

Best practices de la production dans le monde IBM i & les réglementations associées

Présentation avec le Common
France

01/10/2026

Version 2.7

RICOH
imagine. change.



RICOH | Cloud & Cyber

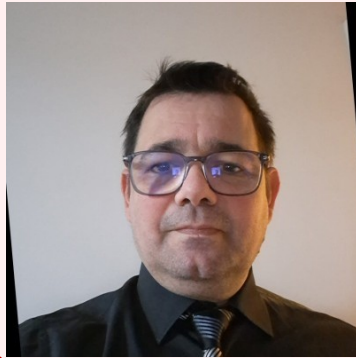
Speakers



Nadir HADI

Client Success
Manager

Corelia



Claude SALE

Lead Client Success
Manager

Corelia



Dominique MOUILLIER

Chief Information
Security Officer

Corelia



Patrice BESNARD

Directeur Commercial
Corelia & Division AMS/Data/IA

Corelia

Sommaire

A Contexte & Réglementations

- 05 Enquête Fortra 2025 — IBM i**
Préoccupations sécurité, tendances et chiffres clés du marché IBM i
- 06 Directive NIS2 & réglementations**
NIS2, DORA, REC, RGPD — cadre légal européen et français

B Sécurisation IBM i

- 08 Les 4 piliers de la sécurité IBM i**
System Values, Authorities, Exit Points, QAUDJRN
- 09 Règles d'or ANSSI pour IBM i**
Segmentation réseau, droits & profils, résilience, audit & détection (09-10)
- 11 Nouveautés sécurité IBM i 7.6**
MFA TOTP natif, chiffrement ASP1, CFGHOSTSVR, profils, NC, APIs crypto

C Stratégie de sauvegarde

- 13 Règle ANSSI de sauvegarde 3-2-1-1-0**
Norme ANSSI et application concrète dans l'environnement IBM i
- 14 Sauvegardes chiffrées IBM i**
Deux méthodes : BRMS logiciel vs GKLM / bibliothèque matériel

D Protection Anti-Ransomware

- 16 IBM SafeGuarded Copy — Architecture**
Architecture SGC, snapshots immuables, air gap physique
- 18 Protections Anti-Ransomware — Immuabilité**
Sauvegarde Sanctuaire (Air Gap physique), Retention Lock, FCM4/5 (17-18)
- 19 IBM Power Cyber Vault — Offre Full Stack**
Détection ransomware < 1 min, SafeGuarded Copy adossé à PowerSC
- 20 IBM Concert — IA & Automatisation des Correctifs**
Scoring IA des CVE (watsonx) et automatisation firmware/VIOS

E Exploitation & Conformité

- 22 Monitoring, Gouvernance & Synthèse**
Monitoring sauvegardes, alertes, feuille de route NIS2 (22-23)

Annexe 1

- 25 Glossaire des acronymes**
Signification de tous les acronymes — traduction française
- 26 ANSSI & les 20 objectifs de sécurité**
L'autorité nationale de cybersécurité et son référentiel d'exigences

Annexe 2

- 28 Architecture IBM i → VTL → DataDomain → Site DR**
Architecture globale de sauvegarde et réplication vers site DR
- 29 Flux de sauvegarde — IBM i au Site DR**
Étapes détaillées, déduplication et immuabilité
- 30 Stratégies de réplication DataDomain**
Topologies VTL 1:1 et 1:N via DD Replicator
- 31 SGC & FlashCore Module**
IBM SafeGuarded Copy, détection ransomware FCM4/5 (31-32)
- 33 Comparatif des méthodes de chiffrement**
BRMS logiciel vs GKLM matériel — tableau comparatif

Annexe 3

- 35 PCA & PRA / Gouvernance & Audit / Check-up NIS2**
Continuité, reprise d'activité, audit IBM i, conformité NIS2 — slides 35–37

