ISO 27001

Arrêter de regarder le doigt, concentrez-vous sur la lune

Les pièges de l'appréciation des risques…entre autres

APSSIS — 2026

INTRODUCTION

1

Les tribulations d'un RSSI

Risques de fuite de données : sidération face à la complexité apparente

2

La sidération des acteurs

Risques et opportunités du SMSI : une liste qui brûle les doigts

3

Le vide des consultants

Appréciation des risques : méthodes pléthoriques, résultats creux

LA LUNE ET LE DOIGT – ET PAS SEULEMENT DANS LA 27001

La préparation à une certification ISO 27001 et les premières années d'une certification se heurtent à quelques difficultés, qui poussent les nouveaux venus soit à faire de la sur-qualité aussi inutile que coûteuse, soit à manquer totalement la cible de ce qu'exige vraiment la norme.

Appréciation des risques, R&O et prévention de la fuite de données : au travers de ces trois exemples, nous décortiquerons à la fois les exigences réelles de la 27001, comment les aborder et les intégrer à son SMSI. Ces 3 cas d'usage illustrent une même erreur : confondre la méthode (le doigt) avec l'objectif (la lune).

Parce que la complexité n'est pas forcément là où on croit la trouver.

Décortiquer la norme — comprendre l'objectif derrière la méthode

LE CONDUCTEUR

✗

Démonter les idées reçues

EBIOS, ISO 27005, scénarios de menaces : ce que la norme ne dit pas.

✓

Ce que la norme exige vraiment

Processus PDCA, cohérence, validation en revue de direction.

◎

Cas concrets illustratifs

Le Louvre, les fuites de données, le contexte climatique.

APPRÉCIATION DES RISQUES — La pratique courante

1. Organiser des ateliers avec les métiers (MOA, DSI, etc.)
2. Utiliser des bibliothèques de risques formalisées
3. Coller des post-it de toutes les couleurs sur des tableaux blancs
4. Dérouler des scénarii EBIOS MACHINCHOSE
5. Faire valider le résultat par les métiers, dans un beau fichier Excel avec 36 onglets et des couleurs partout

✓

Cela fonctionne…

En apparence.

APPRÉCIATION DES RISQUES — La réalité

✗ ...mais cela ne sert à rien (30j d'atelier avec les métier , lol lol lol)

✗ ...cela ne répond absolument pas aux exigences d'un SMSI : qui peut le plus a surtout trop de thune relativement à sa maturité

✗ ...cela ne rend pas meilleur, cela rend même mauvais

✗ ...la preuve : les analyses de root cause racontent une tout autre histoire

Mais cela vide vos budgets et au moins les consultants se gavent.

CAS D'USAGE — CAMBRIOLAGE DU LOUVRE [1/3]

Un responsable de la sécurité physique en poste.

Deux audits d'intrusion physique réalisés.

...et pourtant

Le musée du Louvre a été cambriolé.

CAS D'USAGE — CAMBRIOLAGE DU LOUVRE [2/3]

CHECK sans ACT

- Le premier audit n'a jamais été suivi d'un DSA
- Le second a été passé à la trappe
- Absence de mécanisme de détection des manques du SMQ

Pas de révision du contexte (et notamment les Parties Intéressées)

- Pas de prise en compte de l'impact des changements (reconfiguration de la salle des bijoux) sur la matrice de risques
- Pas de révision des risques et du contexte (30j d'atelier à chaque fois ? Lol lol lol)

Absence de regard extérieur

- Matrice de risques à l'échelon DG excluant le cambriolage
- Pas d'audit externe sur ce risque
- Absence de veille sur les menaces

CAS D'USAGE — CAMBRIOLAGE DU LOUVRE [3/3] — Analyse en cascade

Incident Cambriolage du Louvre — faiblesse de la fenêtre sur la rue

N1 Audit d'intrusion physique sans ACT

N2 Risque de cambriolage absent de la matrice globale des risques

N3 Pas de révision du périmètre de l'appréciation des risques / lacunes dans la veille sur les menaces

N4 Pas de revue globale du SMQ

SE SORTIR DE LA TÊTE QUE...

✗ MYTHE

Il faudrait faire de l'EBIOS

✓ RÉALITÉ

Cette méthode n'est jamais mentionnée dans les documents ISO 27001.

✗ MYTHE

Il faudrait se baser sur la 27005

✓ RÉALITÉ

Cette norme n'est mentionnée que dans la liste des normes et en bibliographie.

