CyberSkills4All, par Orange Security School
Notes de cours éditées le 1er septembre 2025, 12 h 06 CEST

Management de la sécurité

Yann-Arzel LE VILLIO[1,2]*

Résumé
Ce document présente comment **appréhender les enjeux de conformité et de pilotage du client** afin d'être à même de lister les biens à protéger dans une politique de sécurité et de définir un système de management de sécurité conformes aux normes ISO.Comprendre le périmètre de certification et les plans de continuité définis afin de valider les mesures de sécurité et d'organiser les audits de conformité
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information, de la cybersécurité, et de la cyberdéfense. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

Mots clefs
Gouvernance, SMSI, ISO27001, ISO27002, ISO22301, BCCM BCP, PRA, PCA

[1] *Enseignant Sécurité ESIR*
[2] *Directeur Technique et Scientifique Orange Security School*
***email** : yannarzel.levillio@orange.com –

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/L-Orange-Cyberdef101-M4c-Management.doc.pdf

Table des matières

1 Introduction 3

2 Construction de la Politique de sécurité du système d'information 3

2.1 Politique générale de sécurité . . . 3
2.2 Intégration de la politique de sécurité dans la gouvernance du SI . . . 4
2.3 Comment passe t-on de l'analyse de risques à une PSSI ? . . . 5
2.4 Exemples de chapitres de PSSI . . . 5

3 Système de management de la sécurité de l'information : SMSI 7

3.1 Very short intro to ISO/EIC 27001 . . . 9
3.2 Qu'est ce que le périmètre de certification ? . . . 9
3.3 ISO/EIC 27002 . . . 9

4 Audit Organisationnel 11

4.1 Audit de conformité - DASHBOARD niveau de sécurité . . . 11
4.2 Tableaux de bord de la sécurité . . . 12

5 Continuité d'activité 13

5.1 Qu'est-ce que la continuité d'activité ? . . . 13
5.2 Définitions . . . 13

Table des figures

1 AR2PSSI . . . 6

1. Introduction

Nous aborderons dans ce chapitre la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) au sein des entreprises. Cette activité nécessite une approche méthodique et structurée. En effet, environ 80% du temps consacré à la gestion du SMSI est dédié à la définition des actions à entreprendre et à la démonstration de leur mise en œuvre effective. Cela implique une attention particulière à la conformité avec la norme ISO/IEC 27001, qui fournit un cadre pour établir, mettre en œuvre, maintenir et améliorer le SMSI. Nous présenterons cette norme dans la première partie.

Nous étudierons le cadre Méthodologique qui pourra être utilisé pour soutenir cette démarche. En utilisant par exemple des méthodologies telles que l'ISO/IEC 27005 qui offre un cadre pour la gestion des risques liés à la sécurité de l'information, intégrant des outils comme EBIOS et MEHARI. Ces approches permettent d'identifier, d'évaluer et de traiter les risques de manière systématique, facilitant ainsi la prise de décision éclairée. Nous verrons dans la deuxième partie son utilisation en soutien de la politique et du pilotage pour in fine définir une politique de sécurité claire essentielle pour orienter les actions du SMSI. Le pilotage et l'audit du système, notamment à travers des processus de vérification et de validation (VV), garantissent que les mesures mises en place sont efficaces et conformes aux exigences de la norme ISO/IEC 27001. Cela permet également d'identifier les domaines nécessitant des améliorations.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) joue un rôle clé dans cette organisation. Il doit structurer ses préoccupations et identifier les solutions appropriées pour traiter les risques. Cela inclut l'élaboration d'un plan de traitement des risques, qui doit être régulièrement mis à jour pour refléter l'évolution des menaces et des vulnérabilités.

Il est important de noter que 80% du temps consacré à la gestion du SMSI est souvent statique, axé sur la documentation, la mise en conformité et la gestion des processus. Cela souligne la nécessité d'une approche proactive et rigoureuse pour garantir la sécurité de l'information au sein de l'organisation.

En résumé, l'organisation d'un SMSI efficace repose sur une méthodologie bien définie, une politique claire, un pilotage rigoureux et l'implication active du RSSI. Cela permet de garantir une gestion optimale des risques et de renforcer la sécurité des informations au sein de l'entreprise.

2. Construction de la Politique de sécurité du système d'information

La protection des informations sensibles est essentielle pour maintenir la confiance des clients, respecter les réglementations et assurer la continuité des opérations. La construction d'une Politique de Sécurité des Systèmes d'Information (PSSI) constitue le fondement d'une approche systématique et cohérente en matière de sécurité de l'information. Elle définit les objectifs, les principes directeurs et les mesures de sécurité à mettre en œuvre pour protéger les actifs informationnels de l'organisation. En établissant un cadre clair, la PSSI permet de sensibiliser l'ensemble des collaborateurs aux enjeux de la sécurité, de clarifier les rôles et responsabilités, et de garantir une réponse appropriée face aux menaces potentielles.

Cette partie explorera les différentes étapes de la construction d'une PSSI efficace, en mettant l'accent sur l'importance d'une analyse de risques préalable, la définition des objectifs de sécurité, et l'engagement des parties prenantes. En adoptant une approche méthodique, les organisations pourront non seulement renforcer leur posture de sécurité, mais également créer une culture de la sécurité au sein de leur environnement de travail.