Contexte & Réglementations

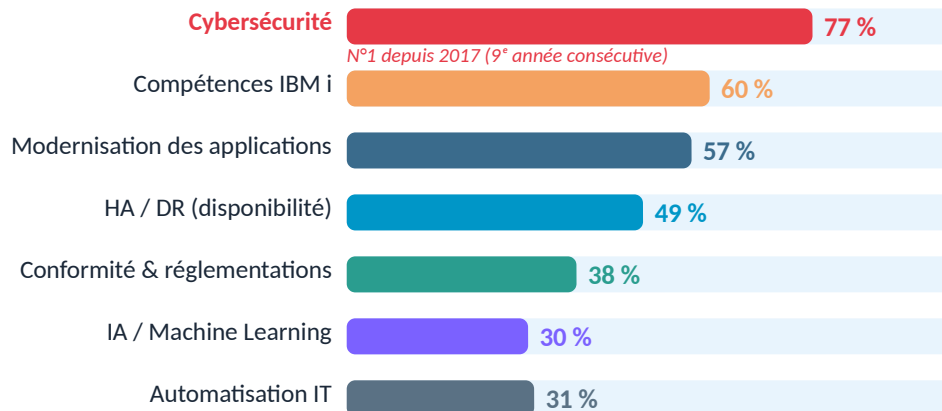
Enquête Fortra, directive NIS2, ANSSI et
cadre légal européen



05 — Enquête Fortra — IBM i Marketplace Survey 2025

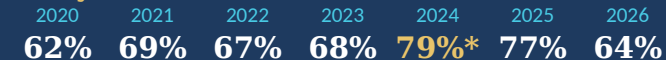
★ Top préoccupations des professionnels IBM i

(% de répondants — sélection de 5 sujets parmi 14)



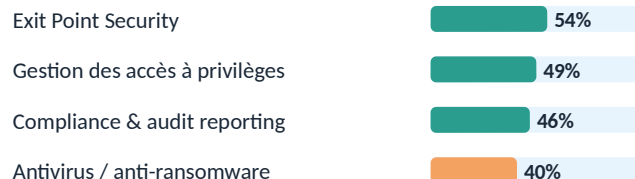
N°1 depuis 2017 (9^e année consécutive)

Évolution de la préoccupation cybersécurité



* Record historique - 2026 : recul lié à l'adoption de IBM i 7.6 MFA et cloud managé
 "La cybersécurité va probablement rester au sommet. Même si tout le monde se sent prêt aujourd'hui, les menaces de demain inquiètent toujours."
 — Steve Will, CTO IBM i

🔑 Solutions de sécurité déployées



⚠️ Seulement 40 % protégés contre les ransomwares !

📊 Chiffres clés à retenir

🔒 88%

des IBM i à QSECURITY 40 ou 50 (État de la sécurité 2025)

🌙 72%

des IBM i tournent sans surveillance hors heures ouvrées

📈 70%

prévoient un upgrade HW ou SW en 2026 (record historique)

🤖 30%→42%

progression de l'IA/ML comme préoccupation (2025→2026)

Les 3 défis sécurité majeurs : menaces en constante évolution (1er), manque de compétences sécurité (2^e), équilibre sécurité vs efficacité métier (3^e)

06 — Directive NIS2 & cadre réglementaire européen

NIS2 — Directive UE 2022/2555

-  Succède à NIS1 : 7→18 secteurs, dirigeants responsables. Transposition française en cours (loi Résilience, 2025).
-  15 000 à 18 000 entités françaises concernées (Entités Essentielles et Importantes), 18 secteurs stratégiques.
-  Sanctions : jusqu'à 10 M€ ou 2 % du CA (EE), 7 M€ ou 1,4 % (EI). Responsabilité personnelle des dirigeants.
-  Notification d'incident à l'ANSSI : 24h (alerte), 72h (rapport détaillé), 1 mois (rapport final).
-  Sécurisation de la chaîne d'approvisionnement : fournisseurs et prestataires IT inclus.

Réglementations complémentaires

DORA

Digital Operational Resilience Act — Résilience opérationnelle numérique
Règlement UE 2022/2554. Secteur financier : gestion des risques TIC, tests de pénétration, supervision des prestataires.

REC

Resilience of Critical Entities — Résilience des entités critiques
Directive UE 2022/2557. Renforce le dispositif SAIV français (Activités d'Importance Vitale), 11 secteurs.

RGPD

Règlement Général sur la Protection des Données
Règlement UE 2016/679. Sécurité des données personnelles (art. 32), notification des violations sous 72h.

🎯 Impact direct sur les environnements IBM i

Les systèmes IBM i hébergeant des applications critiques (ERP, production, banque) entrent dans le périmètre NIS2 et/ou DORA.

