Lecture Individuelle Sierre, le 27 novembre 2023

La gouvernance de la sécurité

Étudiant	DAVID Guillaume, 803_1F
N° de la lecture individuelle :	3
Semestre	3
Sujet	La gouvernance de la sécurité

Choix du sujet

Je m'engage actuellement dans une exploration approfondie de la gouvernance de la sécurité, un domaine essentiel dans l'informatique moderne.

Mon intérêt pour ce sujet découle de sa pertinence essentielle dans la protection des systèmes informatiques contre les menaces croissantes et des risques associés à la sécurité des données mais également de l'infrastructure.

Le premier objectif de ma démarche est d'approfondir ma compréhension du rôle fondamental de la gouvernance de la sécurité dans la préservation de l'intégrité, de la confidentialité et de la disponibilité des données.

En parallèle, je cherche à renforcer mes compétences pour élaborer des stratégies de sécurité pour les systèmes. La connaissance des normes et des réglementations en matière de sécurité est également au cœur de mes préoccupations, car cela s'avère indispensable avec les modifications des réglementation (RGPD, ...). Une notion d'éthique et de responsabilité sociale motive également ce choix.

Enfin je m'intéresse à la compréhension des capacités d'adaptation des entreprises face aux problématiques de sécurité et comment réagir face aux menaces de sécurité. Et si le livre en parle, comment optimiser et mettre en place une procédure afin de « remonter » une infrastructure selon des protocoles éprouvés.

Table des matières

Supports de recherche

La lecture se base sur le livre « Management de la sécurité de l'information et ISO 27'001 ».

Auteur :	Jean-Pierre Lacombe, Nadège Lesage
Éditeur :	Collection DataPro des éditions ENI
ISBN :	978-2-409-02953-0
Année de parution :	2021
Nombre de page :	295

Cette lecture se base également sur de la recherche approfondie d'articles mises en annexes ainsi qu'un soutient notamment dans la relecture de ChatGPT.

Lecture Individuelle Sierre, le 27 novembre 2023

Qu’est-ce que la gouvernance des donnes ?

La gouvernance des données, conformément à la norme ISO 26000, se définit comme le système par lequel une organisation prend et met en œuvre des décisions pour atteindre ses objectifs de sécurité.

La responsabilité de définir les objectifs stratégiques revient à la direction, tandis que le responsable de la gouvernance est chargé de spécifier et de gérer le système approprié. Dans le contexte de la norme ISO 27001, la direction doit avoir le pouvoir d'engager l'organisation dans le domaine d'application défini. La constante dans ces définitions réside dans la nécessité de prendre des décisions et de faire des choix pour assurer une gouvernance efficace. Ainsi, la prise de décision, les choix organisationnels, leur évaluation, et la communication associée sont des éléments cruciaux pour garantir une bonne gouvernance.

L'établissement d'une gouvernance de sécurité s'avère indispensable de nos jours, car la sécurité des systèmes d'information ne se limite pas à des aspects techniques ou organisationnels. Dans un environnement complexe, que ce soit au sein d'une grande entreprise ou d'une société avec des responsabilités réparties, il est crucial de mettre en œuvre une gouvernance de la sécurité adaptée à la culture de l'organisation. Cette gouvernance doit être capable de rassembler toutes les actions liées à la sécurité, transcendant les frontières techniques et organisationnelles.

La sécurité ne peut être considérée comme acquise dans un monde en constante évolution, où les menaces évoluent, de nouvelles vulnérabilités émergent quotidiennement, les besoins métier se transforment, et le système d'information s'ouvre à de nouveaux utilisateurs et modes d'accès. La vigilance doit être une préoccupation permanente, impliquant l'ensemble des acteurs, et les exigences de sécurité doivent être adaptables pour faire face à cette dynamique en constante évolution. Ainsi, la mise en place d'une gouvernance de sécurité devient non seulement nécessaire mais aussi un impératif pour assurer une protection efficace dans cet environnement en perpétuelle mutation.

Points importants

1. **Aspect Transverse**
   La sécurité des systèmes d'information va au-delà de la technique ou de l'organisation ; une gouvernance adaptée doit transcender ces aspects et s'harmoniser avec la culture organisationnelle.