2.1 Politique générale de sécurité

Quelle différence entre une PSG et une PSSI ?

La différence entre une politique de sécurité générale (PSG) et une PSSI réside principalement dans leur portée et leur contenu.

La PSG est un document qui établit les principes et les directives de sécurité au sein de l'ensemble de

l'organisation. Elle couvre un large éventail de domaines, tels que la sécurité physique, la sécurité des ressources humaines et la sécurité des informations. Son objectif est de créer un cadre de sécurité global qui s'applique à tous les aspects de l'organisation, en définissant les attentes et les comportements souhaités en matière de sécurité.

En revanche, la PSSI se concentre spécifiquement sur la **sécurité des systèmes d'information (SSI)**. Ce document aborde des aspects techniques et opérationnels, tels que la gestion des accès, la protection des données et la gestion des incidents de sécurité. La PSSI est généralement élaborée sur la base des résultats d'une analyse de risques, visant à établir des mesures concrètes pour protéger les actifs informationnels de l'organisation.

La PSG et la PSSI sont donc deux documents complémentaires et doivent être alignés pour garantir une approche cohérente et intégrée de la sécurité au sein de l'organisation.

Dans la suite de cette partie, nous nous focaliserons essentiellement sur la PSSI.

2.2 Intégration de la politique de sécurité dans la gouvernance du SI

L'intégration de la politique de sécurité dans la gouvernance du système d'information est essentielle pour assurer une approche cohérente et efficace en matière de sécurité. Pour y parvenir, plusieurs étapes clés doivent être suivies.

Tout d'abord, la politique de sécurité doit être **alignée avec les objectifs stratégiques de l'organisation**. Cela implique de comprendre comment la sécurité de l'information contribue à la réalisation des missions et des objectifs globaux de l'entreprise. En intégrant la sécurité dans la stratégie globale, on s'assure qu'elle est perçue comme une priorité au niveau de la direction. L'adhésion de la direction à tout le processus est indispensable. Nous le reverrons sur plusieurs des sujets.

Ensuite, l'implication des parties prenantes est importante dans le processus d'élaboration et de mise en œuvre de la politique de sécurité. Cela englobe non seulement les équipes de sécurité informatique, mais également les responsables des départements opérationnels, les ressources humaines et la direction. Une communication ouverte et régulière favorise l'adhésion et la compréhension des enjeux de sécurité au sein de l'organisation.

Un autre aspect fondamental est l'établissement de rôles et de responsabilités clairs. Pour une gouvernance efficace, il est essentiel de définir les rôles liés à la sécurité de l'information. Cela inclut la désignation d'un Responsable de la Sécurité des Systèmes d'Information (RSSI) et la création de comités de sécurité qui supervisent la mise en œuvre de la politique. Chaque employé doit également être conscient de ses responsabilités en matière de sécurité.

Par ailleurs, la politique de sécurité doit être intégrée dans les processus de gestion des risques de l'organisation. Cela implique de réaliser régulièrement des analyses de risques et d'évaluer l'efficacité des mesures de sécurité en place. Les résultats de ces analyses doivent être utilisés pour ajuster la politique de sécurité et les contrôles associés.

La formation et la sensibilisation des employés jouent également un rôle crucial dans cette intégration. Il est essentiel de mettre en place des programmes de formation réguliers pour informer le personnel des meilleures pratiques en matière de sécurité et des exigences de la politique. Cela garantit que la politique de sécurité est comprise et appliquée par tous.

Enfin, des mécanismes de suivi et d'évaluation doivent être instaurés pour mesurer l'efficacité de la politique de sécurité. Cela peut inclure des audits réguliers (internes ou externes), des évaluations de conformité (dans le cadre d'un projet de certification ISO27001 par exemple) et des revues de la politique. Les résultats de ces évaluations doivent être analysés afin d'identifier les domaines nécessitant des améliorations et d'adapter la politique en conséquence.

En conclusion, l'intégration de la politique de sécurité dans la gouvernance du système d'information nécessite un alignement stratégique, l'implication des parties prenantes, une définition claire des rôles, une gestion

proactive des risques, une formation continue et un suivi rigoureux. Cette approche garantit que la sécurité de l'information devient une composante essentielle de la gouvernance globale de l'organisation.

2.3 Comment passe t-on de l'analyse de risques à une PSSI ?

La transition de l'analyse de risques à l'élaboration d'une Politique de Sécurité des Systèmes d'Information (PSSI) est un processus structuré qui nécessite plusieurs étapes clés. Cette démarche vise à garantir que la sécurité de l'information est gérée de manière proactive et efficace au sein de l'organisation.

Tout d'abord, la première étape consiste à réaliser une analyse de risques approfondie. Cette analyse implique l'identification des actifs informationnels critiques, l'évaluation des menaces et des vulnérabilités associées, ainsi que l'analyse des impacts potentiels d'un incident de sécurité. En évaluant la probabilité d'occurrence des menaces et en déterminant le niveau de risque associé, l'organisation peut obtenir une vision claire des enjeux de sécurité auxquels elle est confrontée.