Obligations communes : sauvegardes testées, PCA/PRA documenté, journalisation, MFA, notification rapide des incidents, gestion des risques fournisseurs.

📄 Article 21 NIS2 — Mesures de gestion des risques et réponses IBM i

Exigence NIS2 Art. 21

Authentification renforcée (MFA)
Chiffrement des données au repos
Sécurisation des communications
Gestion des incidents & notification

Réponse IBM i 7.6

MFA TOTP natif (coût zéro)
Chiffrement ASP1 natif + BRMS/GKLM
CFGHOSTSVR force TLS
Audit journal + SIEM + notification ANSSI

Bénéfice conformité

Preuve intégrée MFA (audit journal)
Chiffrement démontrable sans SAN
Confidentialité des flux réseau
Traçabilité et détection facilitées

Sécurisation IBM i

Règles d'or ANSSI, nouveautés IBM i 7.6



08 — Les 4 principaux piliers de la sécurité IBM i



Valeurs Système (System Values)

Les valeurs système (QSECURITY, QAUDCTL, QPWDVL, QMAXSIGN...) définissent la politique de sécurité globale de la partition — la base sur laquelle tout repose.



Autorités (Authorities)

Les autorités définissent ce que chaque profil a le droit de faire, objet par objet : autorités spéciales (*ALLOBJ, *SECADM), moindre privilège, adopted authority.



Points de Sorties (Exit Points)

Les points de sortie contrôlent les portes d'entrée réseau — ODBC, JDBC, FTP, DDM. Sans eux, ces accès contournent totalement la sécurité applicative.



Journal d'audit (QAUDJRN)

Le journal d'audit trace ce qui s'est passé : connexions, accès aux objets, changements de profils. La mémoire du système, indispensable en cas d'incident.



Le fil conducteur de la section

Ces 4 notions structurent les règles d'or ANSSI qui suivent — segmentation, droits d'accès, résilience et audit — et répondent directement aux exigences de traçabilité de NIS2.

09 — Règles d'or ANSSI appliquées à IBM i (1/2)

 1. Segmentation & Cloisonnement

L'IBM i est souvent trop ouvert sur le réseau interne, exposant des services dangereux.

 Désactiver les services inutiles

Coupez les serveurs FTP, Telnet non sécurisé, et surtout le NetServer (partage IFS) s'ils ne sont pas strictement nécessaires. Chaque service ouvert est une surface d'attaque.

 Exit Points (Points de sortie)

Point critique ! Utilisez des programmes d'Exit Point pour contrôler les accès via ODBC, JDBC, FTP, DDM. L'ANSSI recommande de filtrer ces accès comme un pare-feu applicatif. Outils : IBM Guardium, Assure Security, PowerTech, iSecurity.

 Micro-segmentation réseau

Ne laissez jamais l'IBM i dans le même VLAN que les postes de travail utilisateurs. VLAN dédié avec ACL restrictives, accès uniquement depuis les segments autorisés.

 2. Gestion des Droits et des Profils **Suppression du *ALLOBJ**

L'ANSSI est formelle sur la limitation des privilèges. Trop d'utilisateurs ont encore l'autorité spéciale *ALLOBJ. Utilisez l'Adopted Authority ou des outils PAM (Privileged Access Management) pour les élévations temporaires.

 Profils système par défaut

Désactivez ou changez les mots de passe des profils livrés par défaut : QSECOFR, QPGMR, QSYSOPR, QUSER... Inventaire des profils *ALLOBJ < 5, documenté et audité trimestriellement.

 MFA — Authentification Multi-Facteur

Pour les accès administrateur (SST/DST) et les sessions 5250, le MFA est une exigence NIS2 forte relayée par l'ANSSI. Solutions : Assure MFA, WALLIX, CyberArk (IBM i compatible).

 Politique de mots de passe

QPWDLVL ≥ 3 (mots de passe longs). Rotation périodique, complexité imposée. Désactiver les profils inactifs > 90 jours automatiquement.

10 — Règles d'or ANSSI appliquées à IBM i (2/2)

3. Résilience & Continuité

La résilience sous NIS2 implique de pouvoir repartir après un ransomware.

