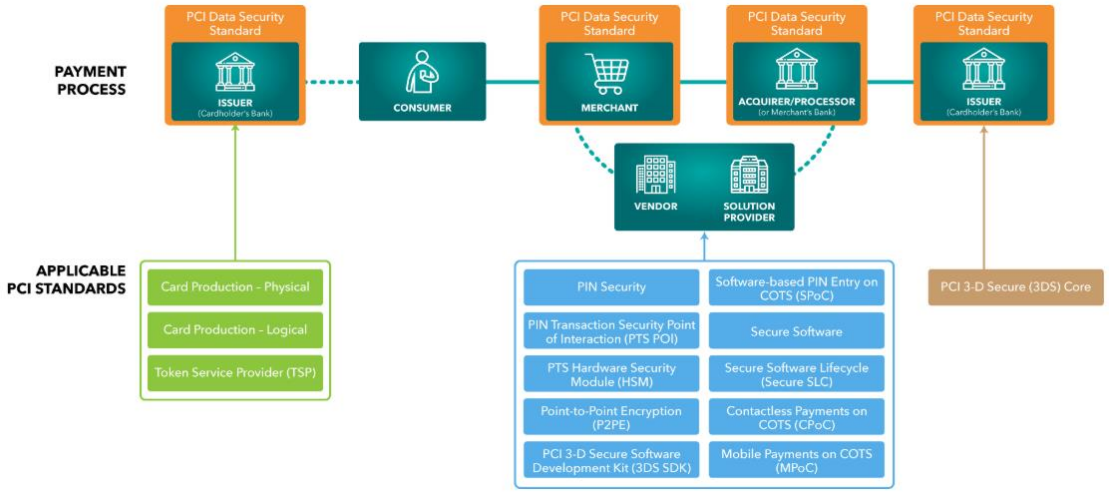


Figure 18 - L'écosystème des normes de sécurité PCI

Certains standards PCI sont destinés à être utilisés par des organisations impliquées dans les paiements, telles que les commerçants, les prestataires de services et les institutions financières, dans leurs propres environnements. Ces standards soutiennent la mise en œuvre de pratiques, de technologies et de processus sécurisés au sein de l'organisation.

[29] Standards PCI (PCI, s.d.)

D'autres standards PCI [30] sont destinés aux développeurs, aux fournisseurs de technologies et aux fournisseurs de solutions souhaitant démontrer que leur produit ou service a été conçu dans un souci de sécurité et répond à un ensemble défini d'exigences de sécurité. Ces standards prennent en charge la validation et la liste des produits et services qui répondent aux exigences du standard et du programme de validation.

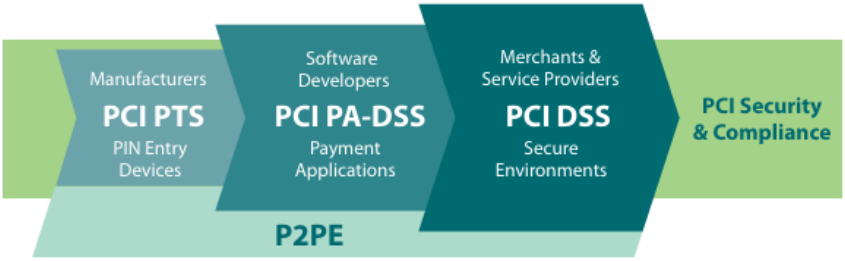


Figure 19 - PCI standards de sécurité

Pour exemple le standard PCI DSS (Payment Card Industry Data Security Standard) est articulé autour de 6 objectifs et 12 exigences. Chaque exigence étant elle-même découpée en plusieurs sous-exigences.

Tableau 2 : Exigences du standard PCI DSS

Objectifs	Exigences du standard PCI DSS
Créer et Maintenir un Réseau et des Systèmes Sécurisés	1. Installer et maintenir des mesures de sécurité du réseau 2. Appliquer des configurations sécurisées à tous les composants du système
Protéger les données de carte	3. Protéger les données de carte pendant leur conservation 4. Protéger les données des titulaires de carte grâce à une cryptographie robuste lors de la transmission sur des réseaux publics ouverts
Maintenir un Programme de Gestion des Vulnérabilités	5. Protéger tous les systèmes et réseaux contre les logiciels malveillants 6. Développer et maintenir des systèmes et des logiciels sécurisés
Mettre en œuvre des Mesures Robustes de Contrôle D'accès	7. Limiter l'accès aux composants système et aux données des titulaires de cartes en fonction des besoins de l'entreprise 8. Identifier les utilisateurs et authentifier l'accès aux composants système 9. Limiter l'accès physique aux données des titulaires des cartes
Surveiller et Tester Régulièrement les Réseaux	10. Enregistrer et surveiller tous les accès aux composants système et aux données des titulaires de cartes 11. Tester régulièrement la sécurité des systèmes et des réseaux
Maintenir une Politique de Sécurité des Informations	12. Renforcer la sécurité des informations à l'aide de politiques et des programmes organisationnels

Pour obtenir la certification PCI DSS, il faut bien entendu se conformer aux exigences et implémenter les contrôles qui permettent de recueillir à une périodicité dictée par le standard PCI DSS, les preuves de l'efficacité des mesures de sécurité qui ont été mise en place.

Ensuite un **audit annuel** est conduit selon le volume de transactions soit par un *Internal Security Assessor* (ISA) ou par un *Qualified Security Assessor* (QSA) qui vérifie la conformité au standard.

Les QSA sont des organismes de sécurité indépendants agréés par le conseil des standards de sécurité PCI.

[30] PCI DSS Quick Reference Guide (PCI)

7.1.3 Les principaux référentiels

Cette partie reprend le détail des référentiels, dont la description est résumée dans un tableau en §3.5

7.1.3.1 NIST

Le NIST (**National Institute of Standards and Technology**) est une agence du département du Commerce des États-Unis qui développe des normes, des directives et des bonnes pratiques pour divers secteurs, y compris en matière de cybersécurité. Le NIST est particulièrement reconnu pour ses cadres de gestion de la cybersécurité, et plus particulièrement le NIST **Cybersecurity Framework** (CSF).

Le NIST Cybersecurity Framework[31] est un ensemble de lignes directrices adoptées pour gérer les risques de cybersécurité. Il a été rendu public pour la première fois en 2014 et est mis à jour régulièrement.

Le noyau du CSF se compose de cinq fonctions principales, subdivisées en catégories et sous-catégories qui couvrent des aspects spécifiques de la cybersécurité :

- Identifier ;
- Protéger ;
- Détecter ;
- Répondre ;
- Récupérer.

La première fonction est **l'identification**, qui consiste à :

- Identifier les risques commerciaux tels que l'interruption des activités et les dommages causés aux biens des clients ;
- Identifier et classer par ordre de priorité les actifs de grande valeur qui représentent un risque commercial majeur en cas de violation ;
- Définir et appliquer des politiques.

Ensuite, il faut **protéger** (et **détecter)** en concevant et en mettant en œuvre un programme de défense à plusieurs niveaux

- Développer les capacités (technologies, processus, personnel) ;
- Atténuer les vulnérabilités ;
- Déployer des contrôles et des mécanismes de cybersécurité ;
- Implémenter un centre d'opérations de sécurité.

Afin de **détecter** les menaces, des sondes seront déployées, et des règles d'alertes diffusées, permettant de surveiller en permanence l'environnement à l'aide d'un SOC (Security Operating Center).

alertes sont ensuite qualifiées et peuvent donner lieu à des actions de remédiation dans le cadre d'une **réponse** à incident, le but étant de minimiser l'impact sur les activités et les opérations grâce au processus de récupération.

Enfin pour améliorer les processus, des enseignements sont à tirer pour chaque incident, dans une optique d'amélioration continue (**récupération**).

[31] Framework NIST (NIST, 2024)

Pour conclure, le NIST Cybersecurity Framework est une ressource essentielle pour les organisations cherchant à renforcer leur cybersécurité. En fournissant des lignes directrices claires et un cadre pour la gestion des risques, le NIST CSF aide les organisations à protéger leurs actifs informationnels, à répondre aux incidents de sécurité et à améliorer continuellement leurs pratiques de cybersécurité.

7.1.3.2 CIS – Center for Internet Security

Le Center for Internet Security, Inc. (CIS®) œuvre pour renforcer le niveau de sécurité des organisations grâce à ses compétences fondamentales en matière de collaboration et d'innovation.

Figure 20 – Le site web CIS (cisecurity.org)

Les CIS benchmarks[32] proposent des recommandations de sécurisation des configurations prescriptives pour plus de 25 familles de produits de fournisseurs. Chacune des recommandations fait référence à un ou plusieurs contrôles CIS, qui ont été développés pour aider les organisations à améliorer leurs capacités de cybersécurité. Les contrôles CIS correspondent à de nombreuses normes et cadres réglementaires établis, notamment le NIST Cybersecurity Framework (CSF) et le NIST SP 800-53, la série de normes ISO 27000, PCI DSS, HIPAA, et d'autres.

