Gouvernance cybersécurité en entreprise

Au-delà des listes de bonnes pratiques

Stéphane FOSSE

fosse.fr

21 février 2026

Résumé

La gouvernance de la cybersécurité en entreprise n'est pas un problème technique : c'est un problème d'architecture organisationnelle. Qui décide, qui porte le risque, qui traduit l'alerte technique en décision stratégique. Les listes de mesures à appliquer existent. Les frameworks — NIST CSF 2.0, ISO/IEC 27001, EBIOS Risk Manager, Zero Trust — sont solides. Ce qui manque, dans la majorité des grandes organisations, c'est la chaîne de transmission entre les couches — entre le SOC qui détecte et le COMEX qui arbitre.

Une pression qui ne faiblit pas

En 2024, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a traité 4 386 événements de sécurité, soit une hausse de 15 % par rapport à 2023. Parmi eux, 1 361 incidents confirmés — cas où un acteur malveillant a réussi à conduire des actions sur le système d'information d'une victime [2]. Les ransomwares touchent en premier lieu les PME et ETI (37 % des victimes), les collectivités territoriales (17 %) et les établissements d'enseignement (12 %). Les grandes entreprises ne sont pas épargnées : elles sont simplement mieux équipées pour survivre, pas nécessairement pour prévenir.

L'ENISA, l'agence européenne de cybersécurité, confirme cette tendance à l'échelle de l'Union. Son rapport annuel sur le paysage des menaces identifie sept catégories de menaces primaires en 2024, avec en tête les attaques sur la disponibilité des systèmes (DDoS), suivies des ransomwares et des atteintes aux données [9]. Le ciblage est de plus en plus sectoriel : l'administration publique absorbe 19 % des incidents recensés, les transports 11 %. Les attaquants étatiques — principalement des groupes réputés liés à la Russie et à la Chine — concentrent leurs efforts sur l'espionnage stratégique et économique, tandis que les groupes hacktivistes multiplient les opérations de déstabilisation à faible technicité mais à forte visibilité médiatique.

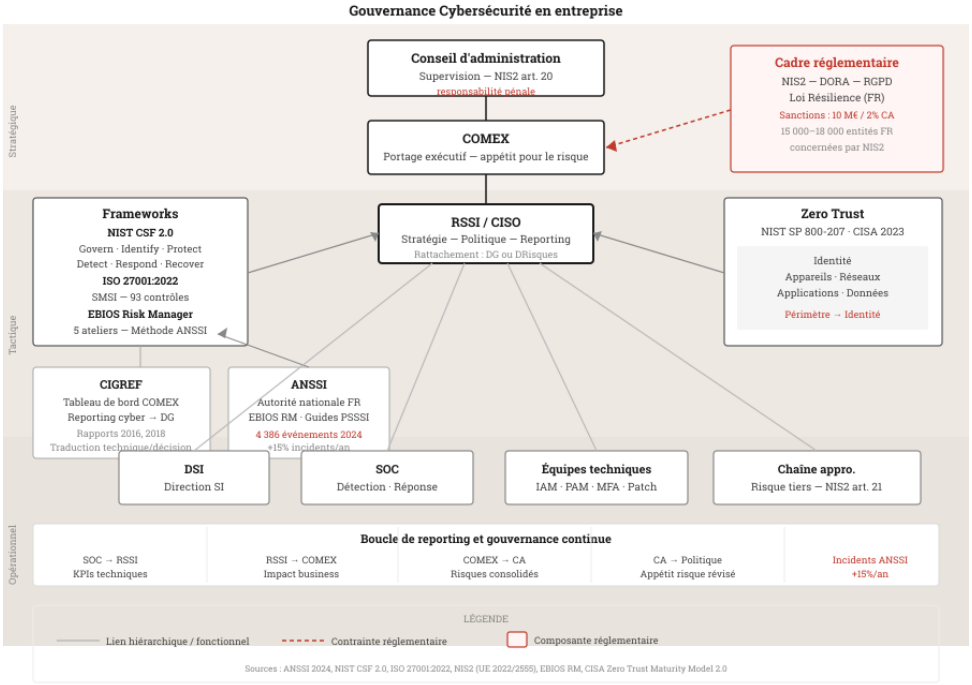
Ce contexte n'est pas nouveau. Ce qui l'est, c'est la réponse réglementaire qui s'y superpose depuis 2022, et qui change fondamentalement la position des dirigeants face à ce risque.