Sauvegardes immuables (Air-Gap)

L'ANSSI préconise des sauvegardes déconnectées. Pour l'IBM i : bandes physiques sorties du lecteur, ou VTL (Virtual Tape Library) avec réplication. Combinaison SGC + bandes sanctuaire.

Full System Save (SAVSYS)

Réalisez des sauvegardes complètes régulières (*SAVSYS + *SAVSECDTA + *SAVCFG), pas seulement les données applicatives. Indispensable pour réduire le RTO (temps de reconstruction complète du système).

Haute Disponibilité (HA) et journalisation

Si vous utilisez la réplication logicielle (journaling), assurez-vous que les journaux ne répliquent pas une corruption ou un chiffrement malveillant vers la cible. Délai de réplication ajustable. Solutions : PowerHA SystemMirror (natif IBM), iCluster, MIMIX, Quick-EDD.

Tests de restauration documentés

NIS2 exige la preuve de restauration. Tests mensuels sur LPAR dédiée, RTO mesuré vs objectif. Documentation du Recovery Report BRMS à jour après chaque modification système.

4. Audit & Détection (Journalisation)

L'IBM i génère énormément de logs, mais ils sont rarement exploités.

Audit Journal (QAUDJRN)

Activez systématiquement l'audit système. L'ANSSI demande une traçabilité complète des actions d'administration. QAUDCTL = *AUDLVL *OBJAUD *NOQTEMP, toutes les valeurs QAUDLVL actives.

Intégration SIEM

Exportez vos logs QAUDJRN et QSYSOPR vers un concentrateur de logs (SIEM) externe : QRadar, Predatar, Sentinel. En cas d'intrusion, les logs sur la machine elle-même pourraient être altérés par l'attaquant.

Surveillance temps réel

Alertes sur : échecs de connexion répétés, modifications de profils *SECADM, changements de valeurs système critiques (QSECURITY, QAUDCTL), accès Exit Points inhabituels.

Rétention et conformité

Conservation des journaux ≥ 5 ans (recommandation ANSSI). Archivage sur support immuable. Les journaux doivent être exploitables pour les audits NIS2 et les investigations forensiques.

11 — Nouveautés sécurité IBM i 7.6 : la release la plus orientée sécurité de l'histoire de la plateforme

✓ MFA natif intégré à l'OS — Authentification multi-facteur TOTP

-  **Natif à l'OS**
Coût zéro, sans logiciel tiers
-  **Basé sur TOTP**
Authy, MS Authenticator, Okta, Duo
-  **Sans réseau requis**
Secret partagé terminal ↔ serveur
-  **Toutes interfaces**
5250, FTP, ODBC/JDBC, ACS, Navigator
-  **SST/DST indépendants**
Clé TOTP séparée par profil de service
-  **Prérequis**
QSECURITY ≥ 40 et QPWLVL = 4
-  **Commandes clés**
CHGUSRPRF AUTHMTH(*TOTP),
CHGTOTPKY
-  **Intégration tierce**
Exit point QIBM_QSY_AUTH (CyberArk,
WALLIX)

⚙️ Autres améliorations sécurité majeures

-  **Chiffrement ASP1**
Disque système natif sans arrêt
(Option 45 SS1)
-  **CFGHOSTSVR**
Force TLS sur chaque serveur hôte
-  **Profils_NC**
QSECOFR_NC etc., protégés contre
modification
-  **APIs crypto renforcées**
PBKDF-2, AES par défaut (fin
DES/3DES)
-  **Suivi PTF sécurité**
Date visible sur DSPPTFGRP, auditable
-  **DCM & TLS Debugger**
TLS 1.3, export PKCS12 sans clé privée

📊 Niveaux de sécurité IBM i (QSECURITY) — Rappel et évolution

Niveau	Protection	Description	Statut IBM i 7.5 / 7.6	Recommandation
10	Aucune	Pas de mot de passe. Profils créés automatiquement avec *ALLOBJ.	Retiré (obsolète)	✗ Interdit
20	Mot de passe seul	Authentification par mot de passe, mais tous les profils reçoivent *ALLOBJ.	Retiré depuis 7.5	✗ Interdit
30	Ressources	Contrôle d'accès aux objets (autorités). Pas de protection d'intégrité OS.	Disponible (non recommandé)	⚠ Insuffisant
40	Intégrité OS	Protection d'intégrité du système + contrôle des accès. Défaut d'usine.	Défaut usine 7.5 / 7.6	✓ Minimum requis
50	Intégrité renforcée	Niveau 40 + protection C2/CAPP, objets domaine restreints, validation params.	Disponible — recommandé	★ ANSSI / NIS2