✗ MYTHE

Il faudrait des scénarii de menaces / vulnérabilités

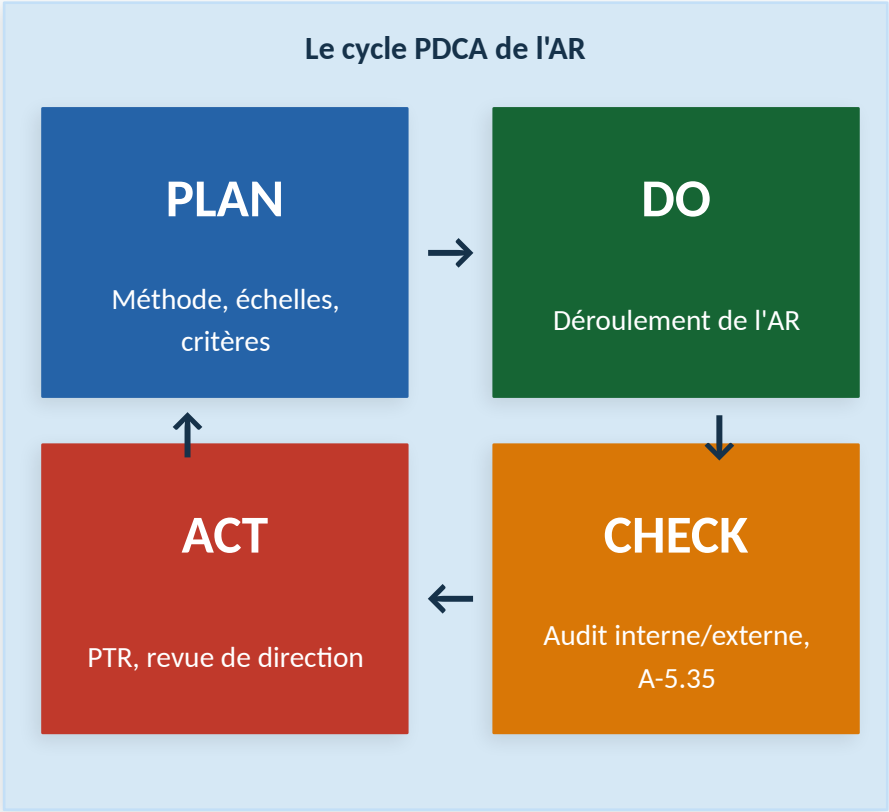
✓ RÉALITÉ

Jamais mentionné dans la norme.

6.1.2.c — "identifie les risques de sécurité de l'information" ... et c'est tout.

CE QU'EST VRAIMENT UNE AR

- C'est un processus avec son propre PLAN (méthode, échelles, documents…)
- Il est déroulé (DO) une première fois, puis régulièrement
- Il alimente le PTR 27001 avec les anomalies (forme et fond)
- Il est challengé (CHECK) par l'audit interne, l'audit externe et l'Annexe A-5.35
- Ses résultats (fond + forme) sont validés en revue de direction



EN BREF… CE N'EST PAS CELA

Une appréciation des risques instable,
sans connexion au reste du SMSI
CE N'EST PAS STATIQUE

C'EST PLUTÔT CELA

Un processus minimaliste, mais équilibré, intégré et challengé / révisé en permanence
C'EST DYNAMIQUE

MAIS PAR CONTRE...

Exigences sur la méthode

- La répétition de l'AR doit donner des résultats cohérents, valides et comparables (6.1.2.b)
- Des échelles (vraisemblance et impact) et des critères d'acceptation sont requis
- La méthode elle-même doit être minimaliste et révisée régulièrement

Connexions au reste du SMSI

- L'AR découle et alimente la DDA
- Établir un PTR découlant de l'AR (6.1.3.e)
- Lier ce PTR aux processus via les Objectifs de sécurité
- Les risques résiduels remontent en revue de direction et sont formellement acceptés par les propriétaires des risques

SANS OUBLIER…

◈ Périmètre des actifs

Les risques portent sur les actifs non informationnels ET AUSSI informationnels.

▲ Remontée des risques résiduels

Les risques résiduels remontent aux processus, puis en revue de direction.

ATTENTION CHAINE DE DECISION / COMMANDEMENT

✓ Contrôles en revue de direction

Méthode, échelles, résultats, choix des options de traitement, risques résiduels : tout est contrôlé en RD.

LES PIEGES

✗ ...pas de révision (PIEGE N°1 !!!)

✗ ...pas de formalisation / révision de la méthode elle-même

✗ ...pas de lien avec la DDA (attention plusieurs pièges)

✗ ...pas de risques résiduels acceptés par les Processus (PIEGE N° 2)

Une AR orpheline est une AR qui ne sert à rien

DONC EN RÉSUMÉ, L'AR...

L'appréciation des risques est, avant tout, un dispositif de management.

1 %

d'évaluation des risques de sécurité de l'information

99 %

de système de management

Le PLAN influe le DO, qui est contrôlé par le CHECK ; celui-ci remonte les anomalies à l'ACT, qui reboucle avec le PLAN.

LES RISQUES ET OPPORTUNITÉS (R&O) — § 6.1.1

À ne pas confondre avec l'Appréciation des Risques

- Les R&O du § 6.1.1 n'ont rien à voir avec l'AR des actifs (§ 6.1.2)
- On parle ici des R&O du SMSI lui-même, pas des assets
- C'est tout le § 6.1.1… et en général la liste nous brûle les doigts : qu'en fait-on ?