Une fois l'analyse de risques effectuée, il est essentiel de développer un plan de traitement des risques. Ce plan doit prioriser les risques identifiés en fonction de leur niveau de criticité et proposer des mesures de sécurité adaptées pour atténuer ces risques. Il est également important d'établir des responsabilités claires pour la mise en œuvre de ces mesures, afin de garantir que chaque action est suivie et exécutée de manière appropriée.

Sur la base des résultats de l'analyse de risques et du plan de traitement, la rédaction de la PSSI peut alors commencer. Ce document doit définir les objectifs de sécurité de l'organisation, énoncer les principes directeurs qui guideront la gestion de la sécurité de l'information, et décrire les rôles et responsabilités des différents acteurs impliqués. La PSSI doit également inclure des mesures de sécurité spécifiques qui seront mises en place pour protéger les actifs informationnels.

Une fois la PSSI rédigée, comme énoncé au paragraphe précédent il est nécessaire de valider le document en obtenant l'approbation des parties prenantes, y compris la direction. La communication de la PSSI à l'ensemble des employés est également essentielle pour assurer une compréhension et une adhésion communes aux exigences de sécurité.

Enfin, la mise en œuvre de la PSSI doit être suivie de près. Cela inclut la formation et la sensibilisation des employés sur les exigences de la politique, ainsi que l'établissement de mécanismes de suivi pour évaluer l'efficacité des mesures de sécurité mises en place. Des audits réguliers et des évaluations de conformité permettront d'identifier les domaines nécessitant des améliorations et d'ajuster la PSSI en fonction des évolutions des risques et des menaces.

En conclusion, la transition de l'analyse de risques à une PSSI efficace repose sur une série d'étapes méthodiques, allant de l'identification des risques à la rédaction et à la mise en œuvre d'une politique de sécurité claire et adaptée. Cette approche permet de garantir une gestion proactive de la sécurité de l'information au sein de l'organisation.

2.4 Exemples de chapitres de PSSI

Voir ci-dessous quelques exemples de chapitre d'une PSSI.

Protocoles d'accès autorisés La sécurité des accès aux équipements est primordiale pour garantir l'intégrité et la confidentialité des données. Seuls les protocoles d'accès sécurisés sont autorisés. Les protocoles SSHv3 et HTTPS, utilisant des certificats générés par l'Infrastructure de Gestion de Clés (IGC) de l'entreprise, sont les seuls acceptés pour les connexions à distance.

L'accès aux machines via le protocole Remote Desktop Protocol (RDP) de Microsoft est également encadré par des conditions strictes. Ce protocole est limité à un accès interne uniquement et doit se faire via un réseau d'administration dédié. En revanche, l'utilisation de protocoles non sécurisés, tels que TELNET, est strictement interdite afin de prévenir toute vulnérabilité potentielle.

Protocoles et méthodes de supervision autorisés Pour assurer une surveillance efficace des équipements,