⚠ IBM i 7.6 : par défaut = niveau 40 • MFA TOTP natif requiert QSECURITY ≥ 40 + QPWLVL = 4 • Recommandation ANSSI/NIS2 : niveau 50 • Niveaux 10 et 20 retirés • Power10 minimum (FW1060+)

Stratégie de sauvegarde

Règle 3-2-1-1-0, chiffrement



13 — Règle ANSSI de sauvegarde 3-2-1-1-0**3****copies**

des données
(1 production + 2
sauvegardes)

2**supports**

différents
(bande + disque ou cloud)

1**copie**

hors site
(site distant, coffre, cloud)

1**copie**

immuable ou
hors ligne (air-gapped)

0**erreur**

de restauration
(tests réguliers validés)

Application concrète dans l'environnement IBM i

Copie 1 — Production : Données live sur disques SSD/FlashSystem du serveur Power (miroir RAID ou SVC)

Copie 2 — Sauvegarde locale : BRMS sur bandothèque IBM (TS4500/TS4300) ou FlashSystem secondaire — chiffrée AES-256

Copie 3 — Hors site : Bandes externalisées en coffre sécurisé (rotation hebdomadaire) ou réplication inter-sites via SVC Stretched Cluster

Copie immuable : Safeguarded Copy sur FlashSystem (snapshots immuables) ou bandes WORM en coffre — protection anti-ransomware

0 erreur : Tests de restauration planifiés mensuellement, documentés et audités — restauration sur LPAR de test dédiée

14 — Sauvegardes chiffrées IBM i

Méthode 1 — Chiffrement logiciel BRMS

Principe

BRMS utilise les services cryptographiques d'IBM i pour chiffrer les données avant écriture sur bande. Le chiffrement est purement logiciel, indépendant du matériel.

Prérequis

- BRMS Advanced Feature (5770-BR2 (remplace BR1, retiré de commercialisation))
- Encrypted Backup Enablement (5770-SS1 Option 44)
- Master Key + Keystore (Q1AKEYFILE dans QUSRBRM)

Fonctionnement

Limitations

- Impact CPU significatif sur le serveur Power
- Fenêtre de sauvegarde potentiellement doublée
- Données non compressibles → volume $\times 2$ à $\times 3$
- Ciblé pour de faibles volumes de données

Méthode 2 — Chiffrement matériel GKLM

Principe

Le chiffrement est réalisé dans le lecteur de bande lui-même (hardware encryption), après la compression. IBM GKLM (Guardium Key Lifecycle Manager) gère les clés de chiffrement.

Architecture

- 2 VM serveurs de clés sous Red Hat Enterprise Linux
- Configuration active/active (haute disponibilité)
- Communication IP avec la bandothèque (KMIP)
- Library Managed Encryption (LME) activé

