Audit Maturité DSI — Groupe Fictif SA

Cybersécurité — CIS Controls v8 · NIST CSF 2.0 · NIS2 · DORA

Score global : **3.6 / 5** Secteur : Distribution & Retail (benchmark : 2.3 / 5) Date : 18 juillet 2026

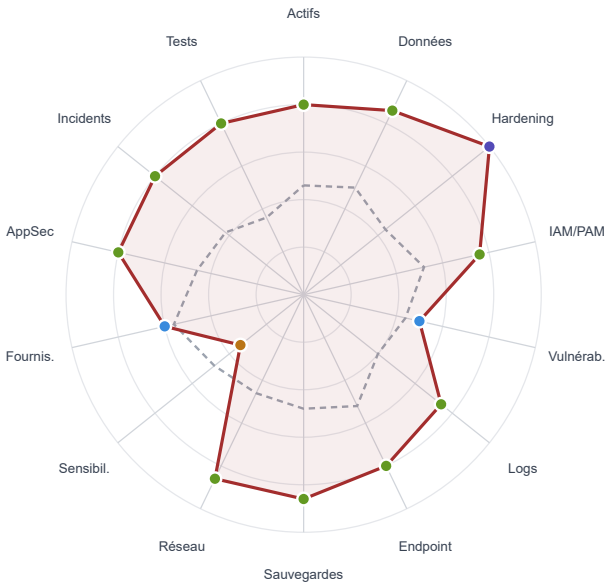
Score CIS v8	NIST CSF 2.0	Conformité NIS2	Conformité DORA	ISO 27001 — Annexe A
3.8	3.2	3.3	3.2	3.9
Géré	Défini	Défini	Défini	Géré
bm 2.3 **+1.5**	bm 2.7 **+0.5**	bm 2.5 **+0.8**	bm 2.4 **+0.8**	bm 2.5 **+1.4**

Roue CIS Controls v8

14 domaines — score de maturité par contrôle

3.8/5 Géré

Radar CIS v8 — 14 contrôles



Actifs	4 /2.3 +1.7	Données	4.3 /2.5 +1.8
Hardening	5 /2.2 +2.8	IAM/PAM	3.8 /2.6 +1.2
Vulnérab.	2.5 /2.2 +0.3	Logs	3.7 /2 +1.7
Endpoint	4 /2.6 +1.4	Sauvegardes	4.3 /2.4 +1.9
Réseau	4.3 /2.3 +2	Sensibil.	1.7 /2.4 -0.7
Fournis.	3 /2.8 +0.2	AppSec	4 /2.3 +1.7
Incidents	4 /2.1 +1.9	Tests	4 /1.8 +2.2

1 Absent · 2 Minimal · 3 Défini · 4 Géré · 5 Résilient · Benchmark

Lecture : **n** score · /n benchmark secteur · **±n** écart

Top 5 risques CIS prioritaires

Contrôles avec le score le plus faible — écart vs Distribution & Retail

±n écart vs benchmark · bm n = benchmark secteur · trait sur la barre = benchmark

1	**Sensibilisation** — Risque élevé · Projet urgent	1.7/5 bm2.4	-0.7
2	**Fournisseurs** — À surveiller · Quick win	3.0/5 bm2.8	+0.2
3	**Vulnérabilités** — À surveiller · Quick win	2.5/5 bm2.2	+0.3
4	**IAM/PAM** — Acceptable · Optimiser	3.8/5 bm2.6	+1.2
5	**Endpoint** — Acceptable · Optimiser	4.0/5 bm2.6	+1.4

ISO 27001 — Annexe A

11 chapitres A.5→A.18 · Benchmark : Distribution & Retail — ENISA 2024

3.9/5 Géré

Politiques	4.5 /2.5 +2		Organisation	3.6 /2.4 +1.2	
Sécu. RH	3 /2.5 +0.5		Actifs	3.5 /2.4 +1.1	
Contrôle accès	3.6 /2.7 +0.9		Crypto	3.5 /2.3 +1.2	
Sécu. physique	4.7 /2.7 +2		Exploitation	4 /2.5 +1.5	
Communications	4.3 /2.4 +1.9		Dév. sécurisé	4.3 /2.8 +1.5	
Fournisseurs	3.3 /2.6 +0.7		Incidents	4.3 /2.4 +1.9	
Continuité	4.5 /2.3 +2.2		Conformité	4 /2.6 +1.4	

1 Absent · 2 Minimal · 3 Défini · 4 Géré · 5 Résilient · Benchmark

Lecture : **n** score · /n benchmark secteur · **±n** écart

Top 5 prioritaires ISO 27001

Chapitres avec le score le plus faible vs benchmark sectoriel

±n écart vs benchmark · bm n = benchmark secteur · trait sur la barre = benchmark