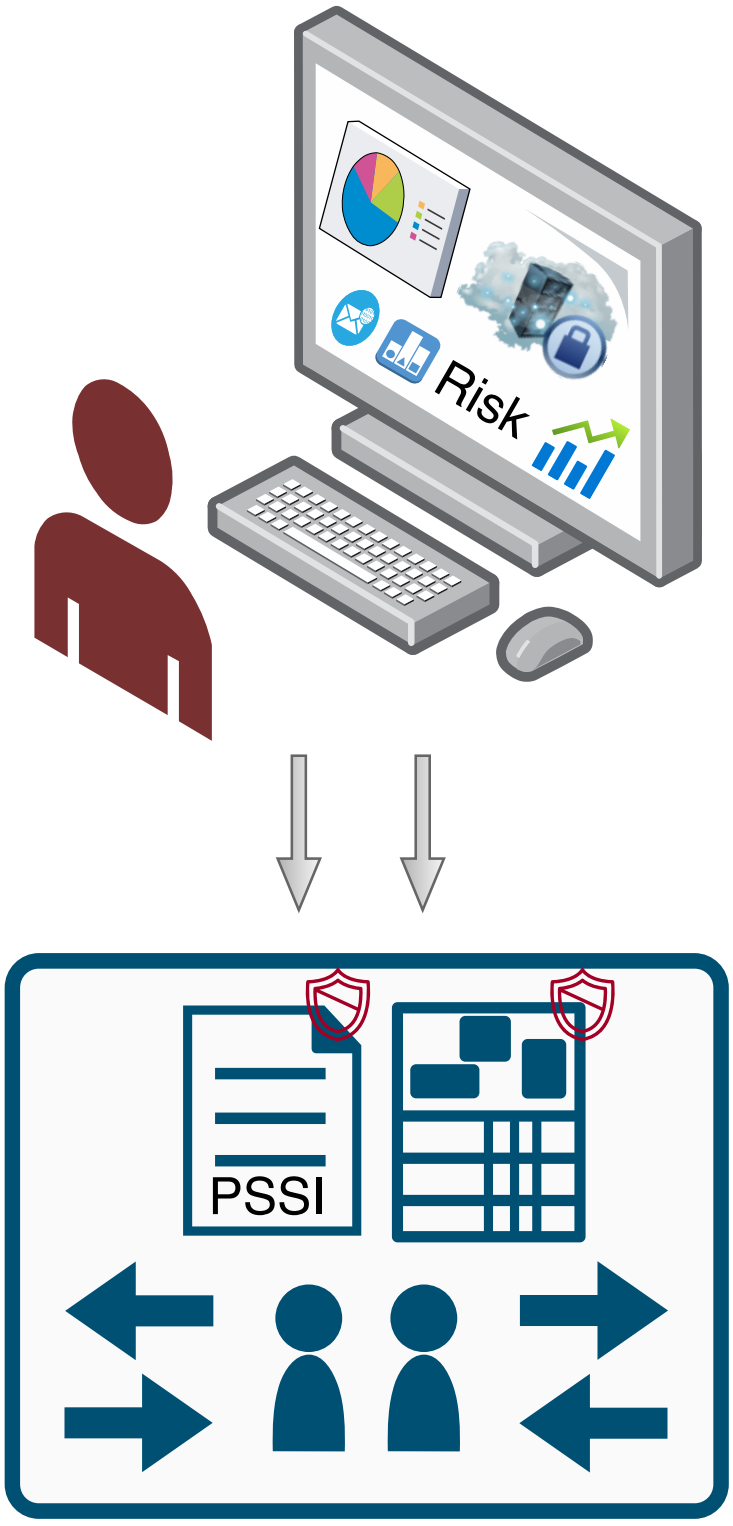

Figure 1. AR2PSSI

seuls les protocoles de supervision de type SNMPv3 sont autorisés. Ces protocoles doivent respecter les configurations spécifiées dans la documentation dédiée, notamment l'utilisation de certificats pour garantir la sécurité des communications. Cette approche permet de maintenir un niveau élevé de sécurité tout en assurant une supervision adéquate des systèmes.

Politique de mot de passe La gestion des mots de passe est un élément clé de la sécurité des accès. Il est impératif que tous les utilisateurs respectent une politique de mot de passe stricte, incluant des exigences telles que la complexité, la longueur minimale et le renouvellement régulier des mots de passe. Cette politique vise à réduire les risques d'accès non autorisé aux systèmes et aux données sensibles.

Gestion des fournisseurs La gestion des fournisseurs doit également être intégrée dans la politique de sécurité. Les accès aux systèmes et aux données par des tiers doivent être soigneusement contrôlés et limités. Les fournisseurs doivent se conformer aux mêmes exigences de sécurité que celles imposées aux employés internes, notamment en ce qui concerne les protocoles d'accès et la gestion des mots de passe. Des audits réguliers doivent être effectués pour s'assurer que les fournisseurs respectent ces normes de sécurité.

3. Système de management de la sécurité de l'information : SMSI

Selon la norme ISO 9000, un système de management est défini comme un ensemble de processus interconnectés ou interactifs, qui sont mis en œuvre par une organisation pour établir, mettre en œuvre, maintenir et améliorer la gestion de la qualité. Ce système vise à atteindre les objectifs de qualité de l'organisation en assurant la cohérence et l'efficacité de ses processus.

Toujours sela la norme ISO 9000, les éléments clés d'un système de management sont :

- processus interconnectés : le système repose sur une série de processus qui interagissent pour atteindre les objectifs de qualité. Chaque processus a ses propres activités, ressources, et résultats attendus ;
- approche processus : la norme encourage une approche basée sur la gestion des processus, permettant une meilleure compréhension, gestion et amélioration continue ;
- orientation client : le système vise à satisfaire les exigences des clients et à améliorer leur satisfaction ;
- amélioration continue : la norme insiste sur la nécessité d'améliorer constamment l'efficacité du système de management ;
- leadership : la direction doit s'engager activement pour établir une vision claire et soutenir la mise en œuvre du système ;
- implication du personnel : la participation et la compétence du personnel sont essentielles pour le succès du système ;
- gestion des ressources : la disponibilité et la gestion efficace des ressources (humaines, matérielles, informationnelles) sont fondamentales ;
- évaluation et amélioration : la surveillance, la mesure, l'analyse et l'audit des processus permettent d'identifier les opportunités d'amélioration.

Pourquoi alors définir un système de management et se lancer dans un processus de certification ? Car les apports sont nombreux et contribuent à la performance globale de l'organisation. Voici quelques éléments principaux :

- Amélioration de la qualité : Permet de mieux répondre aux attentes des clients en assurant une cohérence et une conformité des produits et services.
- Satisfaction client accrue : En se concentrant sur la satisfaction des besoins et attentes des clients, l'organisation peut renforcer leur fidélité.
- Efficacité opérationnelle : La gestion structurée des processus permet d'optimiser les ressources, réduire les coûts et limiter les erreurs.
- Meilleure gestion des risques : La mise en place d'un système de management facilite l'identification, l'évaluation et la maîtrise des risques liés aux activités.

- Engagement et motivation du personnel : La participation active des employés dans un cadre clair et structuré favorise leur implication et leur développement professionnel.
- Amélioration continue : Le système encourage une démarche d'amélioration constante, permettant à l'organisation de s'adapter aux évolutions du marché et de ses environnements.
- Reconnaissance et crédibilité : La certification ISO ou d'autres labels issus du système de management renforcent la crédibilité de l'organisation auprès de ses partenaires, clients et parties prenantes.
- Conformité réglementaire : Facilite le respect des exigences légales et réglementaires applicables à l'activité.