7.1.3.3 Open Web Application Security Project (OWASP)

Les principes de l'OWASP : Open Web Application Security Project (Mondial)

OWASP (Open Web Application Security Project) est une organisation à but non lucratif axée sur l'amélioration de la sécurité des logiciels. Elle fournit des ressources gratuites et ouvertes visant à aider les organisations à sécuriser leurs applications web/mobiles et leurs Application Programming Interfaces (API). Les conférences OWASP, les projets collaboratifs et les rapports sur les menaces aident à façonner les pratiques de sécurité dans l'industrie des logiciels.

[32] CIS Benchmarks (CIS, s.d.)

Projet principal :

Le OWASP Top 10[33] est une liste des dix principales vulnérabilités de sécurité des applications web, mise à jour périodiquement pour refléter les tendances actuelles des cyberattaques. Cette liste vise à sensibiliser les développeurs et les gestionnaires de projet aux risques courants et à leur importance en matière de sécurité. L'actualisation de cette liste est prévue courant 2025.

7.1.3.4 MITRE ATT&CK

MITRE ATT&CK – Adversarial Tactics, Techniques & Common Knowledge – est une base de connaissances publique développée par l'entreprise MITRE depuis 2013, qui sert à modéliser, détecter, anticiper et lutter contre les menaces de cybersécurité basées sur les comportements adverses connus des cybercriminels. La matrice ATT&CK regroupe des techniques de cyberattaque sous trois itérations principales :

- **entreprise :** Axée sur les attaques contre les réseaux d'entreprise, cette itération couvre les systèmes d'exploitation Windows, MacOs et Linux, ainsi que les environnements cloud ;
- **mobile :** Se concentre sur les vecteurs d'attaque spécifiques aux appareils mobiles pour les plateformes Android et iOS ;
- **systèmes de contrôle industriel (ICS) :** Se focalise sur les menaces ciblant les systèmes de contrôle industriels, tels que ceux que l'on trouve dans les secteurs d'infrastructures critiques comme la production d'énergie ou les installations industrielles.

L'utilisation de la matrice MITRE ATT&CK s'avère très intéressante pour savoir quels vecteurs d'attaque les attaquants peuvent utiliser contre leur(s) cible(s) et accompagne les organisations à optimiser leurs plans de réponse aux incidents et leurs tests d'intrusion.

En plus de sa vaste collection de tactiques et de techniques documentées, le MITRE ATT&CK Framework comprend diverses ressources qui aident les organisations à appliquer ces connaissances de manière efficace. Il s'agit notamment des ressources suivantes :

- **les évaluations ATT&CK :** Des évaluations indépendantes qui mesurent le degré d'alignement des produits de cybersécurité sur les recommandations du Framework ;
- **des supports de formation :** Une collection de ressources de formation conçues pour aider les utilisateurs à comprendre et à appliquer le framework de manière efficace ;
- **ATT&CK Navigator :** ATT&CK Navigator est un outil open-source permettant aux équipes de sécurité de visualiser, de personnaliser et de partager leurs matrices ATT&CK en fonction de scénarios de menaces spécifiques ou de capacités défensives.

MITRE ATT&CK est une ressource essentielle pour les professionnels de la sécurité informatique, offrant une vue détaillée et structurée des tactiques, techniques et procédures utilisées par les attaquants.

- En particulier, MITRE ATTCK gère une liste de vulnérabilités, appelées **Common Vulnerability and Exposure**, exposé sur un site accessible aux professionnels de sécurité : www.cve.org

[33] OWAPS TopTen (OWAPS)

7.1.3.5 SAFECODE

SAFECode est un forum industriel mondial[34] où des chefs d'entreprise et des experts techniques se réunissent pour échanger des idées sur la création, l'amélioration et la promotion de programmes de sécurité logicielle évolutifs et efficaces.

Nous pensons que le développement de logiciels sécurisés ne peut être réalisé qu'avec un engagement organisationnel dans l'exécution d'un processus d'assurance holistique. Le partage d'informations de ce processus ainsi que des pratiques qu'il englobe est le moyen le plus efficace pour les fournisseurs de logiciels d'aider les clients et parties prenantes à gérer le risque de sécurité des logiciels.

7.1.3.6 SecNumCloud

Élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le référentiel **SecNumCloud** propose un ensemble de règles de sécurité à suivre garantissant un haut niveau d'exigence tant du point de vue technique, qu'opérationnel ou juridique.

D'une part, les prestataires proposant une offre d'informatique en nuage (cloud) doivent faire preuve d'une bonne **hygiène informatique**, d'autre part, les données doivent être **protégées en conformité** avec le droit européen.

[34] Safecode (Safecode, s.d.)

7.1.4 Détail des organisations européennes et nationales de cybersécurité

Cette partie reprend le détail des organisations, dont la description est résumée dans un tableau en §3.6

- Étatique : ENISA, ANSSI, CNIL, Cert/intercert/SecNumCloud (inclus dans ANSSI), COMCYBER ;
- Associations : Club Ebios, Clusif, Cesin, Safecode, PMI ;

7.1.4.1 ENISA (Européenne)

La **European Union Agency for Cybersecurity** (ENISA), ou Agence de l'Union européenne pour la cybersécurité en français, est une agence européenne indépendante créée en 2004. L'ENISA a pour mission principale de renforcer la cybersécurité de l'Union européenne en fournissant des conseils stratégiques et opérationnels ainsi que des recommandations en matière de sécurité des systèmes d'information.

L'ENISA conseille la Commission européenne, le Parlement européen et le Conseil de l'Union européenne sur les questions de cybersécurité. Elle joue un rôle consultatif en formulant des avis et des recommandations pour soutenir l'élaboration de politiques et de législations dans le domaine de la cybersécurité.

Elle aide les États membres de l'Union européenne à renforcer leurs capacités en matière de cybersécurité en fournissant des conseils pratiques, des bonnes pratiques et des outils opérationnels. L'ENISA favorise également la coopération et l'échange de connaissances entre les autorités nationales de cybersécurité de chaque État membre de l'Union.

Pour accentuer la collaboration, elle joue un rôle de coordination en cas de cybercrises dans la zone UE, facilitant la coopération entre les États membres et les acteurs de la cybersécurité pour une réponse rapide et efficace aux incidents graves et aux attaques cybernétiques.

7.1.4.2 ANSSI – autorité nationale[35]

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité. Placée sous l'autorité du Premier ministre et rattachée au secrétaire général de la défense et de la sécurité nationale (SGDSN), elle bénéficie d'un positionnement lui permettant de déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle.

Cette politique s'attache à défendre les infrastructures numériques publiques et privées les plus critiques. L'ANSSI s'adresse également à l'ensemble des acteurs de la transformation numérique du pays et favorise les conditions d'un dialogue de confiance avec ses homologues à l'échelle européenne et internationale.

[35] cyber.gouv.fr/decouvrir-lanssi

Histoire

- La Direction technique des chiffres (DTC), créée en 1943 à Alger ;
- Le Service central technique des chiffres (STC-CH), qui lui a succédé à Paris en 1951 ;
- Le Service central du chiffre et de la sécurité des télécommunications (SCCST), créé en 1977 ;
- Le Service central de la sécurité des systèmes d'information (SCSSI) en 1986 ;
- La Direction centrale de la sécurité des systèmes d'information (DCSSI) créée par le décret n° 2001-693 du 31 juillet 2001 au sein du Secrétariat général de la défense nationale.

Le décret n° 2009-834 du 7 juillet 2009 créant l'Agence nationale de la sécurité des systèmes d'information donne à cette agence, en plus de la sécurité des systèmes d'informations de l'État, une mission de conseil et de soutien aux administrations et aux opérateurs d'importance vitale, ainsi que celle de contribuer à la sécurité de la société de l'information, notamment en participant à la recherche et au développement des technologies de sécurité et à leur promotion.

L'ANSSI (Decouvrir l'ANSSI, 2023) opère sous l'autorité du Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) et du ministère des Armées. L'ANSSI joue un rôle crucial dans la protection des réseaux informatiques sensibles de l'État, des entreprises stratégiques et des infrastructures critiques.

Dans ce contexte, la raison d'être de l'ANSSI, agence interministérielle, est de construire et d'organiser **la protection de la Nation face aux cyberattaques**. Elle contribue ainsi **à renforcer le niveau de cybersécurité global et la stabilité du cyberespace**.

Ses missions

Défendre

- Les systèmes d'information critiques de la Nation en concevant et opérant le déploiement de capacités de détection des cyberattaques ;
- Les victimes de cyberattaques d'ampleur ;
- La Nation en structurant au niveau national l'assistance aux victimes de cyberattaques.