NIS2 et la responsabilisation des organes de direction

La directive européenne NIS2 (UE 2022/2555), adoptée en décembre 2022, constitue un changement de régime [13]. Elle ne demande plus aux organisations de « faire de la cybersécurité » dans leur coin — elle engage explicitement la responsabilité des organes de direction dans la supervision de la gestion des risques. L'article 20 de la directive est sans ambiguïté : les dirigeants doivent approuver les mesures de gestion des risques et suivre des formations adaptées. L'article 21 liste les mesures techniques et organisationnelles minimales obligatoires, dont la gestion des incidents, la sécurité de la chaîne d'approvisionnement, la continuité d'activité et l'authentification multifacteur.

En France, la transposition sous la forme de la « loi Résilience » était attendue pour octobre 2024. Les dissolutions successives de l'Assemblée nationale ont retardé le processus législatif, mais le texte progresse : adopté au Sénat en mars 2025, passé en commission spéciale à l'Assemblée nationale en septembre 2025, la promulgation est attendue au premier semestre 2026 [12]. Entre 15 000 et 18 000 entités françaises seront concernées, classifiées en entités essentielles (secteurs hautement critiques : énergie, santé, transport, banque) et entités importantes (secteurs critiques : industrie, alimentation, services numériques). Les sanctions atteignent 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les entités essentielles en infraction.

Ce cadre réglementaire oblige à une lecture systémique que les approches purement techniques ont toujours ignorée : la cybersécurité n'est plus un sujet que l'on peut déléguer à la DSI et oublier. Elle est un risque d'entreprise au même titre que le risque financier ou juridique, avec des conséquences pénales pour les dirigeants négligents. DORA (le règlement sur la résilience opérationnelle numérique du secteur financier, entré en vigueur en janvier 2025) va encore plus loin dans ce sens pour les institutions financières.



Les frameworks : des ossatures, pas des recettes

Face à cette pression réglementaire et à la sophistication croissante des attaques, les organisations disposent d'un écosystème de frameworks solides. Encore faut-il les comprendre pour ce qu'ils sont — des structures de raisonnement, pas des plans d'action prêts à l'emploi.

Le NIST Cybersecurity Framework 2.0 (CSF 2.0), publié en février 2024 par le National Institute of Standards and Technology américain, est la mise à jour majeure d'un référentiel utilisé dans le monde entier depuis sa première version de 2014 [11]. L'apport structurant de cette version est l'introduction d'une sixième fonction : **Govern**. Les cinq fonctions initiales — Identifier, Protéger, Détecter, Répondre, Récupérer — décrivent ce que fait une organisation face au risque cyber. La fonction Govern décrit comment elle décide de le faire : stratégie de gestion des risques, politique de sécurité, rôles et responsabilités, supervision. C'est la brique qui manquait au CSF 1.1, et son ajout en tête du framework n'est pas anodin. Le NIST confirme que sans cadre de gouvernance, les cinq autres fonctions ne sont que des actions techniques sans cohérence stratégique.

Du côté français, l'ANSSI a développé la méthode EBIOS Risk Manager (Expression des Besoins et Identification des Objectifs de Sécurité), héritière d'une démarche initiée en 1995 et profondément rénovée en 2018 [3]. EBIOS RM se distingue par une approche en cinq ateliers qui alterne conformité et scénarios de menaces. Le premier atelier établit le cadre de l'étude et le socle de sécurité initial. Le deuxième identifie les sources de risques et leurs objectifs. Les troisième et quatrième ateliers construisent des scénarios stratégiques — à l'échelle de l'écosystème — puis des scénarios opérationnels détaillant les chemins d'attaque techniques. Le cinquième définit la stratégie de traitement des risques et le plan d'amélioration continue. Cette architecture en ateliers collaboratifs a une conséquence importante : elle force l'organisation à impliquer des décideurs non techniques dans le processus d'appréciation des risques. L'analyse de risques n'est plus l'affaire du RSSI seul.

