**CyberSkills4All, par Orange Security School**
**Notes de cours éditées le 30 janvier 2025, 11 h 25 CET**

# 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



# Table des figures

# 1. SMSI Intro

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.

Ensuite 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.

Rôle du Responsable de la Sécurité des Systèmes d'Information (RSSI) 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,

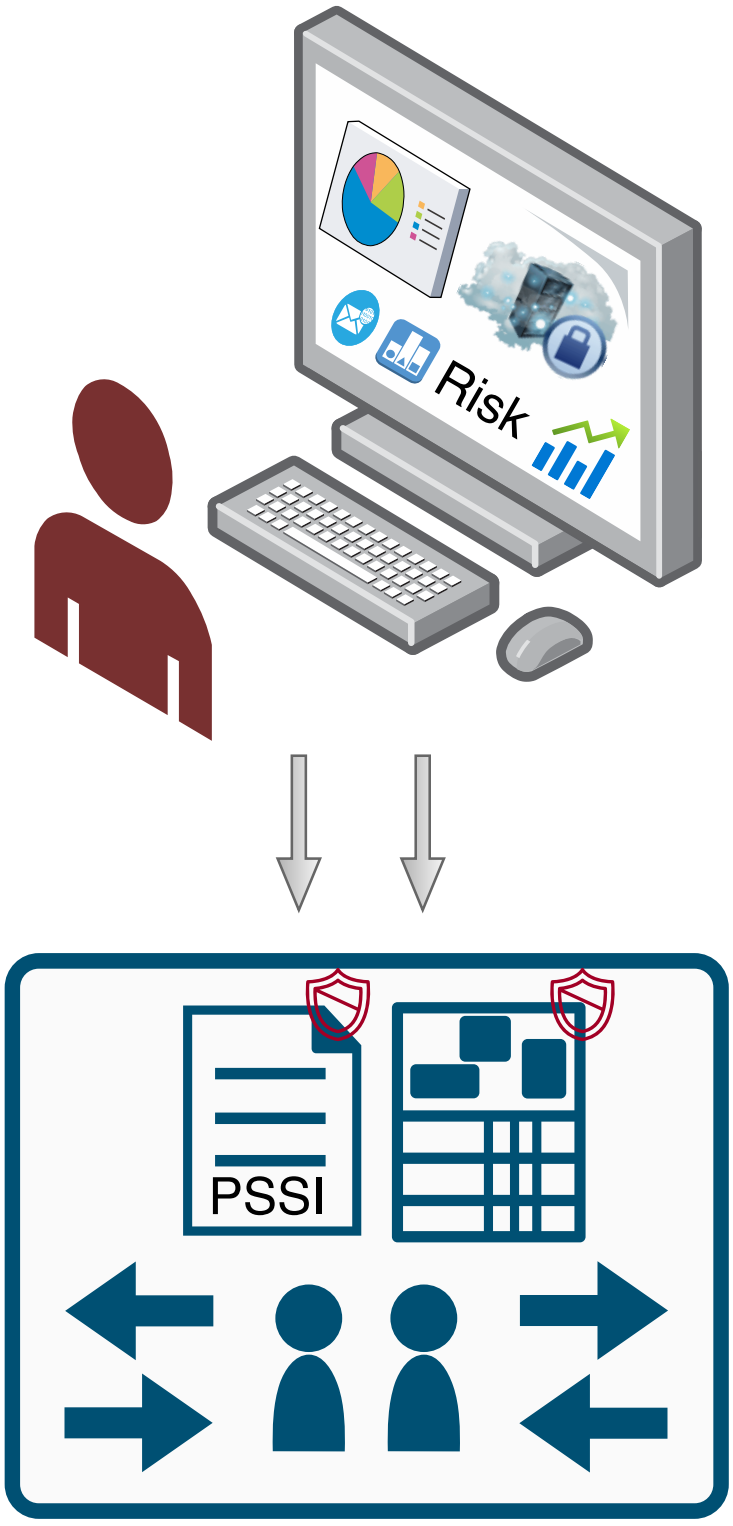


**Figure 1.** AR2PSSI

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

normatif ISO27001 ; périmètre de certification & mesures ISO27002 à appliquer

Définition SMSI (voir cours Fadoua sur l'intro)

## 3.1 Very short intro to ISO/EIC 27001

## 3.2 Historique puis Basiques

que trouve t on dans la norme ?

## 3.3 Qu'est ce que le périmètre de certification ?

Le périmètre de certification 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.

## 3.4 ISO/EIC27002, quelles sont les mesures de sécurité ?

Exemples à donner

# 4. Audit de conformité - DASHBOARD niveau de sécurité

# 5. Contrôles réguliers des procédures et indicateurs clés

# 6. Continuité d'activité

## 6.1 Qu'est-ce que la continuité d'activité ?

Bases de la norme ISO22301

## 6.2 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)