Connaître

- L'état de l'art en sécurité des technologies et des systèmes d'information et en être des experts ;
- Les menaces et les risques dans le cyberespace et développer des méthodes et des outils pour y faire face ;
- Les tendances du monde de la cybersécurité, en France, en Europe et à l'international, pour s'y inscrire pleinement en défendant une vision singulière de la sécurité et de la stabilité du cyberespace.

Partager

- Des recommandations de cybersécurité, des solutions et des outils aux acteurs de la cybersécurité et de la transformation numérique pour démultiplier l'action de l'agence et renforcer la cybersécurité collective ;
- Sur la réponse à la menace au sein des réseaux de coopération techniques, opérationnels et stratégiques français, européens et internationaux ;
- L'expertise de l'agence dans le domaine de la cybersécurité pour former les agents de l'État et des opérateurs régulés à la cybersécurité ;
- Largement les connaissances en matière de cybersécurité et encourager le développement de la filière et des formations en cybersécurité ;
- En lien avec ses partenaires, pour informer et sensibiliser les citoyens aux risques cyber.

Accompagner

- Le développement d'une doctrine française de cybersécurité et la conception des dispositifs normatifs et réglementaires aux niveaux national et européen ;
- Le Gouvernement dans le déploiement d'une politique publique en matière de cybersécurité ;
- Les plus hautes autorités dans leur appréhension du fait cyber ;
- Les opérateurs régulés dans l'application des mesures de sécurisation de leurs systèmes d'information et leurs réponses aux incidents ;
- Le développement d'un écosystème de prestataires de produits et de services de confiance dans le domaine de la cybersécurité.

L'ANSSI est chargée de sécuriser les réseaux informatiques et les systèmes de l'administration publique française, y compris les ministères et les organismes gouvernementaux. Elle surveille les menaces informatiques émergentes, analyse les incidents de sécurité et coordonne la réponse nationale en cas de cyberattaque majeure.

De plus, elle accompagne et conseille les entreprises et organisations considérées comme des Opérateurs d'Importance Vitale (OIV) :

- Les opérateurs télécoms ;
- Les acteurs de l'énergie, de la santé, etc., pour renforcer leur résilience face aux cybermenaces ;
- Les infrastructures critiques françaises, telles que les réseaux d'énergie, les transports, les systèmes financiers, etc., en collaboration avec les acteurs concernés.

Elle mène des actions de sensibilisation et de formation en vue de renforcer les compétences en sécurité informatique aussi bien dans les administrations, les entreprises mais également à destination du grand public.

7.1.4.3 CEPD

Le CEPD, Contrôleur Européen de la Protection des Données, est l'autorité indépendante de l'Union Européenne chargée de surveiller le traitement des données à caractère personnel, par les institutions, organes et organismes européens (IUE).

Ses principales activités en 2024 :

- Surveille et analyse les technologies, y compris les technologies pilotées par l'intelligence artificielle ;
- conseille le législateur de l'UE sur les réglementations de l'UE à venir qui ont un impact direct sur la vie privée et la protection des données des personnes ;
- fournit des outils aux institutions de l'UE (EUI) pour garantir leur conformité avec les lois de l'UE sur la protection des données ;
- influence le développement de la protection des données à l'échelle mondiale.

7.1.4.4 CNIL

La Commission Nationale de l'Informatique et des Libertés (CNIL) est une autorité administrative indépendante française créée en 1978. Son rôle principal est de protéger les données personnelles et la vie privée des individus dans un environnement numérique en constante évolution.

La CNIL est chargée de garantir que les données personnelles collectées et traitées par les organisations (entreprises, administrations publiques, associations, etc.) sont utilisées de manière légale, équitable et transparente. Elle veille à ce que les droits des individus sur leurs données (accès, rectification, suppression) soient respectés.

Elle joue un rôle de contrôle sur les pratiques des responsables de traitement des données (organismes qui collectent et utilisent des données personnelles). Cela inclut l'inspection des systèmes d'information, la vérification de la conformité aux règlements de protection des données, et l'imposition de sanctions en cas de non-respect des règles.

De plus, elle surveille l'évolution de la législation européenne et nationale en matière de protection des données et contribue à l'élaboration de nouvelles normes et directives. La CNIL participe activement à l'harmonisation des règles de protection des données au niveau européen, notamment avec le Règlement Général sur la Protection des Données (RGPD).

7.1.4.5 CERT-FR

Le **CERT-FR** est le **CERT** (Computer Emergency Response Team) ou **CSIRT** (Computer Security Incident Response Team) Gouvernemental et National Français et traite, sur le plan technique, les incidents de cybersécurité. Le CERT-FR est porté par la Sous-Direction Opérations de l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)**.

Les **missions du CERT-FR** sont les suivantes :

- **Répondre aux demandes d'assistance pour donner suite aux incidents de sécurité** sur les réseaux et les systèmes d'informations de ses bénéficiaires. Il traite ainsi la réception des demandes, l'analyse des symptômes des incidents, l'identification d'éventuelles corrélations avec d'autres incidents similaires et la définition de solutions de reprise après incident ;
- **Traiter les alertes et réagir aux attaques informatiques**. A ce titre, le CERT-FR réalise une analyse technique des attaques, participe aux échanges d'informations avec d'autres CERT et contribue à la réalisation d'études techniques spécifiques sur différents sujets de cybersécurité ;
- **Détecter les attaques** ciblant les systèmes d'information gouvernementaux. A ce titre, le CERT-FR opère un service permanent de **supervision de la sécurité** (SOC) **au profit de certains services de l'Etat** ;
- **Détecter les vulnérabilités des systèmes**, au travers notamment d'une veille technologique sur les produits majeurs du marché ;
- **Contribuer à la prévention des attaques informatiques**, en diffusant des informations sur les précautions à prendre pour réduire les risques d'incidents et minimiser leurs conséquences éventuelles ;
- **Coordonner la prévention et la réponse à incidents avec les entités partenaires**. La coordination des opérations permet ainsi de mobiliser, en fonction des besoins, les CERT nationaux et internationaux, les centres de compétences réseaux, les opérateurs et les fournisseurs d'accès à Internet.

InterCERT France :

- est une association loi 1901 qui constitue la première communauté de CERTs en France ;
- n'a pas de vocation commerciale : Partager plus pour être mieux protégés collectivement ;
- fédère aujourd'hui plus de 100 CERTs sur le territoire national.

7.1.4.6 COMCYBER

Le COMCYBER rassemble l'ensemble des forces de cyberdéfense du ministère des Armées. Il a pour mission la défense des systèmes d'information – dont les systèmes d'armes, ainsi que la conception, la planification et la conduite des opérations militaires dans le cyberespace.

Le COMCYBER compte plus de 3600 cyber combattants civils et militaires.

Placé sous l'autorité directe du chef d'état-major des armées (CEMA), le commandement de la cyberdéfense (COMCYBER) est un commandement opérationnel, qui rassemble l'ensemble des forces de cyberdéfense du ministère sous une autorité interarmées.

Créé en mai 2017 par décret, le COMCYBER a pour missions :

- La conduite de la défense des systèmes d'information pour prévenir, détecter et contrer les attaques visant le ministère des Armées ;
- La protection des systèmes d'information de la responsabilité du CEMA ;
- La conception, la planification et la conduite des opérations militaires dans le cyberespace avec des actions de LIO et de L2I ;
- La préparation opérationnelle des forces dans le domaine cyber, *via* des entraînements et exercices nationaux ou internationaux ;
- La cohérence du modèle de cyberdéfense et sa coordination générale (politique RH, besoins techniques, développement de doctrine) ;
- Le développement et l'animation de la réserve de cyberdéfense, opérationnelle et citoyenne.

7.1.4.7 COMCYBER-MI

Le COMCYBER-MI place sous coordination unique (hors opérationnel) tous les services du ministère de l'intérieur traitant de la lutte contre les cybermenaces. Le COMCYBER-MI est chargé d'assurer la cohérence, la performance et la lisibilité du dispositif global du ministère face aux cybermenaces.

Le COMCYBER a pour missions :

- Coordonner, pour un dispositif cohérent, lisible et performant ;
- Anticiper, pour mieux s'adapter ;
- Former, pour garantir un haut niveau de réponse du ministère ;
- Appuyer, pour une offre de service complète contre les cybermenaces, intégrant un haut niveau de technicité et des compétences rares ;
- Prévenir, par l'infusion d'une culture cyber ;
- Coopérer, pour endiguer une cybercriminalité transfrontière.

7.1.5 Détails des associations françaises dédiées à la cybersécurité

7.1.5.1 Club EBIOS

Créé en 2006, le Club EBIOS est une association indépendante à but non lucratif (Loi 1901), composée d'experts individuels et d'organismes. Il supporte et enrichit le référentiel de gestion des risques français depuis 2003.