Toujours la même méthode — ET POURTANT souvent bâclée

- Lister les R&O, justifier leur provenance, les faire valider en revue de direction
- **ET SURTOUT : mettre des actions en face de chaque R&O, au niveau des processus**
- Pas d'action en face d'un risque → il n'existe pas ; pas d'action en face d'une opportunité → elle n'existe pas (liste sans actions = CHECK sans ACT = alerte).

SANS OUBLIER…

◈ La liste…(PLAN)

Comment l'établir, avec quel référentiel

▲ Les actions subséquentes

On en fait quoi ?

ATTENTION CHAINE DE DECISION / COMMANDEMENT

✓ Contrôles en revue de direction

Méthode, référentiel, résultats, actions : tout est contrôlé en RD.

LA ENCORE…

Ce qui compte n’est pas tant le fond que la dynamique

ON N'Y PENSE PAS FORCEMENT MAIS…

- ✗ R&O : les seuls risques don't le RSSI est propriétaire
- ✗ …et donc le SMSI est le seul asset sous responsabilité du RSSI
- ✗ …doit être traité comme les autres risques sur le cycle PDCA
- ✗ …et si le RSSI embarque d'autres assets / risque votre SMSI sent l'oignon

…et si votre DSI ne comprend pas ces 4 items faut qu'il se recycle dans la plomberie

PRÉVENTION DE LA FUITE DES DONNÉES — Annexe A 8.12

Contexte

- ! Nouvelle mesure de l'Annexe A version 2022 (avec 8.10 suppression, 8.11 masquage)
- ! Mesure générant le plus de NCMin dans les audits de certification depuis la v2022
- ! Biais mental fréquent : techno-solutionisme → on cherche d'abord l'outil, pas la méthode

La bonne méthode

1. Chaque propriétaire de processus identifie si ses actifs informationnels doivent implémenter la 8.12
2. Il y apporte une réponse, même minimaliste
3. Réponse vérifiée dans le processus de surveillance (§ 9.1)
4. Les trous dans la raquette → risque résiduels plus tracés dans un DSA
5. Les impossibilités de traitement → remontées en revue de direction

CONCLUSION

L'important dans un SMSI n'est pas le fond mais la forme...
Et cela marche : l'aviation civile pratique cela depuis 50 ans.

- → Ne pas surdimensionner le DO au détriment du PLAN / CHECK / ACT
- → Ne pas faire de la sur-qualité technique au détriment du fonctionnement du SMSI
- → Attention aux pièges de vocabulaire ("cohérents", "valides", "comparables")

Absence de CHECK/ACT → ALERTE

Actions absentes après CHECK/ACT → ALERTE
Absence de remontée au PLAN → ALERTE

Absence de chaîne de décision / commandement : ALERTE

CONCLUSION DE LA CONCLUSION

« Tire la chevillette, la bobinette cherra »

- On doit pouvoir faire un 360° : partir d'un item, établir le PLAN, prouver le DO, passer par le CHECK, faire valider les manques, revenir au PLAN.
- La traçabilité de bout en bout prouve la cohérence du SMSI — sur le fond ET sur la forme.
- Si, à un endroit, le SMSI n'implémente pas cette boucle : non-conformité.

Boucle rompue (manque structurel)
→ NC MAJEURE

Manque ponctuel non validé
→ NC mineure

CONCLUSION DE LA CONCLUSION DE LA CONCLUSION

« Le fond s’efface devant la forme, la forme entraîne le fond »

- Le SMSI c’est la forme, la cyber c’est le fond
- Veiller au respect du de la forme entraîne une amélioration mécanique du fond
- Méthode éprouvée depuis Deming

POUR ALLER PLUS LOIN…

01

Validation des risques résiduels

Vérifier : par qui sont-ils validés, et quand ? La traçabilité est une exigence, pas une option.

02

Trous dans la raquette — DDA

Vérifier que les mesures partiellement mises en œuvre figurent dans l'AR et ont été validées.

03

Cinématique complète des R&O

Vérifier l'ensemble du processus R&O : liste → justification → actions → validation RD.

C'EST KDO — Schéma de cohérence du SMSI

	PLAN	DO	CHECK	ACT
Niveau Processus	Procédures (PROC)	Instructions (DIO)	Audits processus	Plans d'action
Actifs / Risques	PSSI	Mesures de sécurité (MS)	Contrôles (CTRL)	DSA
DDA	Déclaration d'applicabilité	Mise en œuvre des mesures	Vérification des mesures	Traitement des écarts

NOTES ET LIENS

Implémentation d'un SMSI par étapes

https://apssis.com/articles/500/guide-cyber-resilience-opus-8-liso-27001-par-etape

Épisode Code Source — Braquage au Louvre

https://shows.acast.com/code-source/episodes/braquage-au-louvre-les-faits-et-le-point-sur-lenquete