La norme ISO/IEC 27001 :2022, révisée en octobre 2022, définit les exigences d'un Système de Management de la Sécurité de l'Information (SMSI) [10]. Sa révision restructure les contrôles en quatre catégories : organisationnels, humains, physiques et technologiques. 93 contrôles remplacent les 114 de la version précédente, avec 11 contrôles nouveaux dont la surveillance des menaces, la gestion des configurations et la prévention des fuites de données. ISO 27001 reste la norme de certification la plus répandue : plus de 70 000 certificats dans 150 pays. Sa force est aussi sa limite : elle impose un cadre de management rigoureux mais n'indique pas comment traiter des menaces spécifiques. C'est là qu'EBIOS RM complète le dispositif — ISO 27001 fournit la structure, EBIOS RM nourrit l'analyse de risques qui l'alimente.

Zero Trust : la rupture architecturale

Le paradigme Zero Trust représente la transformation la plus profonde dans la conception des architectures de sécurité depuis l'apparition du pare-feu. Le NIST SP 800-207, publié en août 2020 et toujours référence, en pose la logique : ne jamais faire confiance implicitement à un utilisateur, un appareil ou un service du seul fait de sa position dans le réseau ou de son appartenance à l'organisation [14]. Chaque accès est accordé sur

la base d'une vérification dynamique, au moment où il est demandé, selon une politique contextualisée.

Ce changement de paradigme a une signification architecturale précise. Le modèle périmètre classique — dans lequel on suppose que tout ce qui est à l'intérieur du réseau d'entreprise est de confiance — repose sur une hypothèse qui ne tient plus dès lors que les données sont dans le cloud, que les utilisateurs travaillent à distance, et que les partenaires et sous-traitants accèdent aux systèmes de l'extérieur. Zero Trust ne supprime pas le périmètre, il le déplace : du réseau vers l'identité. L'authentification multifacteur (MFA), la micro-segmentation des réseaux, la gestion des accès à privilèges et la surveillance continue du comportement des utilisateurs deviennent les nouveaux points de contrôle.

Le CISA américain a formalisé en 2023 un modèle de maturité Zero Trust en cinq piliers — identité, appareils, réseaux, applications et données — permettant aux organisations d'évaluer leur progression et de planifier leur transition [6]. C'est l'une des rares approches qui donne une feuille de route concrète plutôt qu'un état final idéal. Pour un architecte, Zero Trust est moins un produit à acheter qu'une posture à construire progressivement, en commençant par les actifs les plus sensibles.

Le fossé entre le RSSI et le conseil d'administration

Les frameworks existent. Les méthodes d'analyse de risques existent. La réglementation est en place ou en voie de l'être. Pourtant, la gouvernance cybersécurité reste défaillante dans un grand nombre d'organisations. La raison principale n'est pas technique — elle est communicationnelle.

D'un côté, les conseils d'administration raisonnent en termes de risque financier, de réputation et de conformité réglementaire. De l'autre, les RSSI (Responsables de la Sécurité des Systèmes d'Information) — ou CISO dans la terminologie anglophone — maîtrisent des métriques techniques comme les scores CVSS (Common Vulnerability Scoring System), les indicateurs SOC (Security Operations Center) et les taux de couverture des contrôles [7]. Ces deux langages se comprennent mal. Un CVSS à 9,8 sur une vulnérabilité critique exposée sur un service web ne dit rien à un directeur financier. Ce qu'il comprend, c'est un risque de perte de données clients, une amende RGPD potentielle à 4 % du chiffre d'affaires mondial, et un arrêt de production chiffré en centaines de milliers d'euros par heure.