Il promeut et développe EBIOS, tous ses usages et ses dérivés. Le Club se réunit régulièrement pour échanger des expériences, harmoniser les pratiques et favoriser la satisfaction des besoins des usagers. Il constitue également un espace pour définir des positions et exercer un rôle d'influence dans les débats nationaux et internationaux.

Il a pour objectif d'améliorer la culture de sécurité des systèmes d'information au sein des entreprises et administrations, notamment par la promotion de la gestion des risques.

Les activités :

- Rassembler une communauté de professionnels de la gestion des risques pour notamment :
- Partager des expériences et développer un lieu d'échanges,
- Mettre en évidence les besoins du secteur public et du secteur privé,
- Identifier les experts de gestion des risques et contribuer à leur reconnaissance professionnelle,
- Favoriser les échanges internationaux, notamment en Europe ;
- Gérer un référentiel méthodologique de gestion des risques (documents, logiciels) en cohérence avec :
    - Les besoins des usagers,
    - Les normes internationales,
    - La réglementation,
    - Les outils méthodologiques reconnus, en particulier ceux de l'ANSSI, ceux de ses homologues étrangers et ceux des instances de normalisation ;
- Définir des positions dans le domaine de la sécurité des systèmes d'information et de la gestion des risques en particulier, et exercer un rôle d'influence dans les organismes nationaux, internationaux et de normalisation,
- Dans le secteur public et dans le secteur privé ;
    - Communiquer sur la gestion des risques et les domaines connexes, en particulier sur l'usage du référentiel méthodologique géré par l'association ;
    - Promouvoir et rationaliser la formation dans le domaine de la gestion des risques.

7.1.5.2 CLUSIF

Le Club de la Sécurité de l'Information Français (CLUSIF) est une association française à but non lucratif créée en 1982, dédiée à la sécurité de l'information et à la gestion des risques.

Le 28 novembre 2024, le Clusif est reconnu comme établissement d'utilité publique par l'Etat.

Son objectif principal est de promouvoir les bonnes pratiques en matière de sécurité des systèmes d'information et de favoriser l'échange de connaissances entre professionnels du domaine. Le CLUSIF œuvre pour sensibiliser les entreprises, les institutions et le grand public aux enjeux de la sécurité informatique et à l'importance de la protection des données.

Le CLUSIF organise des sessions de formation, des conférences et des événements pour former les professionnels de la sécurité informatique et sensibiliser les décideurs aux enjeux de sécurité. Son but est de faciliter l'échange d'expériences et de connaissances entre ses membres, issus de divers horizons en termes de secteurs d'activité et d'entreprises de tailles différentes.

7.1.5.3 CESIN

Le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) est une association française à but non lucratif fondée en 1999, regroupant des responsables et des experts de la sécurité de l'information issus d'entreprises privées, d'administrations publiques et d'organisations importantes.

Son objectif principal est de promouvoir la sécurité de l'information à travers le partage de connaissances, l'échange d'expériences et le développement des bonnes pratiques.

Le CESIN représente les intérêts de ses membres auprès des autorités gouvernementales, des régulateurs et des organismes de normalisation. Il joue un rôle actif dans l'élaboration de politiques publiques relatives à la sécurité de l'information et contribue aux débats sur la législation et la réglementation en matière de cybersécurité.

Le CESIN contribue à la sensibilisation aux enjeux de cybersécurité grâce à son baromètre publié annuellement. Ce dernier analyse les tendances et les défis rencontrés par les responsables de la sécurité de l'information (RSSI) en France, offrant ainsi des éclairages précieux sur l'état de la sécurité numérique dans les organisations. Grâce à la diversité de ses membres et ses activités variées, le CESIN continue d'influencer les standards de sécurité informatique et de jouer un rôle clé dans la protection des données et des systèmes d'information contre les menaces émergentes.

7.1.5.4 AFCDP

L'Association française des correspondants à la protection des données à caractère personnel (AFCDP) est une association loi de 1901, créée en 2004, dans le contexte de la modification de la Loi informatique et libertés qui a officialisé une nouvelle fonction, celle de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant informatique et libertés). L'association se focalise sur le métier devenu celui de Délégué à la protection des données, ou DPO (pour Data Protection Officer ou Data Privacy Officer), dans le cadre du Règlement général sur la protection des données (RGPD).

L'AFCDP se focalise sur les objectifs suivants :

- Promouvoir le métier du Délégué à la protection des données, ou Data Protection Officer (DPO) dans le cadre du nouveau règlement européen sur les données personnelles n°2016/679 du 27 avril 2016 ;
- Proposer un cadre d'échanges en développant un réseau en France et à l'international ;
- Concevoir des outils, méthodes et pratiques utiles aux DPO ;
- Défendre le métier, en suivant le cadre juridique de la fonction, en ayant la primeur de l'information, en agissant pour faire valoir la position des professionnels.

L'Association est ouverte aux personnes physiques, aux professions libérales et aux personnes morales (tous secteurs d'activité, privé comme public). Bien que focalisée sur le métier de Délégué à la protection des données ou Data Protection Officer (DPO), l'association n'est pas réservée aux seuls DPO et rassemble largement. Au-delà des professionnels de la protection des données personnelles et des seuls Correspondants désignés par leurs organismes auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données personnelles.

7.2 GLOSSAIRE

AFCDP : Association Française des Correspondants à la protection des Données à caractère Personnel

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

CA: Conseil d'Administration

CEMA : Chef d'Etat Major des Armées

CEPD : Comité Européen de la Protection des Données

CERT: Computer Emergency Response Team

CESIN : Club des Experts de la Sécurité de l'Information et du Numérique

CIGREF : Club Informatique des GRandes Entreprises Françaises

CIS : Center for Internet Security

CISO / RSSI : Chief Information Security Officer / Responsable de la Sécurité du Système d'Information

CLUSIF : CLUb de la Sécurité de l'Information Français

CNIL : Commission Nationale de l'Informatique et des Libertés

COMCYBER : Commandement du ministère des armées dans le cyberespace

COMCYBER-MI : Commandement du ministère de l'Intérieur dans le cyberespace

COMEX : COMité EXécutif

CRA : Cyber Resilience Act

CSIRT : Computer Security Incident Response Team

CSO : Chief Security Officer (directeur de la sécurité)

CTI : Cyber Threat Intelligence (renseignement d'intérêt cyber)

CTO : Chief Technical Officer (directeur technique)

DAF : Direction des Affaires Financières

DORA : Digital Operational Resilience Act

DR : Diffusion Restreinte

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ENISA : European Union Agency for Cybersecurity

Epic : en langage agile, une « Epic » est une « User Story » ou « US » de grand taille (on parle « d'épopée ») qui peut se décomposer en US différentes, dans le but de leur faire appliquer des itérations (« sprint ») chacune selon un rythme adapté

ESN : Entreprise de Services Numériques

ETI : Entreprise de Taille Intermédiaire

HDS : Hébergeur de Données de Santé

HIPPA : Health Insurance Portability and Accountability Act

IE : Intelligence Economique

Ingénierie sociale : ensemble de techniques de manipulation qui servent de levier ou d'outil dans la plupart des cyberattaques

ISO : International Organization for Standardization

KPI : Key Point indicator, indicateur clé de Performance

LPM : Loi de Programmation Militaire

NSA: National Security Agency
NIS: Network and Information System Security
NIS1 et NIS2: directives NIS de l'UE, adoptées respectivement en 2016 et en 2022
NIST : National Institute of Standards and Technology
OIV : Opérateur d'Importance Vitale
PCA : Plan de Continuité d'Activité
PCI : Payment Card Industry
PDCA : Plan-Do-Check-Act (Planifier-Dérouler-Contrôler-Améliorer)
PIV : Point d'Importance Vitale
PRA : Plan de Reprise d'activité
RGPD : Règlement Général sur la Protection des Données
RIA : Règlement Européen sur l'IA
RSSI : Responsable de la sécurité des systèmes d'information
SGDSN : Secrétariat général de la défense et de la sécurité nationale
SIGINT : Signal intelligence (intelligence d'origine électromagnétique)
SISSE : Service de l'information stratégique et de la sécurité économiques
SIIV : Système d'Information d'Importance Vitale
SLA : Service Level Agreement
SMQ : Système de Management de la Qualité
SMSI : Système de Management de la Sécurité de l'Information
SOC : Security Operation Center
Tiering : Le modèle de Tiering de l'ANSSI

7.3 BIBLIOGRAPHIE

7.3.1 Sources indiquées dans ce document

Agence du Numérique en Santé . (2024, Avril). *HDS*. From https://esante.gouv.fr/produits-services/hds

Allianz. (2025). *Allianz Risk Barometer*. From https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2025.pdf

AMF. (2024, Fev 1). *Cybersécurité et risques informatiques : l'AMF appelle les acteurs à se préparer à l'entrée en application du règlement européen DORA*. From Actualités AMF: https://www.amf-france.org/fr/actualites-publications/actualites/cybersecurite-et-risques-informatiques-lamf-appelle-les-acteurs-se-preparer-lentree-en-application

ANSSI. (2018, Novembre). *Agilité et Sécurité numériques*. From https://cyber.gouv.fr/publications/agilite-et-securite-numeriques-methode-et-outils-lusage-des-equipes-projet

ANSSI. (2018, Novembre). *Cartographie du système d'information*. From cyber.gouv.fr/publications/cartographie-du-systeme-dinformation

ANSSI. (2019, Novembre). *Maîtrise du risque numérique - l'atout confiance* . From https://cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance

ANSSI. (2022, Juillet). *Les règles de sécurité*. From https://cyber.gouv.fr/les-regles-de-securite

ANSSI. (2024). *Code de la cybersécurité 2024 annoté et commenté.* Boutique-Dalloz.