1	**A.7 Sécurité RH**	À surveiller · Quick win	3.0/5 bm2.5	+0.5
2	**A.15 Fournisseurs**	Acceptable · Optimiser	3.3/5 bm2.6	+0.7
3	**A.8 Actifs**	Acceptable · Optimiser	3.5/5 bm2.4	+1.1
4	**A.10 Cryptographie**	Acceptable · Optimiser	3.5/5 bm2.3	+1.2
5	**A.6 Organisation**	Acceptable · Optimiser	3.6/5 bm2.4	+1.2

Cartographie CIS — maturité par tier

Vue d'ensemble des 14 contrôles répartis par niveau de maturité

T1 — Partial
score 1-2

Sensibil.	1.7

T2 — Risk Informed
score 2-3

Vulnérab.	2.5
Fournis.	3

T3 — Repeatable
score 3-4

Actifs	4
Données	4.3
IAM/PAM	3.8
Logs	3.7
Endpoint	4
Sauvegardes	4.3
Réseau	4.3
AppSec	4
Incidents	4
Tests	4

T4 — Adaptive
score 4-5

Hardening	5

NIST CSF 2.0 — Fonctions & Tiers

NIST CSF 2.0

Comparaison avec le benchmark sectoriel · Source ISACA 2024

3.2
Défini

Tier 2 — Risk Informed

Risques identifiés, non formalisés.

Partial | Risk Informed | Repeatable | Adaptive

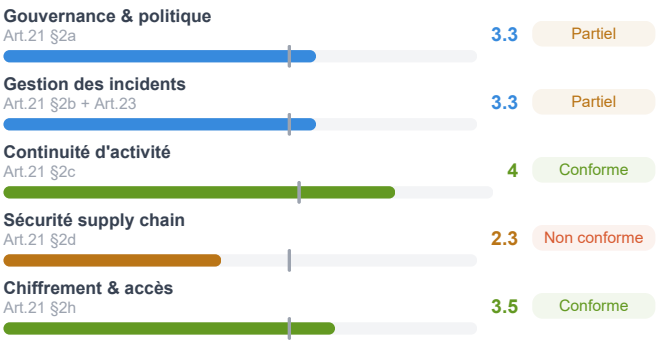
Govern	3	T2
Identify	3	T2
Protect	3.8	T3
Detect	3.3	T2
Respond/Recover	2.8	T2

Tier 1	Tier 2	Tier 3	Tier 4
Partial	**Risk Informed**	**Repeatable**	**Adaptive**
Ad hoc, réactif	Informé, non formalisé	Formalisé, reproductible	Optimisé, proactif

Conformité NIS2 Directive UE 2022/2555

Seuil de conformité minimal : 3/5 — ligne bleue

● Non conforme (<3) ● Partiel (=3) ● Conforme (≥4) ● Exemplaire (=5)



Conformité DORA Règlement (UE) 2022/2554

ISO 27001:2022 — SMSI & Contrôles

Certification

Maturité du SMSI et des contrôles Annexe A · Benchmark sectoriel — ENISA 2024

SMSI — Système de management

7 critères · Chapitres A.9–A.18

4 /5 — Géré

bm 2.5 · +1.5

A.9 Contrôle accès	3.6	+0.9
A.10 Crypto	3.5	+1.2
A.12 Exploitation	4	+1.5
A.13 Comm.	4.3	+1.9
A.16 Incidents	4.3	+1.9
A.17 Continuité	4.5	+2.2
A.18 Conformité	4	+1.4

— Trait gris = benchmark sectoriel

Contrôles complémentaires A.5-A.8

4 critères · Politiques, Org., RH, Actifs

3.6 /5 — Géré

bm 2.5 · +1.1

A.5 Politiques	4.5	+2
A.6 Organisation	3.6	+1.2
A.7 Sécu. RH	3	+0.5
A.8 Actifs	3.5	+1.1

Top 5 axes d'amélioration prioritaires

Domaines avec les scores les plus faibles — niveau actuel → cible recommandée

vs marché : n (±écart) · bm:n / trait sur la barre = benchmark secteur

1 **Sensibilisation**

Risque élevé · Projet urgent

Formation et sensibilisation des utilisateurs aux risques cyber.

vs marché : 2.4 **(-0.7)**

1.7 /5 — bm:2.4 → Cible : 4

2 **Vulnérabilités**

À surveiller · Quick win

Détection, priorisation et remédiation continue des vulnérabilités.

vs marché : 2.2 **(+0.3)**

2.5 /5 — bm:2.2 → Cible : 5

3 **NIST Respond/Recover**

À surveiller · Quick win

Réponse aux incidents et rétablissement des activités.

vs marché : 2.7 **(+0.1)**

2.8 /5 — bm:2.7 → Cible : 5

4 **Fournisseurs**

À surveiller · Quick win

Évaluation et suivi du risque de sécurité des prestataires et tiers.

vs marché : 2.8 **(+0.2)**

3.0 /5 — bm:2.8 → Cible : 5

5 **NIST Govern**

À surveiller · Quick win

Gouvernance : stratégie, rôles et pilotage du risque cyber.