Quelle méthode utiliser pour l'amélioration continue des processus ? La référence des méthodes est le cycle de Deming ou PDCA pour Plan (Planifier), Do (Réaliser), Check (Vérifier) et Act (Agir). le cycle PDCA sert à structurer la démarche d'amélioration continue. Il permet à l'organisation de planifier ses objectifs et ses processus, de mettre en œuvre ces processus, de vérifier leur efficacité, puis d'agir pour corriger ou améliorer les pratiques. Ce cycle favorise une gestion dynamique et proactive, assurant que le système évolue en permanence pour mieux répondre aux exigences et attentes (donc instaurer un climat de confiance), tout en améliorant la performance globale.

Il existe plusieurs systèmes de management, comme celui sur la qualité (ISO 9001), l'environnement (ISO 14001) mais nous allons nous attarder plus précisement dans ce chapitre sur celui de la sécurité de l'information (SMSI) l'ISO 27001. Le système de management d la continuité d'activité (SMCA) ISO 22301 sera lui abordé un peu plus loin dans ce chapitre.

Définition du SMSI Un SMSI, ou Système de Management de la Sécurité de l'Information, est un cadre organisé qui permet à une organisation de gérer de manière systématique la sécurité de ses informations. Selon la norme ISO/IEC 27001, il s'agit d'un ensemble de politiques, de processus, de procédures, de structures organisationnelles et de ressources qui sont mis en place pour protéger la confidentialité, l'intégrité et la disponibilité des informations.

Un SMSI repose sur plusieurs éléments clés. Tout d'abord, il inclut une politique de sécurité qui définit les orientations et les engagements de l'organisation en matière de sécurité de l'information (cf. le chapitre précédent pour plus de détails sur les politiques). Ensuite, il implique une analyse des risques, permettant d'identifier, d'évaluer et de traiter les menaces potentielles pesant sur les actifs informationnels.

L'organisation de la sécurité est également essentielle, avec la mise en place de structures, de responsabilités et de ressources dédiées à la gestion de la sécurité. Des contrôles de sécurité, tant techniques qu'organisationnels et physiques, sont déployés pour protéger l'information. Il est également crucial de disposer d'un processus de gestion des incidents, afin de détecter, répondre et se remettre rapidement en cas de problème. La sensibilisation et la formation du personnel jouent un rôle important pour garantir que tous comprennent les enjeux de sécurité. Enfin, le système doit faire l'objet d'une amélioration continue, grâce à la surveillance, aux audits et aux revues régulières pour assurer son efficacité et son évolution.

Pour mettre en œuvre un SMSI, il est recommandé que la direction s'engage activement dans le projet. Il faut adopter une approche basée sur les risques, en priorisant les actions en fonction des menaces identifiées. La communication interne doit être claire et régulière pour sensibiliser l'ensemble du personnel. La documentation précise des politiques, procédures et mesures est également essentielle. Enfin, il est important de réaliser des audits réguliers pour vérifier la conformité et l'efficacité du système, et ainsi l'améliorer en permanence.

Que trouve-t-on alors dans la norme ISO 27001 ?

Dans la norme ISO 27001, on trouve tout d'abord une description claire des exigences que doit respecter un SMSI. Cela inclut la nécessité d'établir une politique de sécurité, d'évaluer et de traiter les risques liés à la sécurité de l'information, ainsi que de définir des objectifs et des plans d'action pour atteindre ces objectifs.

La norme détaille également les exigences relatives à la gouvernance, à la gestion des ressources, à la sensibilisation du personnel, ainsi qu'à la documentation et à la gestion des enregistrements. Elle insiste sur

l'importance de la surveillance, de l'audit interne, des revues de direction et de l'amélioration continue du système.

En complément, la norme ISO 27001 est accompagnée d'un ensemble de contrôles de sécurité (définis dans l'annexe A) que l'organisation peut choisir d'appliquer en fonction de ses risques spécifiques. Ces contrôles couvrent un large spectre, allant de la gestion des accès à la sécurité physique, en passant par la gestion des incidents et la continuité des activités.

Quel est le but d'être certifié ISO 27001 ?

Le but principal d'obtenir la certification ISO 27001 est de démontrer à ses partenaires, clients et parties prenantes que l'organisation a mis en place un système de gestion de la sécurité de l'information efficace et conforme aux meilleures pratiques internationales. Cette certification vise à renforcer la confiance en assurant que les actifs informationnels sont protégés contre les risques, les menaces et les vulnérabilités.

En étant certifiée, une organisation peut également bénéficier d'une meilleure gestion des risques liés à la sécurité, réduire la probabilité d'incidents de sécurité, et assurer la continuité de ses activités. De plus, la certification ISO 27001 peut constituer un avantage concurrentiel en attestant de la sérieux et du professionnalisme de l'organisation en matière de sécurité de l'information.

3.1 Very short intro to ISO/EIC 27001

3.2 Qu'est ce que le périmètre de certification ?

Le périmètre de certification ISO 27001 est le point de départ de tout projet de certification. Il est indispensable de bien définir quel élément du système d'information devra respecter les exigences de la norme. Le périmètre peut inclure une application, une ferme de serveurs, une équipe de collaborateurs, un data-center, etc. Il doit être clairement délimité et documenté pour assurer une compréhension commune au sein de l'organisation et faciliter la mise en œuvre des contrôles et des processus nécessaires. Une définition précise du périmètre permet également d'évaluer plus efficacement les risques, de cibler les ressources appropriées et de garantir la conformité aux exigences de la norme tout au long du processus de certification.