2. **Fédération des Actions**
   Dans des organisations étendues, la gouvernance de sécurité doit coordonner et unifier toutes les actions liées à la sécurité pour une approche cohérente.

3. **Adaptabilité**
   Face à des menaces changeantes, la gouvernance doit être flexible, s'ajustant rapidement aux nouvelles vulnérabilités, aux besoins métier fluctuants, et aux évolutions du paysage de la sécurité.

4. **Préoccupation Permanente**

La gouvernance doit instaurer une vigilance constante, intégrant la sécurité dans la routine quotidienne de l'organisation pour répondre à une menace potentielle à tout moment.

5. **Engagement de Tous**
   La responsabilité de la sécurité ne se limite pas à un groupe spécifique ; la gouvernance doit encourager la participation active de tous les membres de l'organisation.

La prise de décision

L'importance de la prise de décision réside dans la reconnaissance des trois niveaux de management au sein d'une entité, chacun correspondant à des décisions spécifiques ayant des impacts distincts.

- Le niveau stratégique, dirigé par la direction, prend des décisions stratégiques influençant directement la vie de l'entité.
- Le niveau tactique, géré par des cadres supérieurs et intermédiaires, prend des décisions managériales impactant le métier.
- Le niveau opérationnel, dominé par l'encadrement technique et les exploitants, prend des décisions techniques affectant les processus opérationnels.

Cette structure à trois niveaux permet une connaissance partagée des sujets avec des points de vue variés, favorisant une prise de décision pertinente où chaque acteur contribue selon son expertise et son niveau de responsabilité. Une organisation efficace doit prévoir une structure adaptée pour faciliter cette confrontation de points de vue, bien que dans les entreprises de taille humaine, la fusion des niveaux peut simplifier la structure mais présente des risques liés à la séparation des rôles.

Structure organisationnelle

La définition de la structure organisationnelle est cruciale pour la circulation efficace de l'information. La norme ISO 27001 encourage une organisation de la sécurité, nécessitant une adaptation aux besoins spécifiques. La circulation de l'information se fait en continu et ponctuellement, avec des chaînes hiérarchiques, fonctionnelles, et opérationnelles.

La norme ISO 27001

La mise en avant des avantages de la démarche ISO 27001 est essentielle et doit être intégrée. Les avantages commerciaux, la gestion rigoureuse, et le renforcement de la sécurité sont des éléments clés à communiquer à la fois en interne et en externe. La communication doit intégrer ces avantages comme des marqueurs pour maintenir l'effort et valoriser les investissements.

La norme ISO 27001 est un standard international définissant les exigences pour établir, mettre en œuvre, maintenir et améliorer un système de gestion de la sécurité de l'information (SGSI) au sein d'une organisation. Elle vise à assurer la confidentialité, l'intégrité et la disponibilité des informations, en identifiant et en gérant les risques liés à la sécurité de l'information. Cette norme est étroitement liée à la gouvernance, car elle implique la mise en place d'une structure organisationnelle claire, ainsi qu'à la sécurité en intégrant des mécanismes de protection des données et des processus opérationnels. La mise en conformité avec l'ISO 27001 nécessite une évaluation des ressources nécessaires, une définition des rôles et responsabilités, et un plan

projet budgété pour atteindre les objectifs de sécurité et de gouvernance définis par l'organisation.

Intérêts communs

L'intérêt commun des acteurs est crucial pour la mobilisation à long terme. La communication individualisée, l'explication des avantages pour l'entreprise et les personnes concernées, ainsi que la responsabilisation de chaque acteur contribuent à une meilleure compréhension et acceptation des mesures de sécurité. L'implication de la direction et de tous les acteurs doit être avec une identification claire des rôles et des responsabilités.

Rôles et responsabilités

Il est important de bien identifier les rôles et les responsabilités de chacun des acteurs pour tout processus qui impacte la sécurité.

Identification des rôles

La définition claire des rôles et des responsabilités est cruciale pour la sécurité organisationnelle. L'inventaire des responsabilités doit être détailler pour toutes les tâches et responsabilités.

Cohérence entre l'identification et l'attribution

La cohérence entre l'identification des rôles et leur attribution est essentielle. Elle se base sur la structure organisationnelle préalablement définie. Les incompatibilités organisationnelles, hiérarchiques ou fonctionnelles doivent être évitées. L'attribution des rôles doit être soigneusement contrôlée pour assurer l'exhaustivité des actions et des responsabilités.