Lecteurs compatibles

Avantages majeurs

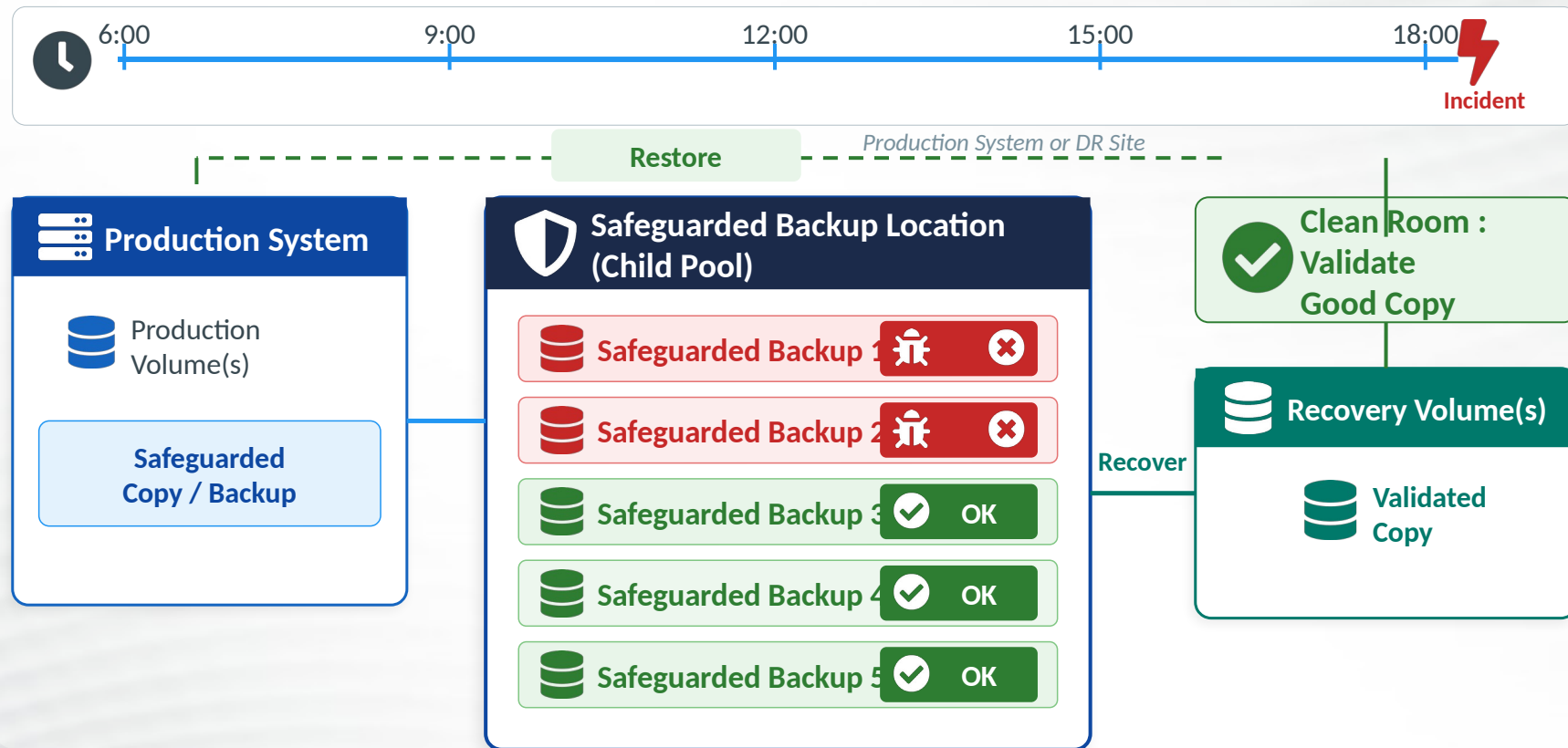
- Zéro impact CPU sur le serveur Power
- Fenêtre de sauvegarde préservée (non doublée)
- Chiffrement AES-256 à vitesse native du lecteur
- Compression AVANT chiffrement → volume optimal

Protection Anti-Ransomware

SafeGuarded Copy, FlashCore Module,
immuabilité



16 — IBM Safeguarded Copy – Architecture Overview



17 — Sauvegarde Sanctuaire (Air Gap physique)

 Le concept de sauvegarde sanctuaire

La sauvegarde sanctuaire est la **couche ultime de protection** des données : une copie physiquement déconnectée de tout réseau, stockée sur bandes magnétiques dans un coffre-fort sécurisé.

Principe fondamental : l'air gap physique

Contrairement à l'air gap logique (SGC/FlashSystem), l'air gap physique garantit une **isolation totale et absolue** du support de sauvegarde. Une bande éjectée de la bandothèque et stockée en coffre est **inatteignable par tout vecteur d'attaque numérique** : ransomware, malware, attaque interne, compromission d'identifiants administrateurs.

Pourquoi la bande reste irremplaçable

- ✓ **Air gap natif** : Bande éjectée = déconnexion physique totale du réseau. Aucun accès distant possible.
- ✓ **Immuabilité WORM** : Cartouches WORM (Write Once Read Many) : données non modifiables ni supprimables. Conformité réglementaire.
- ✓ **Coût au TB imbattable** : 10 à 15× moins cher que le disque/flash pour le stockage longue durée. Zéro consommation électrique au repos.
- ✓ **Durée de conservation** : 30 ans+ de rétention certifiée. Idéal pour archivage légal et conformité NIS2 / RGPD.
- ✓ **Chiffrement matériel** : AES-256 natif via GKLM/LME. Données chiffrées même si la bande est volée ou perdue.