ANSSI. (2024). *Code de la cybersécurité 2024 annoté et commenté (boutique-dalloz.fr).* Dalloz.

ANSSI. (2024, Mars). *La méthode EBIOS Risk Manager*. From cyber.gouv.fr/la-methode-ebios-risk-manager

ANSSI. (2024). *Panorama de la Cybermenace.* Paris: ANSSI. From https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

ANSSI. (2025, MArs). *Construire la gouvernance de sécurité numérique adaptée à son organisation*. From https://cyber.gouv.fr/construire-la-gouvernance-de-securite-numerique-adaptee-son-organisation

ANSSI. (2025, Avril). *L'homologation de sécurité*. From cyber.gouv.fr/lhomologation-de-securite

ANSSI. (2025, mars). *Sécurité et projets*. From https://cyber.gouv.fr/integrer-la-securite-dans-les-projets

ANSSI. (n.d.). *CyberDico de l'ANSSI.* From ANSSI - Comité éditorial: https://cyber.gouv.fr/le-cyberdico

CIS. (n.d.). *CIS Benchmarks List*. From https://www.cisecurity.org/cis-benchmarks

Clusif. (1999). *INCAS.V2 INtégration dans la Conception des Applications de la Sécurité.* Paris: Club de la Sécurité des SI France. From https://clusif.fr/wp-content/uploads/2015/10/incas991.pdf

Clusif. (2022). *Intégrer la sécurité dans les projets Cloud.*

CNIL. (n.d.). *La protection des données dans le monde*. From https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Decouvrir l'ANSSI. (2023, nov 14). From https://cyber.gouv.fr/decouvrir-lanssi

Gouvernement. (2018). *La méthode e-Bios Risk Manager - le guide.* https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide.

Intercert-France. (n.d.). *Rapport d'incidentologie*. From https://www.intercert-france.fr/rapport-dincidentologie-2024/

ISO. (n.d.). *La famille ISO/IEC 27000*. From https://www.iso.org/fr/standard/iso-iec-27000-family

Ministère de l'Economie et des Finances. (2023, Avril 11). *Le Règlement Général sur la Protection des Données, Mode d'emploi*. From Bercy Entreprises - Infos: https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd

Ministère de l'économie et des finances. (n.d.). *Risques cyber : des pistes pour la protection des entreprises*. From Portail - Numérique: https://www.economie.gouv.fr/risques-cyber-pistes-protection-entreprises#

Ministère des Armées. (2023). *LPM 2024-2030 - Les grandes orientations.* Paris: DICoD.

MITRE ATTACK. (n.d.). From https://attack.mitre.org/

NIST. (2024). *The NIST Cybersecurity Framework (CSF) 2.0.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

NIST. (n.d.). *Evolution du cout des corrections en fonction du cycle de vie*. From https://www.nist.gov/system/files/documents/director/planning/report02-3.pdf

OWAPS. (n.d.). *OWAPS Top Ten.*

PCI. (n.d.). *PCI DSS Quick Reference Guide.* From https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

PCI. (n.d.). *PCI Security Standards Overview*. From https://www.pcisecuritystandards.org/standards/

Safecode. (n.d.). From https://safecode.fr/

Safecode. (n.d.). *Safecode*. From safecode.fr

Schneier, B. (2000, Avril). *The Process of Security*. From Schneier on Security: www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

7.3.2 Autres sources documentaires

CUSAK Austin, Case Study: The Impact Of Emerging Technologies On Cybersecurity Education And Workforces (2023). Récupéré sur https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss1/3

DESFORGES Alix, Les représentations du cyberespace : un outil géopolitique (2014). Récupéré sur https://shs.cairn.info/revue-herodote-2014-1-page-67?lang=fr.

GHERNAOUTI Solonge, Cybersécurité (2016)

GHERNAOUTI Solonge, Analyser les risques mettre en oeuvre les solutions(2022)

IVANTI, The State of Cybersecurity Report. Récupéré sur https://www.ivanti.com/fr/resources/research-reports/state-of-cybersecurity-report

Livre blanc sur la défense et la sécurité nationale (2013). Récupéré sur https://www.vie-publique.fr/rapport/33131-livre-blanc-sur-la-defense-et-la-securite-nationale-2013

7.4 A PROPOS DE CE LIVRE BLANC

Vous trouverez dans cette partie, une présentation des auteurs et des animateurs de ce Livre Blanc ainsi que des sociétés qui les emploient.

De plus, nous présenterons le fonctionnement des Cercles d'entreprise du chapitre PMI-France.

7.4.1 Les co-auteurs du Livre Blanc

Les membres du Cercle des Entreprises du PMI, ayant collaboré à la réalisation de ce Livre Blanc sont par ordre alphabétique :

7.4.1.1 Hinda Amalou, Information Security Officer au sein d'Allianz Technology

HINDA A. est titulaire de deux masters en sécurité globale et en intelligence économique. Passionnée par la cybersécurité, elle débute sa carrière dans le conseil en 2018, où elle accompagne des grandes organisations et les organismes étatiques dans des projets de sécurité, avec une expertise particulière en GRC (gouvernance, risque et conformité).

Son parcours l'a conduite à travailler dans divers secteurs, tels que la banque, l'énergie, l'industrie et la défense.

Depuis 2022, elle évolue dans le secteur de l'assurance en rejoignant Allianz Technology en tant qu'ISO (Information Security Officer) pour la France.

Coordonnées : hinda.amalou@gmail.com

7.4.1.2 Grégoire Banag, Effitek

Grégoire Banag est consultant senior en cybersécurité et dirigeant associé des sociétés Effitek et Quovadev.

Avec plus de 15 ans d'expérience dans la sécurisation des systèmes d'information complexes, Il s'est spécialisé dans l'intégration de la sécurité dès la conception des projets informatiques (Security by Design), avec une expertise approfondie en analyse des risques (EBIOS RM, ISO 27005), sécurisation des infrastructures (Active Directory, PKI, Cloud).

Il contribue à accompagner les grandes entreprises de différents secteurs dans leurs projets stratégiques liés à l'intégration, la sécurisation et l'optimisation de leurs systèmes d'informations.

Coordonnées : gbanag@effitek.fr

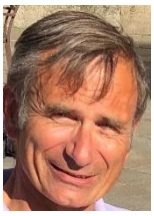
7.4.1.3 Emeric Blumberger, Directeur de Programme Cybersécurité et Vice-président de l'AEGE

Avec plus de 20 ans d'expérience en IT et en cybersécurité, Emeric Blumberger dirige aujourd'hui de grands programmes réglementaires de sécurité en environnement bancaire. Diplômé de l'École des Ponts et de l'École de Guerre Économique, il conjugue expertise technique, pilotage d'équipes internationales et vision stratégique.

Vice-président de l'AEGE, il s'engage à rapprocher intelligence économique, innovation et résilience numérique au service des professionnels.

Coordonnées : emeric.blumberger@aege.fr

7.4.1.4 Lionel Bourceret, ex-Directeur Qualité RSE



Lionel Bourceret, certifié PMP® en 2005, est diplômé de l'Institut Supérieur d'Electronique de Paris (ISEP) en 1980, et d'un Certificat d'Administration des Entreprises de l'IAE en 1989.

A fait toute sa carrière dans les ESN (ou Entreprises de Service Numérique) : Cap Gemini, Atos, Aubay. A mené des projets de mise en œuvre et de transformation auprès de grands donneurs d'œuvre en Système d'Information : Groupes Crédit Agricole et Société Générale, Orange, Vivendi, ...

De 2006 à 2021 a été directeur qualité et RSE de Aubay France, en charge de l'amélioration des processus et d'élever la maturité en développement durable. Plusieurs certifications ont été obtenues : ISO 9001, ISO14001 et ISO27001 (contribution partielle). Ainsi qu'une évaluation qualité en matière de développement informatique (CMMI for development level 3).