Le cadre juridique

Le cadre garantit que les précautions garantissent que les rôles et responsabilités sont attribués conformément aux contraintes légales, évitant des implications juridiques indésirables.

1. **Chief Information Security Officer (CISO) / Directeur de la Sécurité de l'Information (DSI)**
   Le CISO est responsable de la direction stratégique de la sécurité de l'information, tandis que le DSI occupe un rôle similaire en français.

2. **Compliance Officer / Responsable de la Conformité**
   Ce professionnel veille à ce que l'organisation respecte les réglementations en vigueur. En français, on le désigne souvent comme Responsable de la Conformité.

3. **Risk Management Officer / Responsable de la Gestion des Risques**
   En charge de l'identification, de l'évaluation et de la gestion des risques liés à la sécurité de l'information.

4. **Data Protection Officer (DPO) / Responsable de la Protection des Données**
   Responsable de veiller à la conformité avec les lois sur la protection des données et à la mise en place de mesures appropriées pour assurer la sécurité des données.

5. **Security Awareness Officer / Responsable de la Sensibilisation à la Sécurité**
   En charge de sensibiliser les employés aux bonnes pratiques de sécurité et de mettre en place des programmes de formation.

Les ressources

La mise en place d'une approche ISO 27001 exige des ressources pour aborder les aspects stratégiques, tactiques et opérationnels du projet.
Les ressources peuvent être de nature différente.

- Structurale
  Infrastructures physiques, logistique, répartition géographique
- Financières
  Budget adapté aux objectifs
- Techniques
  Outils informatiques, solutions dédiées à la sécurité
- Humaines
  Qualification pour les tâches de sécurité

Un projet pour atteindre la conformité de la gouvernance de la sécurité nécessite une clarté sur les éléments présentés ci-dessus.

Finalité de la norme ISO 27’001

Principes de la norme ISO 27’001

- **Démarche Rigoureuse**
  La norme ISO 27001 offre une démarche rigoureuse pour la gestion de la sécurité des informations numériques. Adoptant un système de management similaire à d'autres normes, elle structure la prise en compte de la sécurité au sein des organisations.

- **Prescriptive et Souple**
  Bien que prescriptive dans ses exigences, elle offre une souplesse d'interprétation. Elle définit « quoi » doit être fait, laissant la liberté sur « comment » répondre à ces exigences. En complément, la norme ISO 27002 détaille les mesures de sécurité, fournissant ainsi une combinaison flexible et complète.

- **Enjeux d'Interprétation**
  L'un des défis majeurs réside dans l'interprétation des exigences et leur adaptation contextuelle. Son implémentation peut être formelle, visant la certification, ou libre, selon les besoins spécifiques de l'organisation. L'expertise en sécurité de l'information est cruciale, bien que la norme ne soit qu'une partie de cette expertise.

- **Finalités de la Norme :** Au-delà de la certification, la norme sert de référentiel pour les bonnes pratiques et l'évaluation de la sécurité. En articulant les concepts de sécurité de manière rigoureuse et exhaustive, elle est devenue une source reconnue des "bonnes pratiques" dans le domaine.

- **Cible de la Norme**
  - **Personne Morale**
    La norme est applicable à toute entité, indépendamment de sa taille, de son secteur d'activité, ou de sa forme juridique, pourvu qu'elle puisse répondre aux exigences de gouvernance. La certification ISO 27001 est envisageable pour une large variété d'organisations, de petites entreprises à des entités multinationales, sous réserve de respecter le cadre légal et réglementaire.

  - **Personne Physique**
    La norme est également utilisable par toute personne souhaitant approfondir ses connaissances en gouvernance et sécurité de l'information. La certification de personnes est possible, mais exige une expérience significative dans le domaine de la sécurité de l'information.

- **Investissement Induit**
  La démarche de certification est un engagement à long terme, avec des activités planifiées sur plusieurs années. L'investissement nécessaire comprend des ressources humaines, des compétences, et une maîtrise approfondie de la norme par les experts. Pour d'autres finalités, les investissements peuvent être plus ciblés et adaptés à des activités spécifiques, offrant une flexibilité budgétaire et une gestion maîtrisée des ressources.