Le CIGREF (Club Informatique des Grandes Entreprises Françaises) a identifié ce problème dès 2016 dans son rapport « Le cyber risque dans la gouvernance de l'entreprise. Pourquoi et comment en parler en Comex ? » [5]. Son diagnostic reste d'actualité : la cybersécurité est trop souvent traitée comme un sujet d'experts, alors qu'elle engage des processus vitaux de l'entreprise. Son rapport de 2018, « Cybersécurité : Visualiser, Comprendre, Décider », va plus loin en proposant un cadre de tableau de bord adapté au COMEX — articulant données d'actualité, analyse de risques consolidée, indicateurs quantitatifs agrégés et éléments de coût [4]. Ce travail de traduction entre la couche technique et la couche décisionnelle est précisément le rôle stratégique du RSSI, trop souvent cantonné à son rôle opérationnel.

La question du rattachement hiérarchique du RSSI est à cet égard politiquement significative. Historiquement subordonné au DSI (Directeur des Systèmes d'Information), le RSSI se trouve alors en situation de conflit d'intérêts structurel : son supérieur hiérarchique direct est précisément la personne dont il doit auditer les choix techniques et opérationnels [1]. Les pratiques évoluent vers un rattachement direct au Directeur Général ou au Directeur des Risques, donnant au RSSI l'indépendance nécessaire pour arbitrer sans contrainte organisationnelle. NIS2 accélère cette évolution en imposant une responsabilité explicite des organes de direction — ce qui rend intenable le schéma où la sécurité informatique reste une affaire de techniciens entre eux.

Ce que gouverner signifie vraiment

Gouverner la cybersécurité, ce n'est pas valider une politique de sécurité une fois par an ni recevoir un tableau de bord rouge-orange-vert sans savoir comment il a été construit. C'est définir un appétit pour le risque — le niveau de risque résiduel acceptable compte tenu des enjeux métier — et s'assurer que les décisions opérationnelles s'inscrivent dans ce cadre. C'est allouer un budget en connaissance de cause, pas sous la pression d'un incident qui vient de se produire.

La fonction Govern du NIST CSF 2.0 structure cette posture en plusieurs dimensions : définir le contexte organisationnel, formaliser la stratégie de gestion des risques cybersécurité, établir une politique de sécurité appliquée à tous les niveaux, clarifier les rôles et responsabilités, gérer le risque lié à la chaîne d'approvisionnement, et superviser la mise en œuvre. Ce n'est pas une checklist — c'est un mode de raisonnement qui doit traverser toute l'organisation, de la direction générale aux équipes techniques.

L'approche par les scénarios d'EBIOS Risk Manager traduit concrètement cette exigence. Plutôt que d'évaluer des risques abstraits sur une matrice impact/probabilité remplie par des techniciens, EBIOS RM construit des scénarios réalistes en partant des sources de menaces identifiées — cybercriminels, attaquants étatiques, partenaires compromis, menaces internes — et de leurs objectifs probables face aux actifs de l'organisation. Ce cadrage par les intentions des attaquants force l'organisation à penser comme ses adversaires, et non comme un auditeur interne vérifiant des cases.

La protection de la vie privée des citoyens s'inscrit dans cette logique de gouvernance systémique. Une organisation qui gère correctement ses risques cyber protège par construction les données personnelles qu'elle

traite — celles de ses clients, de ses employés, de ses partenaires. NIS2 et le RGPD forment à cet égard un binôme cohérent : l'un impose la résilience des systèmes, l'autre la protection des données qui y transitent. Les manquements dans l'un exposent presque toujours dans l'autre.

Construire une gouvernance qui tient

Une gouvernance cybersécurité efficace repose sur trois conditions qui n'ont rien de secret mais qui sont rarement réunies simultanément dans la même organisation.

La première est un portage au niveau exécutif. Pas une délégation formelle au RSSI, mais un membre du COMEX qui porte réellement le sujet, défend le budget, arbitre les conflits de priorité entre performance opérationnelle et sécurité, et rend compte au conseil d'administration. Ce portage peut venir du DSI, du Directeur des Risques, voire du Directeur Financier — peu importe la fonction, ce qui compte est l'engagement réel. NIS2 rend ce portage obligatoire en engageant la responsabilité personnelle des dirigeants.