3.3 ISO/EIC 27002

La norme ISO/IEC 27002 est un guide de bonnes pratiques et de recommandations pour la gestion de la sécurité de l'information. Elle fournit un ensemble de contrôles de sécurité détaillés que les organisations peuvent mettre en œuvre pour gérer efficacement les risques liés à la sécurité de l'information.

Cette norme offre un catalogue de contrôles de sécurité répartis en plusieurs domaines, tels que la gestion des accès, la sécurité physique, la gestion des incidents, la continuité des activités, etc. Elle sert de référence pour sélectionner, mettre en œuvre et gérer ces contrôles en fonction des risques spécifiques à chaque organisation. Contrairement à la norme ISO 27001, elle ne définit pas d'exigences obligatoires, mais fournit des recommandations pour renforcer la sécurité.

Quelles différences entre les deux normes ISO 27001 et ISO 27002 ?

Comme vu aux paragraphes précédents, la norme ISO 27001 définit les exigences pour établir, mettre en œuvre, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI). Elle est donc une norme certifiable, qui permet à une organisation d'obtenir une certification officielle. La norme ISO 27002 est elle un guide de bonnes pratiques, destiné à aider à la sélection et à la mise en œuvre de contrôles de sécurité. Elle n'est pas certifiable en soi.

En conclusion, on peut retenir les différences suivantes :

- ISO 27001 est une norme normative avec des exigences obligatoires pour la certification ;
- ISO 27002 est une norme de recommandations, fournissant des lignes directrices pour la mise en œuvre ;
- ISO 27001 sert à établir un cadre de gestion de la sécurité, avec des processus, des politiques et des

contrôles ;
- ISO 27002 accompagne cette démarche en proposant des contrôles concrets et des bonnes pratiques pour leur mise en œuvre.

Quelles sont les mesures ?

La norme ISO/IEC 27002 propose un ensemble de 114 contrôles de sécurité répartis en 14 domaines ou sections principales. Ces contrôles couvrent un large éventail de mesures visant à gérer efficacement les risques liés à la sécurité de l'information.

Ces contrôles sont regroupés en 14 domaines, tels que :

1. Politique de sécurité de l'information
2. Organisation de la sécurité de l'information
3. Sécurité des ressources humaines
4. Gestion des actifs
5. Contrôle d'accès
6. Cryptographie
7. Sécurité physique et environnementale
8. Sécurité des opérations
9. Sécurité des communications
10. Acquisition, développement et maintenance des systèmes d'information
11. Relations avec les fournisseurs
12. Gestion des incidents de sécurité de l'information
13. Aspects de la sécurité de l'information dans la gestion de la continuité d'activité
14. Conformité

Voir ci-dessous quelques exemples concrets de mesures de sécurité :

Contrôles d'accès

- Mise en place de mots de passe robustes et de politiques de gestion des mots de passe.
- Utilisation de l'authentification à deux facteurs pour accéder aux systèmes sensibles.
- Attribution de droits d'accès en fonction du principe du moindre privilège, pour limiter l'accès aux seules informations nécessaires à chaque utilisateur.

Sécurité physique :

- Installation de caméras de surveillance et de systèmes d'alarme dans les data-centers et autres zones sensibles.
- Contrôle d'accès par badge ou biométrie pour entrer dans les locaux sensibles.
- Protection contre les incendies et les inondations dans les centres de données (Datacenters).

Gestion des incidents :

- Mise en place d'un plan de réponse aux incidents pour détecter, analyser et répondre rapidement aux cyberattaques ou incidents de sécurité.
- Formation du personnel à la reconnaissance et à la signalisation des incidents de sécurité.

Sécurité des réseaux :

- Utilisation de pare-feu et de systèmes/sondes de détection/prévention d'intrusions (IDS/IPS).

- Chiffrement des données transmises via des protocoles sécurisés comme TLS ou IPSEC.
- Segmentation des réseaux pour limiter la propagation d'éventuelles attaques.

Sauvegarde et continuité :

- Réalisation régulière de sauvegardes des données critiques, stockées hors site ou dans le cloud.
- Mise en place de plans de reprise d'activité (PRA) pour assurer la continuité en cas d'incident majeur.

Sensibilisation et formation :

- Organisation de sessions de formation pour sensibiliser les employés aux risques liés à la sécurité (phishing, ingénierie sociale, etc.).
- Envoi de campagnes de sensibilisation régulières pour maintenir une vigilance constante.