Certification ISO 27’001

L'obtention de la certification ISO 27001 est fondamentale pour établir une démarche de sécurité validée et répondre aux normes internationales. Cette certification, décernée après une phase d'implémentation et d'audit, valide la conformité de l'organisme aux exigences de la norme. Elle joue un rôle crucial dans la communication externe, renforçant la position de l'organisme face à la concurrence, rassurant les clients sur la conformité des services, et ouvrant des opportunités d'accès à des marchés spécifiques. Cependant, des limites subsistent, soulignant que la certification ne garantit pas l'absence totale de risques ou de failles, et que le niveau de maturité de sécurité demeure un objectif évolutif dans le temps.

Mise en pratique selon les recommandations

La norme ISO 27001, reconnue internationalement et conçue par des experts en sécurité de l'information, fonctionne comme un référentiel de bonnes pratiques. En intégrant cette norme, il devient essentiel de maîtriser ses repères, notamment le vocabulaire et les concepts, facilitant ainsi la communication entre experts et non-experts, tout en normalisant la gestion de la sécurité. La norme, en plus d'être pragmatique, agit comme un guide pratique en fournissant une philosophie, une logique, une rigueur, et une exhaustivité qui définissent un niveau d'exigences à atteindre. Outre son rôle dans la certification, elle est également utilisée

comme une référence majeure dans la perspective des bonnes pratiques et de l'état de l'art en matière de sécurité.

La norme ISO 27001 suit le modèle PDCA (Planifier, Réaliser, Contrôler, Améliorer) pour l'amélioration continue, avec les étapes suivantes :

1. **Planification (Plan)**
   Comprendre le contexte, les contraintes légales, définir le périmètre, les objectifs stratégiques et de sécurité, identifier les acteurs, et évaluer les risques.
2. **Mise en œuvre (Do)**
   Mettre en place la gouvernance, définir les politiques de sécurité, adopter un plan d'actions, coordonner les acteurs, mettre en œuvre les mesures, et établir des indicateurs de contrôle.
3. **Contrôle (Check)**
   Collecter et utiliser les indicateurs sur l'existence et l'efficacité des mesures et de la gouvernance, réaliser des audits internes, et identifier les domaines à améliorer.
4. **Amélioration (Act)**
   Utiliser la veille, les résultats des audits et les domaines d'amélioration identifiés pour renforcer la gouvernance et améliorer l'efficacité des mesures de sécurité.

Politique de gouvernance

1. Préciser les objectifs

Préciser les objectifs de gouvernance de la sécurité débute par la compréhension approfondie d'un objectif stratégique énoncé par la direction. Il est essentiel de clarifier les enjeux et motivations sous-jacents à travers des entretiens avec la direction, permettant de déterminer si l'objectif vise à améliorer la conformité aux exigences réglementaires, répondre aux attentes des principaux clients, explorer de nouveaux marchés, accroître la visibilité internationale, ou satisfaire les actionnaires. Cette étape sert également à préciser si l'objectif concerne l'ensemble de la structure ou des secteurs spécifiques. Une fois les objectifs clairement définis, le responsable de gouvernance recommandera une étude de faisabilité pour évaluer la position actuelle de l'organisation par rapport aux objectifs fixés, identifier les actions nécessaires, mesurer le travail restant, et présenter un projet. En général, la demande de la direction s'accompagne souvent d'une phase d'étude, soulignant l'importance d'assurer que la direction comprend pleinement les implications et la viabilité de l'objectif proposé.

2. État des lieux

Le succès d'un projet de gouvernance et de sécurité dépend de la compétence du responsable, questionnant la maîtrise des deux composantes. La nécessité de formation ou d'accompagnement, interne ou externe, est soulignée, surtout lorsque les compétences en gouvernance diffèrent de celles en sécurité. Le contexte du projet, les parties impliquées, et les exigences réglementaires sont ensuite précisés, en identifiant les rôles majeurs. Les entretiens avec ces acteurs visent à évaluer leur adhésion, analyser la maturité sécurité, et identifier les leaders de la gouvernance et des chantiers opérationnels. Cette étape est complétée par l'analyse de la documentation existante. L'analyse globale du projet, incluant les principaux chantiers, le calendrier, le budget, les compétences, et les besoins supplémentaires, est réalisée en collaboration étroite avec les directions concernées. Enfin, le bilan de l'analyse est présenté à la direction pour évaluer la faisabilité du projet.