vs marché : 2.6 **(+0.4)**

3.0 /5 — bm:2.6 → Cible : 5

Analyse — Cybersécurité

Evaluation globale

Score global : 3.6/5 — Niveau avancé

Positionnement : au-dessus du secteur Distribution & Retail (benchmark : 2.3/5)

Synthese de la dimension

La DSI intermédiaire de Groupe Fictif SA montre une bonne maîtrise des fondations techniques (inventaire actifs, MFA, segmentation réseau) mais révèle des faiblesses critiques dans la gouvernance des accès privilégiés, la gestion des vulnérabilités et la sensibilisation des équipes. Ces lacunes sont accentuées par la contrainte de délais liée à l'intégration d'acquisitions et au déploiement multi-pays de l'ERP, ainsi que par la pression des pics de trafic (Black Friday). Le score global de 3.6/5 dépasse largement le benchmark du secteur (2.3/5), mais les points faibles (scores 1-2) exposent l'entreprise aux risques majeurs de ransomware, de perte de données clients (RGPD, PCI-DSS) et de rupture de la chaîne d'approvisionnement IT.

Points forts identifies

- Gestion des actifs matériels et logiciels (inventaire exhaustif, autorisation) – scores 5/5.
- Contrôles d'accès forts (MFA généralisée, revues d'accès, gestion des mots de passe) – scores 5/5.
- Architecture réseau segmentée, NGFW, ZTNA et protections endpoint – scores 5/5.

Risques prioritaires lies au secteur

⚠️ Risques prioritaires liés au secteur Distribution & Retail :

- RGPD / données clients – score 3/5 (politique de chiffrement, classification) — impact : amendes potentielles jusqu'à 4 % du CA.
- PCI-DSS paiements – score 4/5 (chiffrement, DLP) — impact : fraude, perte de confiance client.
- Ransomware e-commerce – score 3/5 (sauvegardes immuables, gestion des supports amovibles) — impact : interruption des ventes en ligne, perte de CA immédiate.

Quick wins - Actions immediates

⚡ Actions immédiates (< 3 mois, effort limité, fort impact) :

- Interdiction des comptes partagés → Politique d'accès unique documentée → Réduction du risque d'escalade d'accès.
- Mise en place d'une campagne de sensibilisation ciblée (phishing + bonnes pratiques) → Kit de formation en ligne → Amélioration du taux de détection des tentatives de phishing.
- Renforcement de la gestion des supports amovibles (blocage USB, DLP) → Configuration GPO et tableau de bord de conformité → Diminution du vecteur d'infection par malware.

📋 Plan action structure

1 **Gestion des comptes partagés** — 1/5 → cible 5/5

- **Actions** · Élaborer et diffuser une politique d'interdiction des comptes partagés, mettre en place un contrôle technique (détection et blocage via IAM).
- **Livrable** · Document de politique « Comptes partagés » signé par la direction + règle de conformité IAM.

3 mois | Effort Faible

2 Sensibilisation et formation cybersécurité

1/5 → cible 4/5

- **Actions** · Déployer un programme de formation obligatoire (e-learning) pour tous les collaborateurs, incluant des simulations de phishing mensuelles.
- **Livrable** · Plateforme de formation active + tableau de bord de complétude (≥ 90 %).

3 mois | Effort Modéré

3 Gestion des supports amovibles

1/5 → cible 4/5

- **Actions** · Appliquer des restrictions GPO sur tous les postes, activer le chiffrement BitLocker, intégrer la surveillance des ports USB dans le SIEM.
- **Livrable** · Rapport de conformité des postes (audit mensuel).

3 mois | Effort Faible

4 Processus de remédiation des vulnérabilités

2/5 → cible 4/5

- **Actions** · Formaliser un flux de travail de remédiation basé sur le score CVSS, automatiser la priorisation via le système de gestion des vulnérabilités, définir des SLA de correction (48 h pour CVSS ≥ 7).
- **Livrable** · Playbook de remédiation + tableau de bord KPI de temps moyen de correction.

6 mois | Effort Modéré

5 Veille sur les CVE et menaces

1/5 → cible 4/5

- **Actions** · Souscrire à un service de threat intelligence (ex. MISP, commercial), intégrer les flux dans le SIEM et automatiser les alertes de nouvelles vulnérabilités critiques.
- **Livrable** · Dashboard de veille cyber avec indicateurs de couverture (≥ 90 %).

6 mois | Effort Modéré

Risques operationnels si inaction

🔴 Risques opérationnels si inaction :

- Propagation d'un ransomware via supports amovibles – Probabilité : élevée – Impact : perte de chiffre d'affaires en période de Black Friday, coûts de récupération estimés à plusieurs millions d'euros.
- Escalade d'accès via comptes partagés – Probabilité : moyenne – Impact : violation de données clients, sanctions RGPD et atteinte à la réputation.