Audit Maturité DSI — Groupe Fictif SA

Analyse des risques SI — ISO 27005 + ISO 31000 + COBIT EDM03

Score global : **2.5 / 5** Secteur : Distribution & Retail (benchmark : 3.4 / 5) Date : 18 juillet 2026

Risques critiques	Risques élevés	Risques modérés	Risques faibles
≥16	9-15	4-8	1-3
3	4	10	5
Bench: 1.5 +1.5	Bench: 3 +1	Bench: 6 +4	Bench: 7 -2
Action immédiate	Prioritaire	À planifier	Surveiller

Score maturité gestion des risques

2.5/5

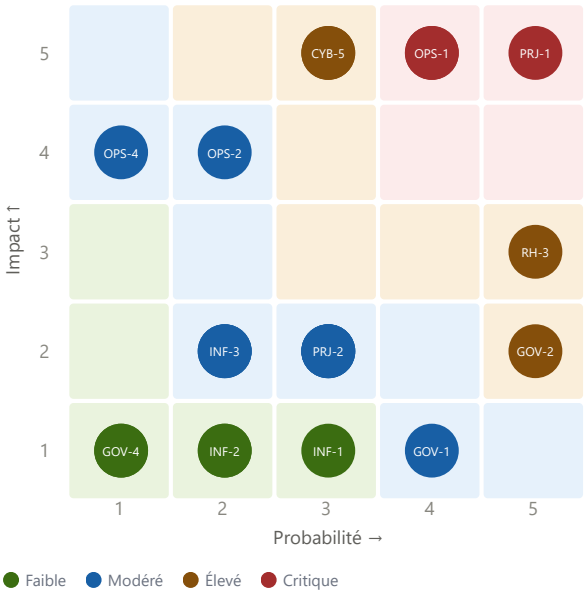
-0.9 vs benchmark Distribution & Retail (3.4)

Votre score vs secteur

0 5

Matrice P×I — Probabilité × Impact

Position de chaque risque selon sa probabilité et son impact



REGISTRE DES RISQUES

R-PRJ-1	Dérapage d'un projet IT critique	25
R-CYB-1	Cyberattaque majeure	20
R-OPS-1	Indisponibilité prolongée d'un système critique	20
R-CYB-2	Fuite ou exfiltration de données sensibles	15
R-CYB-5	Attaque sur la chaîne d'approvisionnement	15
R-RH-3	Bus factor — dépendance à un individu unique	15
R-GOV-2	Dérapage budgétaire IT non anticipé	10
R-OPS-2	Perte irrémédiable de données critiques	8
R-CYB-4	Non-conformité réglementaire IT	6
R-GOV-3	Désalignement IT/métiers chronique	6
R-RH-1	Départ de collaborateurs IT clés	6
R-PRJ-2	Non-réalisation des bénéfices attendus des projets IT	6
R-CYB-3	Compromission d'un compte privilégié	4
R-OPS-3	Défaillance d'un fournisseur IT critique	4
R-OPS-4	Incident datacenter majeur	4
R-GOV-1	Absence de gouvernance IT formalisée	4
R-INF-3	Vendor lock-in cloud	4
R-INF-1	Obsolescence critique de l'infrastructure IT	3
R-RH-2	Obsolescence des compétences IT	2
R-INF-2	Panne réseau étendue	2
R-OPS-5	Dette technique critique bloquant les évolutions	1
R-GOV-4	Décrochage technologique vs concurrents	1

Score = Probabilité × Impact (max 25)

Top 5 risques prioritaires

Classés par score P×I (max 25) — stratégie de traitement associée

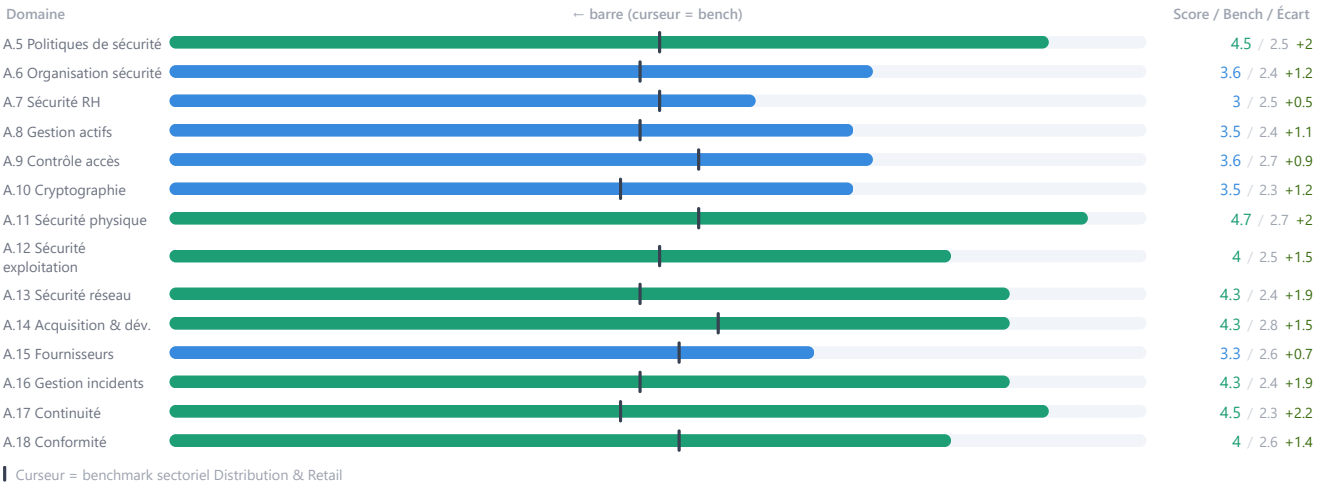
Score = P × I (max 25) | Stratégie : Réduire · Transférer · Accepter · Éviter