3. Négocier les objectifs et calendrier

La présentation de l'état des lieux devant la Direction et les directions impliquées vise à évoquer les points forts, les axes d'amélioration, et à proposer des échéances réalistes, ainsi qu'une enveloppe budgétaire et les ressources nécessaires. L'objectif est de parvenir à une négociation aboutissant à un calendrier réaliste et à l'obtention des moyens humains et financiers nécessaires. Une fois ces éléments confirmés, la rédaction d'une politique de gouvernance intervient, servant de contrat interne où la Direction s'engage à fournir les moyens, et les directions concernées s'engagent à mettre en place les actions nécessaires pour atteindre les objectifs du projet.

4. Points clés de la gouvernance

- **Objectifs stratégiques, enjeux et contexte**
  La politique de gouvernance énonce les objectifs stratégiques, précise les enjeux pour la structure, et identifie les exigences réglementaires et contractuelles.

- **Domaine d'application**
  La politique de gouvernance détermine le domaine d'application, définissant le périmètre de la gouvernance de la sécurité, incluant métiers, processus, sites, architecture du système d'information, métiers supports, interfaces, et tiers.
- **Objectifs de sécurité**
  Décliner les objectifs stratégiques en objectifs de sécurité, en visant une approche opérationnelle et mesurable, liant ces objectifs aux objectifs stratégiques pour évaluer l'atteinte au niveau opérationnel et renseigner la sphère stratégique.

- **Stratégie de gestion des risques**
  Définir les modalités de gestion des risques dans le cadre de gouvernance, en précisant une méthode d'analyse (libre choix sous certaines précautions) et en optant pour une fréquence de révision, idéalement annuelle, permettant d'évaluer les actions d'amélioration continues et d'ajuster en fonction de l'évolution des risques.

- **Comité stratégique :**
  - Membres permanents : direction générale, responsable de la gouvernance, directions métier, systèmes d'information, ressources humaines, juridique, achats, bâtiments, contrôle interne, communication.
  - Missions : pilotage du budget, suivi des enjeux internes et externes, suivi du plan d'appréciation des risques, approbation du plan de traitement des risques, approbation et suivi du plan d'action, analyse des indicateurs de gouvernance et d'efficacité, traitement des incidents de sécurité, prise de connaissance et validation des résultats d'audit, suivi des améliorations, suivi des plans de sensibilisation et de formation, suivi de la communication, gestion des allocations de ressources.
- **Comité opérationnel :**
  - Composition : responsable de la gouvernance, responsable sécurité, maîtrises d'ouvrage/maîtrise d'œuvre (administrateur réseau, système, gestionnaire des postes de travail, équipe support, responsables des développements, intégration, production, hébergement, gestion des sauvegardes, des projets, représentant RH, achats, logistique, DPO ou représentant juridique).

- Missions : faire évoluer le plan d'action, assurer sa déclinaison opérationnelle, suivre les projets, identifier les points durs, résoudre les problèmes, proposer des actions de remédiation, analyser les indicateurs de suivi du plan d'action, remonter les indicateurs consolidés en comité stratégique, analyser les indicateurs de suivi de l'efficience des mesures et des risques résiduels, suivre la gestion des incidents de sécurité, suivre les résultats d'audit, proposer des opportunités d'amélioration au comité stratégique.

5. Organisation de la gouvernance

Il convient là de définir les moyens humains en charge de la gouvernance et de définir les rôles de chacun.

- **Comité stratégique**
  - **Membres permanents**
    Direction générale, responsable de la gouvernance, directions métier, systèmes d'information, ressources humaines, juridique, achats, bâtiments, contrôle interne, communication.

  - **Missions**
    Pilotage du budget, suivi des enjeux internes et externes, suivi du plan d'appréciation des risques, approbation du plan de traitement des risques, approbation et suivi du plan d'action, analyse des indicateurs de gouvernance et d'efficacité, traitement des incidents de sécurité, prise de connaissance et validation des résultats d'audit, suivi des améliorations, suivi des plans de sensibilisation et de formation, suivi de la communication, gestion des allocations de ressources.

