

4 - Management de la sécurité

Éléments de cybersécurité d'entreprise

Yann-Arzel LE VILLIO

yannarzel.levillio@orange.com

<http://campus.orange.com>

CyberSkills4All

Direction technique & scientifique OSS

Publication Éléments de cours CYBERSKILLS4ALL



CYBERDEF 101

Éléments de cybersécurité
et de cyberdéfense
d'entreprise



Abstract



⚙️ Hashtags : Gouvernance, SMSI, ISO27001, ISO27002, ISO22301, BCCM BCP, PRA, PCA

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

Sommaire

1. SMSI Intro

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

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

4. Audit de conformité - DASHBOARD
niveau de sécurité

5. Contrôles réguliers des procédures et
indicateurs clés

6. Continuité d'activité



Gouvernance et management de la sécurité



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

- # Organisation des entreprises
- # Gouvernance : cadre, méthodologie, objectifs
- # Comment raisonne un Responsable de la sécurité de l'information (RSSI) ?

Construction de la Politique de sécurité du système d'information



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

Politique générale de
sécurité

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Contenu du texte ce que l'on veut comme par exemple

- # Définition d'une politique de sécurité
- # Intégration de la politique de sécurité dans la gouvernance du SI

Concept de PSG



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

Intégration de la
politique de sécurité
dans la gouvernance
du SI

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

La politique de sécurité générale (PSG) est généralement basée sur l'architecture de l'ISO/EIC 27001, et donne le cadre général de conformité pour les projets, les organisations sous-jacentes (divisions, filiales), les produits ainsi que l'organisation des responsabilités.

Cette PSG est déclinée en différentes politiques de sécurité par secteurs (souvent structurées par les chapitres de l'ISO/EIC 27001)

IAM

Filtrage et sécurité périmétrique

Détection et remédiation

continuité d'activité

AR2PSSI



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

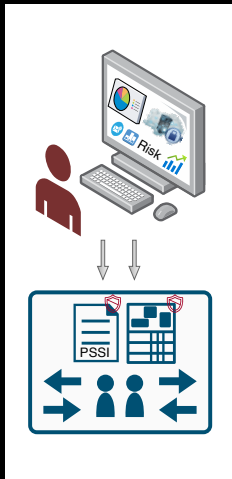
Comment passe-t-on
de l'analyse de
risques à une PSSI ?

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité



Approche par les risques



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Identification des biens essentiels à protéger

Intégration dans la politique de sécurité

Exemples de chapitres de PSSI



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

Exemples de
chapitres de PSSI

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Gestion de l'administration des équipements

- protocoles d'accès autorisés : SSHv3, HTTPs, interdiction de TELNET
- protocoles de supervision autorisés : SNMPv3

Politique de mot de passe

Gestion des fournisseurs

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



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

1. Présentation de la norme ISO/EIC 27001
2. Périmètre de certification
3. Mesures de sécurité : ISO/EIC 27002

Very short intro to ISO/EIC 27001



Quel est le but d'ISO 27k1? Pourquoi l'utiliser?

SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

Very short intro to
ISO/EIC 27001

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Périmètre de certification



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

Qu'est ce que le
périmètre de
certification ?

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Quel est le périmètre de certification ?

SOA : définition, rôle -> BOF

ISO/EIC27002



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

ISO/EIC27002,
quelles sont les
mesures de sécurité ?

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Définition mesures de sécurité

Exemples

Audit de conformité



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Exemples :

- # nb d'incidents critiques
- # % remediation vulnérabilité critiques
- # % parc administrés suivant les règles de la politique
- # nombre de PKI déployées, %PKI dans les équipes sécurité incluses dans le périmètre de certification
- # % de personnes sensibilisées

Continuité d'activité : ISO22301



SMSI Intro

Construction de
la Politique de
sécurité du
système
d'information

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

Audit de
conformité -
DASHBOARD
niveau de sécurité

Contrôles
réguliers des
procédures et
indicateurs clés

Continuité
d'activité

Définitions

- # Business Impact Analysis (BIA)
- # Business Continuity Plan (BCP)
- # Plan de Continuité d'Activité (PCA) / Disaster Recovery Plan (DRP)
- # Plan de Reprise d'Activité (PRA)



des questions ?

Contributions

Les notes et les présentations sont réalisées sous \LaTeX . Vous pouvez contribuer au projet du cours CYBERDEF101. Les contributions peuvent se faire sous deux formes :

- # Corriger, amender, améliorer les notes publiées. A chaque session des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- # Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de vos expertises dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : [edufaction/CYBERDEF101](https://github.com/edufaction/CYBERDEF101) ^a.

a. <https://github.com/edufaction/CYBERDEF101>



Mises à jour régulières

Vérifiez la disponibilité d'une version plus récente de

L-Orange-Cyberdef101-M4c-Management.przt.pdf sur GITHUB CYBERDEF ¹



2025 eduf@ction - Publication en Creative Common BY-NC-ND



CYBERDEF 101

Eléments de cybersécurité
et de cyberdéfense
d'entreprise