Coordonnées : lionel.bourceret@pmi-france.org

7.4.1.5 Samuel Braure, RSSI au sein de Schneider Electric

Samuel BRAURE est responsable de la cybersécurité pour la France et le Benelux chez Schneider Electric depuis janvier 2023.

En tant que RSSI, il est amené à superviser les questions d'IT et d'OT. Concrètement, il est chargé d'exécuter la cyber stratégie de Schneider Electric sur le territoire français, de faciliter la gestion du cyber comme un risque business ou de recenser les incidents de sécurité sur le territoire et d'en tirer les leçons appropriées.

Ingénieur de formation, il évolue depuis 18 ans, sur des métiers orientés techniques dans plusieurs domaines d'expertise comme la sûreté de fonctionnement, le management de l'énergie ou la distribution électrique.

Au fil de ses activités chez Schneider Electric qu'il intégra fin 2012, la prise d'importance croissante de la cybersécurité structura ses aspirations et le conduisit à prendre part à un mastère spécialisé sur le sujet. Cette formation complémentaire lui permit de devenir le Leader Activité Audit et Conseil en cybersécurité OT pour Schneider.

Coordonnées : samuel.braure@se.com

7.4.1.6 Laurent Butti, RSSI au sein d'Orange

Laurent est RSSI à Orange France dans une entité en charge des services Grand Public critiques pour l'activité d'Orange, comme la boutique en ligne, l'assistance en ligne, l'espace client, l'identité...

Spécialiste sécurité informatique depuis plus de 30 ans, il a évolué dans différents contextes entre recherche et production. Il a notamment contribué à l'image d'Orange en présentant plus de 20 conférences internationales dont les plus renommées comme BlackHat USA, BlackHat EU, FIRST et SSTIC. Mais aussi en déposant au nom d'Orange, plus de 20 brevets autour de la sécurité informatique.

Passionné de sport et de nature, il pratique régulièrement trail, VTT et tennis de table.

Coordonnées : laurent.butti@orange.com

7.4.1.7 François Delignette, Manager de transformation au sein de Musubi Consulting

François Delignette, certifié PMP® depuis 2005 et PMI-ACP® depuis 2016, est diplômé de Polytech Nancy (Ex ESSTIN) en 1991 et diplômé de l'Exécutive MBA des Ponts et Chaussées en 2010.

Après un VSNE au Portugal et d'autres expériences à l'international, il devient, en 1995, consultant indépendant pendant 17 ans à Paris.

Par la suite, il rejoint le cabinet Daylight de 2012 à 2023. Daylight Consulting est un cabinet de conseil spécialisé en Projet, Programme, Portefeuille et Agilité.

Daylight Consulting a rejoint le groupe Blue Soft en 2018 pour devenir ultérieurement Blue Soft Consulting.

Courant 2023, il crée son propre cabinet de conseil, Musubi Consulting dédié aux projets de transformations des entreprises.

Il démarre fin 2024 un Exécutif MBA en Gouvernance de la Cybersécurité à l'Ecole de Guerre Economique qui s'achève en septembre 2025. Il est certifié ISO27001 et Ebios Risk Manager

Il pratique la plongée sous-marine, l'Aïkido et l'escalade

Coordonnées : fdelignette@musubi.consulting

7.4.1.8 Mathieu Germain, Expert Cybersécurité et Auditeur au sein d'Orange

Diplômé des Mines d'Alès en 2018, il rejoint une équipe transverse responsable de la cybersécurité pour les infrastructures ainsi que les cloud privés et publics d'Orange France.

Certifié GPEN puis GXPEN en 2019 et 2022, il participe à la construction d'un pôle d'audit de sécurité interne pour promouvoir l'internalisation des activités de pentest.

Il porte au sein d'Orange une expertise sur la sécurité au sein des activités d'automatisation et du DevSecOps et dirige les chantiers DevSecOps dans le programme transverse à Orange France de Sécurité pour les Cloud. Il est également acteur et moteur dans les programmes d'opérationnalisation des principes Zero Trust.

Sur son temps personnel, il passe beaucoup de temps en montagne, sur neige, sur rocher, au bout d'une corde, ou d'une aile de parapente.

Coordonnées : mathieu.germain@orange.com

7.4.1.9 Manon Mécharle, Junior RSSI en VIE au sein de Schneider Electric

Manon Mécharle est diplomée ingénieur généraliste de l'école ESEO.

Pendant la dernière année de ses études, elle a fait une année d'alternance chez Schneider Electric dans l'équipe RSSI de la région Europe Moyen-Orient Afrique (EMEA).

Après une année d'alternance, elle continue dans la même équipe en tant que VIE à Barcelone.

Elle participe à ce projet dans le cadre de son VIE. C'est le premier livre blanc auquel elle contribue.

Elle a comme loisirs le tir au pistolet.

Coordonnées : manon.mecharle@se.com/ manon.mecharle@hotmail.com

7.4.1.10 Riad Roubache, CTO et CISO au sein de Tersedia

Riad Roubache est **Chief Technology Officer (CTO)** et **Chief Information Security Officer (CISO)** chez **Tersedia**, où il travaille depuis 18 ans. Il cumule **28 ans d'expérience** dans les domaines de l'informatique, de la cybersécurité et de la conformité réglementaire. Certifié **ISO/CEI 27001 Lead Implementer** (LSTI) et **DPO** (PECB), il pilote les projets stratégiques, le delivery management et les normes de sécurité de l'entreprise.

Il a notamment dirigé pendant plus de 10 ans les équipes de production et d'exploitation d'un **Asset Manager**, développant une expertise forte en **SSI**, **normes ISO** et **cloud sécurisé.**

Acteur impliqué de l'écosystème cybersécurité, il est membre d'**Hexatrust** (groupes de travail Cloud de Confiance et Admissions), du **Clusif** (où il siège au **comité scientifique**), et enseigne au **Master 2 SIEE** de **Paris Dauphine**. Il est également mécène d'un **projet de recherche en IA & cybersécurité** porté par le laboratoire **DRM**.

Coordonnées : riad.roubache@tersedia.fr

7.4.1.11 Frédéric Vilanova, RSSI GRC de la Banque BIA et dirigeant expert d'Effective Yellow

Frédéric VILANOVA est un dirigeant et expert reconnu dans le domaine de la cybersécurité, de la gouvernance des systèmes d'information et de la gestion des risques numériques. Il a un profil hybride, combinant la vision stratégique d'un CEO, l'expertise opérationnelle d'un consultant senior, et l'ancrage terrain d'un RSSI GRC en environnement bancaire. Frédéric occupe depuis trois ans un poste de RSSI GRC à temps partiel dans une banque internationale à Paris. Il y assure le pilotage des risques numériques, la gestion de la conformité DORA / NIS2 et le contrôle interne de niveau 2. Il a été auditeur et directeur de mission chez PWC et EY. Après un passage chez Cap Gemini puis à Monaco Digital pendant sept ans, il a fondé Effective Yellow en 2014 pour accompagner les ETI dans leur renforcement des dispositifs de cybersécurité, de gouvernance du système d'information et de conformité réglementaire ou normative (NIS2, DORA, IA Act , ISO 27001, ISO 27005, ISO 42001…). Très engagé dans l'écosystème professionnel, il est membre du CLUSIF, de l'IFACI, de l'ISACA. Frédéric est ingénieur Polytech, diplômé de l'ESCP (MSY91), titulaire du DECF et d'un Master en Stratégie Internationale. Il suit également un parcours "executive" à l'INSEAD (Chief Strategy Officer).

Fort de cette pluralité d'expériences, il agit comme un interlocuteur de confiance pour les instances dirigeantes, capable de formuler des recommandations claires, structurées et alignées sur les priorités stratégiques de l'organisation. Il facilite ainsi la prise de décision éclairée face aux enjeux complexes de la cybersécurité et de la conformité numérique.

Coordonnées : frederic.vilanova@effectiveyellow.com

7.4.1.12 Philippe Werle, RSSI/CSN GRC au sein de l'Université Paris Dauphine - PSL

Philippe WERLE est depuis février 2020 Responsable de la sécurité des systèmes d'information et Conseiller à la sécurité numérique en Gouvernance, risque et conformité auprès du Président de l'Université Paris Dauphine - PSL. Il est élu au Comité scientifique du CLUSIF, 1er VP co-fondateur de CyberEdu, membre du Club EBIOS et de l'AFCDP. Il coanime le GT Intelligence économique et sécurité de l'information et le GT IA du CLUSIF.

Développeur en SSII puis chez Fuji Film France, il est diplômé du CNAM en Informatique fondamental en vue des applications où il réalisera son mémoire sur la Warren abstract machine. Il intègre l'Université Sorbonne Paris Nord comme ingénieur d'étude et y développe les activités de génie logiciel en Intelligence artificielle.