- **Comité opérationnel**
  - **Composition**
    Responsable de la gouvernance, responsable sécurité, maîtrises d'ouvrage/maîtrise d'œuvre (administrateur réseau, système, gestionnaire des postes de travail, équipe support, responsables des développements, intégration, production, hébergement, gestion des sauvegardes, des projets, représentant RH, achats, logistique, DPO ou représentant juridique).

  - **Missions**
    Faire évoluer le plan d'action, assurer sa déclinaison opérationnelle, suivre les projets, identifier les points durs, résoudre les problèmes, proposer des actions de remédiation, analyser les indicateurs de suivi du plan d'action, remonter les indicateurs consolidés en comité stratégique, analyser les indicateurs de suivi de l'efficience des mesures et des risques résiduels, suivre la gestion des incidents de sécurité, suivre les résultats d'audit, proposer des opportunités d'amélioration au comité stratégique.

6. Sensibilisation et formation

La politique de gouvernance s'engage à mettre en œuvre des actions de sensibilisation et de formation, couvrant la sensibilisation des utilisateurs aux règles de sécurité qui les concernent, la formation en gouvernance pour les participants à la comitologie lorsque nécessaire, ainsi que la formation en sécurité pour garantir les compétences nécessaires aux personnes chargées d'actions spécifiques, avec généralement des plans de sensibilisation et de formation en soutien à cet engagement.

7. Réalisation d'audits

La politique de gouvernance engage à effectuer des audits internes réguliers pour évaluer la mise en œuvre de la gouvernance et l'efficacité des mesures, avec détermination de la fréquence, référence à un plan et à un programme d'audit détaillant les modalités, les périmètres, les compétences nécessaires des auditeurs, etc.

8. Fonctionnement et performance

La politique de gouvernance s'engage à contrôler et évaluer le fonctionnement du système de management en définissant des indicateurs liés à la gouvernance et à la sécurité, en les renseignant, et en remontant et analysant les données par les comités concernés.

9. Communication

La direction s'engage à instaurer des actions de communication, tant internes qu'externes, pour soutenir la mise en place et le fonctionnement du système de gouvernance, pouvant inclure un plan de communication détaillant les besoins, les cibles, les supports, la fréquence, et la gestion des communications en situation de crise.

10. Amélioration en continue

La politique de gouvernance inclut un engagement crucial en faveur de l'amélioration continue, avec la direction s'engageant à faire évoluer le système au fil du temps, à mettre en œuvre le plan d'action, à corriger les non-conformités identifiées par le biais d'audits, de gestion des incidents et d'indicateurs, tout en saisissant les opportunités d'amélioration autant que possible.

Conclusion générale

En résumé, la gouvernance de la sécurité joue un rôle clé dans la gestion de la sécurité d'une organisation. Elle aide à aligner les objectifs stratégiques avec des actions concrètes. En utilisant des règles claires, des audits réguliers, et des évaluations de performance, elle crée un cadre solide. La communication, la sensibilisation, et la formation sont tout autant importantes, tout comme l'engagement pour s'améliorer constamment.

La gouvernance de la sécurité implique une collaboration entre différents groupes pour renforcer la résilience de l'organisation face aux nouveaux risques, tout en respectant les normes et règlements.

Conclusion personnelle

En conclusion, ma plongée dans ce livre sur la gouvernance de la sécurité m'a confronté à un jargon parfois trop qualitatif voire « juridique » ce qui rendait la lecture complexe. De plus, le livre explicite énormément la norme ISO 27'001...

À l'origine, je ne m'attendais pas à une focalisation aussi marquée sur les normes ISO. Cependant, après des recherches approfondies, j'ai réalisé que la gouvernance de la sécurité se concentre davantage sur l'organisation et la structuration au sein de l'entreprise, plutôt que sur des techniques de sécurité et des outils concrets. Cette nuance m'a permis de mieux comprendre l'importance de créer un cadre solide pour anticiper les défis complexes de la sécurité se définissant dans un premier abord davantage « méta ».

Bibliographie

LACOMBE, J.-P., & Nadège, L. (2021). *Management de la sécurité de l'information et ISO 27001.* ENI-Edition.