LA TRILOGIE NORMATIVE · GRC

ISO 27001 27005 · 27002

Trois normes. **Un seul système de management.**
Pourquoi les traiter en silos vous fait échouer là où l'audit regarde vraiment.

ISO 27001
STRUCTURE

ISO 27005
RISQUE

ISO 27002
EXÉCUTION

Ignace YAO — Expert Cybersécurité · Auditeur SI

Glissez →

01 LE CONSTAT

Certifier l'ISO 27001 seule, c'est bâtir une façade.

27005 ✕ Sans **appréciation du risque**, vos contrôles sont choisis au catalogue, pas selon l'exposition réelle. Impossibles à justifier.

27002 ✕ Sans **guide de mise en œuvre**, vos contrôles sont mal implémentés. Auditables sur la forme, vides sur le fond.

= 0 Résultat : un SMSI conforme **sur le papier**, fragile face aux menaces réelles.

> **L'auditeur ne teste pas des cases cochées. Il teste une chaîne de cohérence.**

02 LE PRINCIPE

ISO 27001 structure le SMSI.
ISO 27005 oriente la gestion des risques.
ISO 27002 fournit les mesures de sécurité.

Une **vision** qui gouverne. Une **priorisation** qui décide. Une **exécution** qui applique. Assemblées, elles forment un système — pas trois silos.

◆ Stratégique ◆ Tactique ◆ Opérationnel

ISO/IEC 27001:2022

LE CADRE STRATÉGIQUE

Elle structure et gouverne le SMSI.

- **Clauses 4→10** — contexte, leadership, planification, support, opération, évaluation, amélioration.
- **Annexe A** — 93 contrôles répartis en 4 thèmes : organisationnel, humain, physique, technologique.
- **Cycle PDCA** — amélioration continue du système de management.
- **SoA** — la Déclaration d'Applicabilité : pivot d'inclusion / exclusion des contrôles. La seule norme **certifiable** de la trilogie.

NIVEAU

Stratégique

RÉPOND À

« Comment gouverner la sécurité de l'information ? »

ISO/IEC 27005:2022

LE MOTEUR DU RISQUE

Elle décide où porter l'effort.

- **Alignée ISO 31000** — décline le cadre générique de management du risque aux actifs informationnels.
- **Cycle** — identification → analyse → évaluation → traitement du risque.
- **Deux angles** — approche par événement et par actif (event-based / asset-based).
- **Alimente le SoA** — justifie chaque contrôle retenu ou écarté. Sortie clé : registre des risques + plan de traitement.

NIVEAU

Tactique

RÉPOND À

« Que dois-je protéger, et dans quel ordre ? »

ISO/IEC 27002:2022

LA BOÎTE À OUTILS

Elle traduit les contrôles en pratiques.

- **93 contrôles détaillés** — chacun avec son objet (purpose) et son guide de mise en œuvre.
- **5 attributs** — type de mesure, propriétés SI (C/I/D), concepts cyber, capacités opérationnelles, domaines.
- **Référence de l'Annexe A** — code de bonnes pratiques qui outille directement les contrôles d'ISO 27001.
- Guide d'implémentation — **non certifiable**, mais indispensable à la qualité de la mise en œuvre.

NIVEAU

Opérationnel

RÉPOND À

« Comment implémenter le contrôle correctement ? »

03 LA MÉCANIQUE

Une chaîne, pas trois silos.

Le risque décide. La norme structure. La pratique exécute. L'audit vérifie la boucle.

04 EN UN COUP D'ŒIL

Trois rôles, une lecture.

	ISO 27001	ISO 27005	ISO 27002
Finalité	Gouverner le SMSI	Prioriser les risques	Implémenter les contrôles
Répond à	Comment piloter ?	Quoi protéger ?	Comment faire ?
Certifiable	OUI	Non	Non
Niveau	Stratégique	Tactique	Opérationnel
Livrable clé	SoA + politiques	Registre des risques	Standards de mise en œuvre

Une seule des trois se certifie — mais elle ne tient que si les deux autres l'alimentent.

05 ÉLARGIR LE CADRE

La trilogie ISO est la colonne vertébrale. Pas la seule pièce.

NIST CSF 2.0 6 FONCTIONS

Govern · Identify · Protect · Detect · Respond · Recover. Grille de lecture stratégique qui se superpose au SMSI et au registre de risques — utile pour dialoguer avec le COMEX.

CIS Controls v8 18 CONTRÔLES · IG1-3

La **granularité technique** et la mesure d'exécution. Les Implementation Groups priorisent selon la maturité et la taille de l'organisation.

Mapping type : ISO 27005 ≈ Identify · ISO 27001 ≈ Govern · ISO 27002 + CIS v8 ≈ Protect / Detect.

06 CE QUE VOUS Y GAGNEZ

Quatre gains, mesurables.

01

Résilience

Des contrôles justifiés par le risque, pas par le catalogue.

02

Optimisation

Investir là où l'exposition est réelle — pas partout, pas au hasard.

03

Auditabilité

Une traçabilité continue : risque → contrôle → preuve.

04

Confiance

Une certification crédible auprès des clients & régulateurs.

07 LÀ OÙ L'AUDIT REGARDE

Le SoA est le point de jonction des trois normes.

Chaque contrôle de l'Annexe A doit être justifié par un risque identifié, implémenté selon une pratique reconnue, et adossé à une **preuve**. C'est cette cohérence — pas la liste des contrôles — que l'auditeur met à l'épreuve.

> **Ne certifiez jamais un SMSI que vos risques ne justifient pas.**

À RETENIR

Votre chaîne risque → contrôle → preuve tient-elle en audit ?

Si vous ne pouvez pas la tracer sur un contrôle donné, l'auditeur ne le pourra pas non plus.

↻ Repartagez

Envoyez ce carrousel à votre équipe GRC.

☆ Enregistrez

Gardez-le pour vos revues de SMSI.

✎ Commentez

Où votre chaîne casse-t-elle le plus souvent ?

IY

Ignace YAO

Expert en Cybersécurité | Auditeur des SI · ISO 27001 Lead Auditor & Aspirant CISA