Il contribue dans des domaines techniques tels les systèmes, les réseaux et les annuaires X500. Ingénieur de recherche, il pilote des projets inter-établissements comme celui de la gestion des identités, le GT Confiance numérique d'UnivCloud ou le projet d'urbanisation commun à quatre universités. En tant que RSSI et de CIL, il suit de nombreux stages de l'ANSSI et de la CNIL avant de prendre la fonction de RMSI à plein temps à l'Université de Bordeaux. Il est en charge des architectures de sécurité conforme au RGS sur les projets de refonte du réseau de distribution de l'université, du réseau de collecte régional REAUMUR et de la Salle d'hébergement mutualisée pour les établissements de la COMUE d'Aquitaine.

Pour la COMUE d'Aquitaine, il installe et coanime le GT des RSSI et DPO pour livrer une PSSI conforme aux cadres réglementaires PSSIE, RGS, RGPD et PPST.

7.4.2 Les animateurs du Livre Blanc

7.4.2.1 Lionel Bourceret, Directeur du Développement Professionnel

Lionel est membre du PMI-France (Project Management Institute) depuis 2005 et volontaire depuis 2011. Il a été membre du CA du chapitre de 2014 à 2017 puis responsable de la branche Ile-de-France de 2018 à 2021. Il est responsable du développement professionnel entre 2012 et 2014 et depuis 2022. A ce titre développe l'initiative du Cercle des Entreprises en contribuant à plusieurs livres blancs.

Coordonnées : lionel.bourceret@pmi-france.org

7.4.2.2 François Delignette, Directeur du Développement Professionnel IdF

Il est membre du PMI-France (Project Management Institute) depuis 2003 et volontaire depuis 2004. Il a été membre du CA du chapitre et responsable de la branche Ile-de-France de 2011 à 2014. Il est le fondateur du Cercle des Entreprises du PMI-France en 2011 et a contribué à plusieurs livres blancs en tant qu'animateur et co-rédacteur. Il a été directeur du Développement Professionnel en Ile de France pendant plusieurs années et en 2025 il reprend le rôle au niveau national.

Il relance le Cercle des Entreprises en 2024 en lançant un livre Blanc sur Projet & Transition Energétique ainsi qu'un livre blanc sur Projet & Cybersécurité.

Coordonnées : francois.delignette@pmi-france.org

7.4.3 Les relecteurs du Livre Blanc

Le CLUSIF, remarques issues de plusieurs relecteurs

Djamel DEBBICHE, Consultant senior en direction de programmes IT et cybersécurité (MOND2 Consulting)

Christophe DELALANDE, Expert en contexte international, en gestion de projets, portefeuilles et programmes (bénévole PMI-France)

Maxime FITAN, Assistant RSSI et responsable Gouvernance, Risque (Orange)

Cuneyt KAYA, certifié PMP, Bid & Project Manager (THALES)

Matthieu ROUSSEAU, Chef de département (Ministère de l'Intérieur)

7.4.4 Les entreprises contributrices du Cercle

Les Entreprises ayant collaboré - par ordre alphabétique - au Cercle des Entreprises du PMI©, considèrent le Project Management comme une activité stratégique pour leur organisation.

Nom/ Logo	Présentation
	L'AEGE est le réseau des experts en intelligence économique, plus vaste réseau en France. Forte de ses plus de 3500 membres, l'association a pour triple mission d'accompagner ses membres dans leurs vies professionnelles, de contribuer au rayonnement de l'intelligence économique et de l'Ecole de Guerre Economique, et enfin de mobiliser son réseau et à travers ses clubs pour les projets tant pédagogiques que d'utilité publique. L'AEGE gère et organise notamment le Portail de l'Intelligence Economique, le Gala de l'IE, les challenges CTF et OSINT, des journées thématiques (Cyber, Risques, etc.). Actualités et activités disponibles via le site aege.fr
Allianz Technology	Allianz Technology est le fournisseur technologique mondial du groupe Allianz, chargé d'accompagner sa transformation digitale à travers des solutions innovantes et intégrées. Présente dans plus de 20 pays, l'entreprise développe et opère infrastructures, applications et services pour l'ensemble des entités Allianz.
Dauphine | PSL	Établissement public à caractère scientifique et culturel, l'Université Paris Dauphine - PSL est une université et un grand établissement public d'enseignement et de recherche spécialisé dans les sciences des organisations et des décisions. Réputée pour la qualité de ses enseignements en économie, gestion, droit, science politique, sociologie, mathématiques et informatique, l'université figure chaque année aux premiers rangs des établissements les plus réputés. L'établissement est une université composante de l'Université PSL. Conformément à la réglementation, le Responsable de la sécurité des systèmes d'information/Conseiller à la sécurité numérique est placé sous la responsabilité directe de l'autorité qualifiée de la SSI, le Président de l'université. Sous l'autorité de l'AQSSI, une organisation de la SSI a été formalisée composée de RSSI et d'ingénieurs SSI, d'un réseau de correspondants SSI dans les directions et unités mixtes de recherche, d'un comité gouvernance risque conformité composé du RSSI/CSN, du Fonctionnaire sécurité défense et du DPO rattaché à la cellule de crise de l'exécutif et en charge d'accompagner les analyses de risque, les homologations et les procédures de remédiation, et d'un Comité stratégique de la SSI en charge du pilotage et de la définition des moyens. Le comité GRC prépare les sujets à l'ordre du jour du CoStraSSI. Le réseau de correspondants permet au RSSI/CSN de diffuser les postures issues de la chaîne fonctionnelle SSI de l'Etat et de faire remonter les incidents.
Effective Yellow	Cybersécurité, sérénité et lucidité pour les dirigeants. Effective Yellow est un cabinet de conseil aux dirigeants dédié à la maîtrise de la trajectoire cybersécurité. Nous relions la stratégie à l'exécution : définition d'une cible claire, gouvernance & KPI lisibles en COMEX, management de portefeuille/programmes et sécurisation des projets, validation technique (tests d'intrusion, revues d'architecture, exercices de crise) et pilotage des fournisseurs (IT Supply Chain). Notre approche business-driven priorise par scénarios d'impact, industrialise la conformité (ISO 27001, NIS2, DORA, IA Act, ISO 42001, ISO 9001, RGPD) et démontre la résilience avec des résultats mesurables. Objectif : des décisions plus rapides, un risque maîtrisé, une organisation prête pour le board et le terrain, des RSSI et DSI secondés de façon confidentielle.

Nom / Logo	Présentation
orange	Afin d'améliorer son efficacité et sa capacité à satisfaire ses clients et ses salariés, Orange s'est doté d'une politique ambitieuse de professionnalisation des métiers de management de projet. Elle vise à répondre aux enjeux suivants : Mieux maitriser les projets stratégiques du Groupe, Booster la performance des projets (délai, coût, livrable et qualité) en libérant l'énergie des équipes, Accompagner la transformation de l'entreprise vers la digitalisation et l'agilité. Pour valoriser la filière management de projet et la possibilité de déroulement de carrières riches et diversifiées, Orange a mis en place une communauté de management de projet et une certification visant l'excellence avec Orange Project Manager. Par ailleurs Orange participe toujours activement aux activités du PMI.
Schneider Electric	La raison d'être de Schneider Electric est de permettre à chacun de tirer le meilleur de son énergie et de ses ressources, afin de concilier progrès et développement durable pour tous. Cette ambition s'appelle : Life is On. Leader mondial de la transformation numérique de la gestion de l'énergie et des automatismes, Schneider Electric connecte technologies, logiciels et services pour bâtir des environnements plus efficaces, résilients et durables. La cybersécurité est au cœur de cette transformation : elle constitue un impératif stratégique pour protéger les infrastructures critiques, renforcer la confiance numérique et accompagner nos clients dans leur transition vers des opérations connectées et sécurisées. Notre approche « Secure by Design » et « Secure by Operations » s'appuie sur des standards internationaux (IEC 62443, ISO 27001), des partenariats stratégiques (ISA, WEF, CISA) et une gouvernance robuste. Nous agissons sur l'ensemble de notre écosystème — collaborateurs, clients, partenaires, fournisseurs — pour anticiper les risques, renforcer la résilience et promouvoir une culture de la sécurité. Chez Schneider Electric, nous croyons que la cybersécurité est un levier d'innovation, de performance et de durabilité.

7.4.5 PMI® et PMI-France

PMI® (Project Management Institute) est l'une des plus importantes associations au monde pour les activités de Gestion de Projet, à destination de toutes les parties prenantes et en particulier des chefs de projet.

PMI® met à disposition ses ressources professionnelles et de recherches, au travers des activités suivantes :

- Standards mondialement reconnues et programme de certification ;
- Vastes programmes de recherche : académique et du marché ;
- Chapitres locaux et communautés de pratiques ;
- Possibilités de perfectionnement professionnel.