R-PRJ-1	Dérapage d'un projet IT critique Critique · P5×I5	25	Réduire 3 mois
R-CYB-1	Cyberattaque majeure Critique · P4×I5	20	Réduire 3 mois
R-OPS-1	Indisponibilité prolongée d'un système critique Critique · P4×I5	20	Éviter 3 mois
R-CYB-2	Fuite ou exfiltration de données sensibles Élevé · P3×I5	15	— 6 mois
R-CYB-5	Attaque sur la chaîne d'approvisionnement Élevé · P3×I5	15	Éviter 6 mois

Couverture sécurité — ISO 27001 Annexe A

Données issues de la dimension Cybersécurité

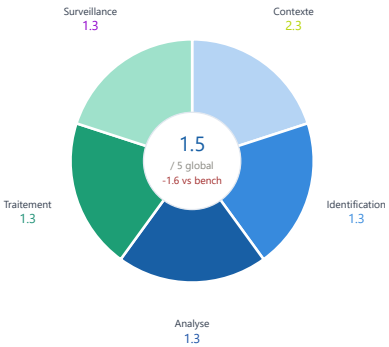
Score moyen par domaine · curseur = benchmark sectoriel



Curseur = benchmark sectoriel Distribution & Retail

Maturité processus risques — ISO 31000

5 axes · score vs benchmark Distribution & Retail

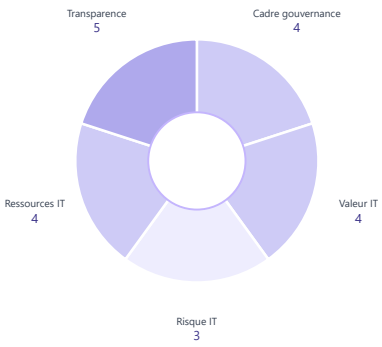


Axe processus	Score / Bench / Écart
Contexte	2.3 / 3 -0.7
Identification	1.3 / 3.2 -1.9
Analyse	1.3 / 3.1 -1.8
Traitement	1.3 / 3.4 -2.1
Surveillance	1.3 / 3 -1.7

Curseur = benchmark Distribution & Retail

Gouvernance des risques — COBIT EDM03

Optimisation du risque IT · score vs benchmark ISACA



Pratique	Score / Bench / Écart
EDM01 Cadre de gouvernance	4 / 3.9 +0.1
EDM02 Valeur investissements	4 / 3.7 +0.3
EDM03 Optimisation risque IT	3 / 3.6 -0.6
EDM04 Optimisation ressources	4 / 3.8 +0.2
EDM05 Transparence parties	5 / 3.5 +1.5

Curseur = benchmark ISACA / Gartner

Plan de traitement des risques

Actions prioritaires classées par criticité — actions détaillées dans l'analyse IA ci-dessous

Score = P × I (max 25) · Stratégie : Réduire · Transférer · Accepter · Éviter

Risque	Score	Stratégie	Action principale	Délai
R-PRJ-1 Dérapage d'un projet IT critique	25	Réduire	*Voir analyse IA ↓*	3 mois
R-CYB-1 Cyberattaque majeure	20	Réduire	*Voir analyse IA ↓*	3 mois
R-OPS-1 Indisponibilité prolongée d'un système critique	20	Éviter	*Voir analyse IA ↓*	3 mois
R-CYB-2 Fuite ou exfiltration de données sensibles	15	—	*Voir analyse IA ↓*	6 mois
R-CYB-5 Attaque sur la chaîne d'approvisionnement	15	Éviter	*Voir analyse IA ↓*	6 mois