La deuxième condition est une méthode d'analyse de risques vivante. Un audit de sécurité annuel figé ne suffit plus. Les menaces évoluent trop vite — l'ANSSI recense une augmentation de 15 % des incidents chaque année depuis plusieurs exercices consécutifs [2]. EBIOS RM, avec sa logique itérative et ses ateliers collaboratifs, est conçue pour être une démarche continue. Le registre des risques doit être mis à jour à chaque évolution significative du système d'information, à chaque incident notable, et à chaque changement dans le paysage des menaces.

La troisième condition est la qualité du reporting vers la direction. Un tableau de bord cybersécurité destiné au COMEX doit répondre à des questions simples : où sommes-nous les plus exposés ? Qu'est-ce qui a changé depuis la dernière revue ? Quels arbitrages sont attendus de la direction ? Les métriques techniques (nombre de vulnérabilités critiques non corrigées, délai moyen de détection et de réponse aux incidents, couverture MFA) ne valent que si elles sont traduites en termes d'impact business compréhensibles sans formation préalable en sécurité informatique [4].

Ces trois conditions forment un système. Une direction impliquée sans méthode solide produit de l'agitation sans direction. Une méthode rigoureuse sans portage exécutif produit des analyses que personne ne lit. Un reporting sophistiqué sans décision qui s'ensuit est une dépense d'énergie sans retour. C'est l'articulation entre les trois qui fait la gouvernance.

Ce que les frameworks comme NIST CSF 2.0 ou ISO 27001 ont mis du temps à formuler explicitement, les organisations qui gèrent bien leur risque cyber l'avaient compris empiriquement : la cybersécurité ne se gouverne pas différemment du reste de l'entreprise. Elle demande un commanditaire clair, une vision du risque accepté, des ressources en rapport, et des mécanismes de contrôle. L'erreur a été, pendant des années, de penser qu'elle était l'exception — trop technique, trop complexe, à laisser aux spécialistes. NIS2 met fin à cette exception.

Références

[1] Alliancy. Cybersécurité : quelle répartition des rôles entre le CIO, le Comex et le conseil d'administration ? Sept. 2024.

[2] ANSSI. Panorama de la cybermenace 2024. CERTFR-2025-CTI-003. Agence nationale de la sécurité des systèmes d'information, mars 2025.

[3] ANSSI et Club EBIOS. EBIOS Risk Manager — Le Guide, version 1.0. Agence nationale de la sécurité des systèmes d'information. 2018.

[4] CIGREF. Cybersécurité : Visualiser, Comprendre, Décider. Club Informatique des Grandes Entreprises Françaises, oct. 2018.

[5] CIGREF. Le cyber risque dans la gouvernance de l'entreprise. Pourquoi et comment en parler en Comex ? Club Informatique des Grandes Entreprises Françaises, 2016.

[6] CISA. Zero Trust Maturity Model, Version 2.0. Rapp. tech. Cybersecurity et Infrastructure Security Agency, avr. 2023.

[7] Cybersécurité Management. Du technique au stratégique : le CISO face au défi du langage de la gouvernance. In : *Cybersécurité Management* (déc. 2025).

[8] ENISA. 2024 Report on the State of Cybersecurity in the Union. European Union Agency for Cybersecurity, nov. 2024.

[9] ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, oct. 2024.

[10] ISO/IEC. ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Oct. 2022.

[11] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Rapp. tech. NIST CSWP 29. National Institute of Standards et Technology, fév. 2024.

[12] Orange Cyberdefense. NIS2 : obligations, échéances, sanctions et mise en conformité. 2025.

[13] Parlement européen et Conseil de l'Union européenne. Directive (UE) 2022/2555 — NIS2 — concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. Déc. 2022.

[14] Scott Rose et al. Zero Trust Architecture. Rapp. tech. NIST SP 800-207. National Institute of Standards et Technology, août 2020.