L'impact de ces activités, bénéficie au plus de 700.000 adhérents, pour partie détenteurs de certifications et bénévoles dans presque tous les pays du monde, de faire progresser leur carrière, d'améliorer la réussite de leurs organisations et de contribuer à accroître la maturité de la profession

PMI-France est l'association française loi 1901 représentant le PMI® en France. Créée en 2013, à partir d'associations PMI régionales, son activité principale est d'organiser des évènements sur le territoire français.

7.4.6 Les Cercles d'Entreprise du chapitre PMI-France.

Le chapitre PMI-France regroupe les managers de projets de tous les secteurs d'activité en France. Son objectif est de promouvoir le PMI© (Project Management Institute), ses standards et ses certifications. Ses membres sont des personnes physiques. Ses activités sont gérées bénévolement par des volontaires non rémunérés conformément aux statuts de l'association.

7.4.6.1 Origine

Le « Cercle des Entreprises du PMI » est une initiative lancée en 2011 par la direction du Développement Professionnel du Chapitre Paris Ile-de-France, entité PMI qui fusionnée au sein du PMI-France en juin 2013. Dorénavant le chapitre PMI-France finance et contrôle cette activité destinée aux entreprises, et confirme sa mission d'origine : espace d'échange de bonnes pratiques de gestion de projet à destination des entreprises.

Le Cercle des entreprises du PMI-France bénéficie des études, enquêtes et standards publiés par le Project Management Institute.

7.4.6.2 Objectifs du Cercle

Les objectifs premiers du Cercle sont :

- Promouvoir la gestion de projet auprès des entreprises ;
- Sensibiliser les entreprises au caractère stratégique de la Gestion de Projet ;
- Aider opérationnellement les entreprises en s'appuyant sur le corpus de connaissance du PMI©, ses nombreux référentiels et les Certifications ;
- Se rapprocher des entreprises afin de mieux connaître leurs besoins et voir comment les aider ;
- Privilégier les témoignages de bonnes pratiques à travers la constitution d'ateliers thématiques. La synthèse de ces échanges permet de comprendre les conditions de succès et les raisons des échecs, puis de proposer des recommandations d'amélioration.

Les objectifs secondaires du Cercle sont :

- Faire la promotion du PMI©, de son corpus de connaissance ainsi que de ses référentiels et certifications ;
- Faire la promotion de la marque PMI© ;
- A travers ses actions, faire la promotion des certifiés et des membres du PMI© et augmenter leur employabilité.

7.4.6.3 Cible du Cercle des Entreprises

Le Cercle des Entreprises est destiné aux Entreprises pour qui la gestion de projet représente une compétence stratégique, qui gèrent des projets d'envergure ou qui démarrent un processus d'amélioration continue de leur organisation à la gestion de projet.

Au sein des entreprises, les thèmes d'étude du Cercle des Entreprises intéressent les chefs de projet, les responsables PMO, les responsables de portefeuilles projets/programmes et globalement toute personne en charge du processus d'amélioration continue et de la montée en compétence de leur organisation en management de projets/programmes.

Les responsables de ressources humaines qui doivent accompagner ces profils particuliers que sont les chefs de projet peuvent également trouver au cercle des réponses à leurs interrogations.

Pour adhérer au « Cercle des Entreprises », l'entreprise doit faire acte de candidature auprès du président du Chapitre PMI-France, ou bien du Directeur du Développement Professionnel PMI-France ou lorsqu'il existe, de ce Directeur au niveau de la branche PMI.

L'adhésion est valide pour l'année courante. Elle sera renouvelée par tacite reconduction sauf avis contraire d'une des deux parties.

En fonction du nombre des entreprises appartenant déjà au Cercle et dans un souci d'homogénéité et de représentativité de ces dernières, le chapitre se réserve le droit de donner une suite négative à une demande d'adhésion.

L'adhésion suppose qu'au minimum le représentant officiel de l'entreprise au Cercle des Entreprises soit membre du Chapitre PMI-France, à jour de cotisation lors de la réunion de lancement du Cercle.

7.4.6.4 Les responsabilités du Cercle des Entreprises du PMI

Le président du Cercle

Le président du Cercle des Entreprises pour l'année en cours est nommé parmi les membres du bureau par le bureau du chapitre PMI-France. Généralement le Directeur du Développement Professionnel est le président du Cercle. Il constitue le lien entre le Conseil d'Administration (CA) du chapitre PMI-France et le Cercle des Entreprises.

Il rapporte au CA le suivi des activités du Cercle des Entreprises et propose les évolutions pertinentes afin de s'assurer que le Cercle répond bien aux attentes des entreprises.

Il apporte soutien et aide aux différents responsables en veillant, en particulier, à la promotion des commissions et aux recrutements de nouvelles entreprises.

De plus, opérationnellement, il s'assure que chaque commission est bien gérée par un responsable dédié, qu'elle prend effectivement en charge un sujet en début d'année et le structure sous la forme d'un projet.

En cas de besoin, le président du cercle contribue au premier cadrage du projet et à la mobilisation d'un groupe de travail avec le responsable de la commission.

Le responsable de commission du Cercle

Chaque commission est gérée par un responsable de commission qui travaille de concert avec le président du Cercle. Le responsable de commission est proposé par le président du Cercle et nommé par le bureau de la branche où se tient la commission, à défaut par le CA du chapitre PMI-France.

Le responsable de commission prépare les ordres du jour des réunions et des séances de travail, anime les séances avec son groupe de professionnels et suit l'avancement des travaux. Les comptes rendus des séances de travail sont rédigés sous sa responsabilité avec l'aide de ses volontaires.

En fin de projet, le responsable de commission coordonne la rédaction et la bonne livraison du Livre Blanc.

Les animateurs du Cercle

Les animateurs du Cercle sont tous des bénévoles de la Direction du Développement Professionnel de la branche ou du chapitre PMI-France. En général, il s'agira de professionnels du sujet en question, permettant d'apporter un réel éclairage en s'appuyant sur les référentiels du PMI. Ils travaillent de concert avec le responsable de la commission en question.

Les commissions du Cercle

Le Cercle fonctionne à travers des commissions qui traitent en profondeur un sujet majeur, avec une périodicité variable : annuelle, biannuelle…. L'objectif de chaque commission est de délivrer un livre blanc, synthèse des bonnes pratiques révélées à travers les différents ateliers.

Ce livre blanc est co-rédigé par les membres de la commission avant d'être finalisé par les volontaires du Cercle.

Les commissions peuvent explorer des domaines globaux de la gestion de projet ou au contraire être sectorielles. A titre d'exemple, ces commissions traitent en 2024-2025 des sujets suivants :

- Women By PMI ;
- Les projets au service de la Transition Energétique.

Chaque commission s'organise pour mener les rencontres nécessaires aux échanges entre participants, nécessaire pour confronter leurs idées et proposition de rédaction.

Typiquement, en dehors de contraintes empêchant ce déroulement, cinq rencontres physiques d'une demi-journée sont planifiées tout au long de l'année pour chacune des commissions. De plus, les soirées ou conférences de la branche d'accueil des commissions se dérouleront si possible le même jour, afin de permettre aux membres du cercle d'y assister.

Les réunions s'échelonnent ainsi :

- La première réunion est le kick-off du chantier : cadrage du sujet, plan de travail sur l'année, répartition des tâches, identification des experts invités à participer, objectifs de chacun, calendrier ;
- Les réunions suivantes permettent d'approfondir réellement le sujet ;
- Néanmoins, les deux dernières réunions permettent également de faire une synthèse de l'année et de préparer le Plan de travail de la rédaction du livre blanc sous l'impulsion des responsables de chaque commission.

Les informations utiles au bon déroulement du chantier (comptes rendus, documents de travail) sont conservées sur un espace interne au Cercle des Entreprises et accessibles par les seuls acteurs du chantier.

Les livrables du Cercle

Chaque sujet traité au cours d'une année par une commission fait l'objet d'un rapport final rassemblant toutes les conclusions utiles aux gestionnaires de projets et aux sociétés soucieuses de mieux intégrer la gestion de projet dans leurs pratiques.

Ces rapports ou Livres Blancs sont placés sur le site http://www.pmi-france.org/ et accessibles aux membres du chapitre PMI-France ainsi qu'aux membres du Cercle des Entreprises. Une présentation de synthèse aux membres du chapitre pourra être faite lors de l'assemblée générale ou lors d'une soirée de branche dédiée à cette occasion.

Confidentialité

Les informations échangées pendant les séances restent confidentielles. Les adhérents s'engagent à ne pas divulguer les écrits, présentations, paroles échangées sans l'accord de leur auteur et du président du cercle. Seuls les ordres du jour et les retours d'expérience synthétiques - Livres Blancs - pourront être diffusés.