Analyse IA — Risques SI

📋 Synthèse

La DSI intermédiaire de Groupe Fictif SA, confrontée à des délais serrés et à la conduite du changement liée à l'industrialisation d'un ERP multi-pays, montre une capacité à définir un appétit pour le risque (score 4) mais peine à le traduire en gouvernance opérationnelle. L'absence de cartographie des risques, de registre à jour et de comité dédié explique les scores très faibles (1-2) sur la plupart des processus de gestion des risques. Cette faiblesse expose l'entreprise aux risques sectoriels critiques (RGPD, PCI-DSS, ransomware e-commerce) et aux incidents de disponibilité pendant les pics de vente (Black Friday). Les forces observées (appétit clairement exprimé, reconnaissance de risques majeurs) sont donc largement neutralisées par des lacunes de formalisation et de suivi, ce qui rend la cible « dépasser le marché » difficile à atteindre sans actions structurées.

✅ Points forts identifiés

- . Appétit pour le risque IT clairement défini et validé (score 4/5) – facilite la priorisation stratégique.
- . Identification des risques majeurs (ransomware, indisponibilité critique, supply-chain) avec notation P×I pertinente (scores 5/5).
- . Reconnaissance de la nécessité d'un comité de pilotage des risques (même si non mis en place) – indicateur de prise de conscience de la gouvernance.

⚠️ Risques prioritaires liés au secteur

⚠️ Risques prioritaires liés au secteur Distribution & Retail :

- . RGPD / données clients : score 3/5 — impact potentiel d'amendes jusqu'à 4 % du CA et perte de confiance client.
- . PCI-DSS paiements : score 3/5 — risque de fraude et de vol de données de cartes, impact financier direct.
- . Ransomware e-commerce : score 5/5 — arrêt des ventes en ligne pendant les pics (Black Friday) = perte de CA immédiate.

⚡ Quick wins — Actions immédiates (< 3 mois)

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

- . Formaliser le registre des risques IT et le tenir à jour → Registre des risques IT version 1.0 → Visibilité immédiate des 10 % de risques les plus critiques.
- . Définir et publier une matrice P×I standardisée (échelles de probabilité et d'impact) → Matrice P×I documentée → Alignement des évaluations entre équipes.
- . Instaurer un reporting mensuel des risques critiques vers la direction générale → Tableau de bord KPI risques → Décisions éclairées et réactivité accrue.

📋 Plan d'action structuré

1 Registre des risques IT — 1/5 → cible 4/5

Actions : Concevoir un registre centralisé (outil Excel/SharePoint) incluant tous les actifs critiques, les scénarios, la probabilité, l'impact, le traitement et le propriétaire.

Livrable : Registre des risques IT – version 1.0, validé par le comité de pilotage.

3 mois | Effort Faible

2 Comité de pilotage des risques IT — 1/5 → cible 4/5

Actions : Nommer un sponsor C-level, définir la composition (DSI, RSSI, Métiers, Finance), établir un charter et planifier des réunions mensuelles.

Livrable : Charte du comité + planning annuel des réunions.

3 mois | Effort Modéré

3 Matrice de probabilité × impact — P×I)** (score actuel 1/5 → cible 4/5

Actions : Adapter le référentiel ISO 31000 pour créer une échelle à 5 niveaux, former les analystes risques, appliquer sur les 20 % de risques les plus critiques.

Livrable : Matrice P×I documentée et guide d'utilisation.

3 mois | Effort Faible

4 Plans de traitement des risques critiques — 2/5 → cible 4/5

Actions : Pour chaque risque classé « élevé » ou « critique », définir la stratégie (Éviter, Réduire, Transférer, Accepter), allouer un budget prévisionnel et désigner un responsable d'exécution.

Livrable : Catalogue de plans de traitement avec budget associé.

6 mois | Effort Modéré

5 Indicateurs de risques clés — KRI) et reporting** (score actuel 2/5 → cible 4/5

Actions : Sélectionner 5 KRI (ex. % de risques critiques traités, temps moyen de résolution, incidents de conformité RGPD, tentatives de ransomware, disponibilité des services critiques). Mettre en place un tableau de bord automatisé (Power BI ou équivalent).

Livrable : Dashboard KRI – mise à jour mensuelle.

6 mois | Effort Modéré

🔴 Risques opérationnels si inaction

🔴 Risques opérationnels si inaction :

- . Survenue d'un ransomware pendant le Black Friday – Probabilité élevée – Impact : perte de CA immédiate, atteinte réputationnelle, coûts de remise en service estimés à plusieurs millions d'euros.
- . Non-conformité RGPD ou PCI-DSS détectée lors d'un audit externe – Probabilité moyenne – Impact : amendes réglementaires, suspension de la plateforme de paiement, perte de confiance client.