Pour conclure sur ce chapitre, l'implémenteur d'un système de management de la sécurité de l'information suit une démarche structurée pour sélectionner les mesures de la norme ISO 27002 à appliquer. Tout d'abord, il réalise une analyse des risques afin d'identifier les actifs, les menaces et les vulnérabilités, puis d'évaluer leur impact potentiel. Sur la base de cette analyse, il détermine quels risques doivent être traités en priorité. Ensuite, il définit le contexte de l'organisation, ses enjeux et ses objectifs en matière de sécurité, ce qui l'aide à orienter la sélection des contrôles. Il consulte la liste des 114 contrôles de la norme ISO 27002 et choisit ceux qui sont pertinents pour réduire les risques identifiés. La sélection doit respecter le principe du « juste nécessaire », en appliquant uniquement les contrôles qui apportent une réelle valeur ajoutée. Après cela, il priorise ces contrôles en fonction de leur efficacité, de leur coût et de leur complexité, puis élabore un plan de déploiement avec des échéances et des responsabilités. Les mesures choisies sont ensuite mises en œuvre concrètement, accompagnées de procédures et de formations pour garantir leur efficacité. La documentation est mise à jour pour refléter ces mesures. Enfin, un suivi régulier permet d'évaluer leur performance, et si nécessaire, la sélection des mesures est révisée pour s'adapter aux changements dans l'organisation ou dans le contexte des risques.

4. Audit Organisationnel

4.1 Audit de conformité - DASHBOARD niveau de sécurité

Ici on parle d'audit de conformité, compliancy ou audit organisationnel. On ne parle pas d'audits techniques à la recherche de vulnérabilités d'un produit ou d'un système qui compromettrait la confidentialité, l'intégrité et/ou la disponibilité des données. Le but est de vérifier que l'organisation, les procédures et les actions sont conformes. Cette conformité peut être par à rapport à une norme, ISO27001 par exemple, ou plus simplement à une politique et des objectifs fixés par la direction de l'entreprise.

Comment préparer une certification ? Le responsable du projet de certification doit s'assurer que le périmètre qui sera audité soit conforme aux exigences de la norme. Pour ce faire, il doit préparer les documents listés ci-dessous et s'assurer de leur existence et de la qualité de leur contenu. Cette liste est non exhaustive :

1. Déclaration de portée du SMSI. Il est impératif de définir clairement le périmètre du Système de Management de la Sécurité de l'Information (SMSI). En particulier les zones, processus, sites, actifs inclus ou exclus. Par exemple, le périmètre du SMSI de notre entreprise SEC*** couvre le cloud privé hébergé par le centre de données situé à Paris, les serveurs hébergeant les applications métiers, et le personnel de l'équipe informatique à Paris.
2. Politique de sécurité de l'information. Comme vu aux paragraphes précédents c'est le document qui formalise l'engagement de l'organisation en matière de sécurité.
3. Liste des actifs et leur classification. C'est l'inventaire des actifs informationnels et leur classification. Par exemple, le serveur hébergeant le moteur de transformation des données pour utilisation avec l'IA, classifié confidentiel, et situé au centre de données à Paris.
4. Analyse de contexte et parties prenantes. Ce document contient l'identification des enjeux et des exigences des parties prenantes.

5. Évaluation des risques et traitement des risques. Quelle méthodologie d'évaluation des risques est utilisée (EBIOS, ISO27005, etc.) ? Quels sont les risques identifiés et le plan de traitement associé ?
6. Objectifs de sécurité et plans d'action. Quels sont les objectifs liés à la sécurité de l'information et quels sont les plans pour atteindre ces objectifs ? Par exemple, un des objectifs pourrait être de réduire le nombre d'incidents de sécurité de 20 % d'ici la fin de l'année. Le plan d'action associé pour y arriver pourrait être de renforcer la sensibilisation du personnel et mettre à jour les procédures de sécurisation des serveurs.
7. Procédures opérationnelles. Ces documents formalisent l'ensemble des procédures relatives à la gestion de la sécurité. Elles doivent être connus et contenir des instructions spécifiques pour les processus clés. Par exemple, les procédures de gestion des accès ou encore de destruction des supports en fin de projet.
8. Registres de formation, sensibilisation et compétences. Quels sont les modules de formation de sensibilisation utilisés ? Il est important aussi de conserver les preuves d'action de formation de sensibilisation du personnel (feuilles d'émargement collectées à la fin des sessions de formation).
9. Documents de contrôle et de surveillance : Audits internes, revues de direction, actions correctives. Par exemple, le rapport d'audit interne daté de février 2025 sur l'applicatif IAGen X, la revue de direction du 10 mars 2025, ainsi que les actions correctives mises en œuvre suite à un incident en janvier 2025.
10. Contrats et accords avec les tiers : Accords de confidentialité, contrats de sous-traitance. Par exemple le contrat de sous-traitance avec le fournisseur de cloud public, incluant des clauses de sécurité et de confidentialité, signé le 1er janvier 2025.

L'ensemble de ces documents et des indicateurs collectés sur ces sujets permettent d'alimenter le tableau de bord de la sécurité. Le RSSI l'utilisera pour évaluer le niveau de sécurité de l'entreprise en fonction de ses objectifs et contraintes réglementaires.

4.2 Tableaux de bord de la sécurité

Les tableaux de bord de la sécurité jouent un rôle clé dans la gestion du système de management de la sécurité de l'information, en particulier lorsque l'organisation vise à certifier un périmètre selon la norme ISO 27001. En effet, cette norme exige la mise en place de mesures permettant de suivre, d'évaluer et d'améliorer en continu la sécurité du système d'information. Dans ce contexte, le tableau de bord devient un outil central pour démontrer la maîtrise des risques et le respect des exigences de la norme.

Par exemple, la clause 9 de la norme ("Évaluation de la performance") impose d'analyser les résultats et de mesurer l'efficacité du système de management de la sécurité de l'information. Les tableaux de bord permettent justement d'illustrer ces analyses à travers des indicateurs concrets sur la gestion des vulnérabilités ou des incidents de sécurité par exemple.

Plus précisement, citons quelques indicateurs importants de suivre dans le tableau de bord (liste non-exhaustive) :

- nombre d'incidents de sécurité traités ;
- taux de non-conformité détectées lors des audits internes et leur évolution dans le temps ;
- pourcentage de correctifs de sécurité appliqués dans les délais définis par les politiques internes, en lien avec le contrôle A.12.6.1 ("Gestion des vulnérabilités techniques") ;
- nombre de revues d'accès aux comptes sensibles réalisées sur la période, pour démontrer la maîtrise des droits d'accès (contrôle A.9).

Les tableaux de bord constituent également un support précieux lors des audits internes et externes de certification. Ils facilitent la traçabilité des actions, l'analyse des tendances, le suivi des plans d'actions correctifs ainsi que la restitution des preuves exigées par les auditeurs.

Par exemple, en cas de constat d'anomalie, le tableau de bord peut montrer rapidement qu'un incident a été détecté, analysé, traité et clôturé, avec l'ensemble des preuves et des délais associés. Cette capacité de démonstration s'avère essentielle pour justifier la conformité et l'amélioration continue exigées par la norme.

Lorsque l'on élabore un tableau de bord pour un périmètre certifié selon la norme ISO 27001, il est essentiel d'apporter une attention particulière à plusieurs aspects clés. Il convient tout d'abord de s'assurer que les

indicateurs suivis concernent exclusivement le périmètre défini dans la déclaration d'applicabilité (SoA). Cela garantit la cohérence entre les informations présentées et les exigences de la norme. Il est important de vérifier que chaque indicateur retenu contribue directement aux objectifs précisés dans la politique de sécurité et dans le plan de gestion des risques du SMSI. Il est recommandé de documenter systématiquement les sources, les méthodes de collecte et la fréquence de mise à jour des données présentées dans le tableau de bord. Ces éléments serviront de preuves lors des audits. Il est nécessaire de conserver un historique des indicateurs, afin de pouvoir démontrer l'amélioration continue du système de management de la sécurité de l'information, telle qu'exigée par l'ISO 27001. La gestion de la confidentialité et de l'intégrité des informations affichées doit être irréprochable, i.e. les accès aux tableaux de bord doivent être restreints aux personnes habilitées et les supports sécurisés pour éviter toute fuite ou modification non autorisée. Enfin, il est crucial d'adapter les tableaux de bord et les rapports aux besoins des audits internes et externes, afin de faciliter la traçabilité des actions et la démonstration de la conformité lors du processus de certification.

En conclusion, pour un périmètre soumis à la certification ISO 27001, le tableau de bord de la sécurité devient un élément stratégique. Il offre une visibilité en temps réel sur l'état de la sécurité, facilite la démonstration de conformité aux exigences de la norme et soutient l'amélioration continue du système de management. Bien conçu et aligné avec la démarche ISO 27001, il renforce la crédibilité de l'organisation lors des audits et participe activement au maintien de la certification.

5. Continuité d'activité

5.1 Qu'est-ce que la continuité d'activité ?

Bases de la norme ISO22301

La continuité d'activité consiste à mettre en place des mesures pour que les opérations essentielles d'une organisation puissent continuer, même en cas d'incident ou de crise. Par exemple, une entreprise de e-commerce peut prévoir un plan pour continuer à traiter les commandes si son centre de données tombe en panne ou si une cyberattaque bloque ses systèmes. De même, une usine peut avoir des plans pour continuer à produire en utilisant des fournisseurs alternatifs ou en déplaçant temporairement ses activités.

La norme ISO 22301 fournit un cadre pour structurer cette démarche. Elle insiste sur l'importance d'évaluer les risques, comme une inondation ou une panne électrique, et de planifier en conséquence. Par exemple, une banque peut élaborer un plan pour assurer la continuité de ses services en cas de coupure de courant ou de cyberattaque, en utilisant des centres de secours ou des sauvegardes de données.

La norme demande aussi à la direction de s'engager activement dans cette démarche. Elle doit définir des objectifs clairs, comme réduire le temps de reprise après un incident, et allouer les ressources nécessaires. Ensuite, il faut tester régulièrement ces plans, par exemple en organisant des exercices pour vérifier si les employés savent comment réagir en cas d'urgence.

Enfin, la norme encourage une amélioration continue. Si un test révèle une faiblesse, l'organisation doit ajuster ses plans pour mieux faire face à de futurs incidents. Par exemple, si une entreprise découvre que ses sauvegardes de données ne sont pas suffisantes, elle doit renforcer ses mesures de sauvegarde pour garantir la disponibilité des informations critiques.

5.2 Définitions

Sources : NIST, ANSSI

- Business Impact Analysis (BIA) Process of analyzing operational functions and the effect that a disruption might have on them.
- Business Continuity Plan (BCP) The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

- Plan de Continuité d'Activité (PCA) / Disaster Recovery Plan (DRP) A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
- Plan de Reprise d'Activité (PRA)