Architecture sauvegarde sanctuaire IBM i**Best practices sauvegarde sanctuaire IBM i**

Rotation : Hebdomadaire minimum — bandes mensuelles conservées 13 mois, annuelles 7 ans (conformité NIS2/RGPD)

Inventaire : BRMS Media Inventory à jour — réconciliation mensuelle avec le prestataire de coffre-fort

WORM : Utiliser des cartouches WORM LTO pour les sauvegardes critiques — garantie d'immuabilité physique

Tests : Restauration trimestrielle depuis les bandes sanctuaire sur LPAR isolée — documenter le RTO mesuré

18 — Protections Anti-Ransomware — Immuabilité des Sauvegardes

**Retention Lock
(WORM)***DataDomain Compliance Mode*

- Verrous horodatés sur chaque sauvegarde
- Suppression impossible même admin local
- Conformité réglementaire automatique
- Durée : 30j court terme / 90j+ long terme
- Audit trail complet (syslog / SIEM)

**SafeGuarded Copy
(IBM i)***Copies isolées hors production*

- Snapshots immuables périodiques
- Isolés du réseau de production
- Restauration rapide post-incident
- Compatible avec FlashCopy / DS8000
- Testé régulièrement (restore test)

**Air-Gap Logique
(DataDomain)***Isolation réseau des copies DR*

- Fenêtre de réplication limitée
- Hors fenêtre : réseau DR coupé
- Copie hors portée ransomware
- Compatible avec cyber-vault physique
- RPO maîtrisé selon politique

Règle 3-2-1-1-0 : 3 copies | 2 supports différents | 1 hors site | 1 immuable | 0 erreur de restore vérifiée

NIS2
Art. 21 — Sauvegardes testées

DORA
Art. 12 — Résilience numérique

ANSSI
LPM / RGS — Immuabilité
requis

RGPD
Art. 32 — Intégrité des données

ISO 27001
A.12.3 — Backup Management

19 — IBM Power Cyber Vault — Offre Full Stack adossée à PowerSC

 Identification

Ateliers et évaluations de la résilience cyber de l'environnement Power (IBM i, AIX). Cartographie des risques et recommandations prioritisées avant mise en œuvre.

**Protection**

Création et sécurisation de snapshots immuables (Safeguarded Copy) selon un calendrier propre au client. Orchestration garantissant la cohérence applicative (crash-consistency).

 Détection

Surveillance temps réel des menaces et vecteurs d'attaque. S'appuie sur PowerSC (conformité temps réel, Zero Trust Execution), IBM FlashSystem et l'intégration SIEM.

**Réponse & Reprise**

Activation des protocoles de réponse, contrôles d'intégrité et restauration d'une copie saine, dans les objectifs RPO/RTO définis avec le client.

Écosystème mobilisé par l'offre

Power11 : racine de confiance matérielle

SIEM : corrélation des alertes

FlashSystem : Safeguarded Copy immuable

Expert Labs : cadrage et mise en œuvre

PowerSC : temps réel + Zero Trust

Détection : < 1 minute (garanti Power11)

 Ce que couvre l'offre Full Stack **Infrastructure & Stockage**

Serveurs IBM Power11 (E1080, E1180, S1122...) | IBM FlashSystem 5600/7600/9600 + Safeguarded Copy | SAN Fibre Channel dédié | Capacité isolée pour les copies immuables

 PowerSC, IA & Services

PowerSC (Compliance Automation, EDR, Zero Trust Execution, MFA) | Intégration au SIEM existant | IBM Expert Labs (cadrage + déploiement) | Objectifs RPO/RTO contractualisés avec Corelia

20 — IBM Concert — IA & Automatisation des Correctifs CVE

🔗 Qu'est-ce qu'IBM Concert ?

Plateforme propulsée par **watsonx (IA générative)** qui agrège les données de multiples sources — scanners de vulnérabilités, inventaires applicatifs, base CVE — pour cartographier automatiquement la topologie applicative.

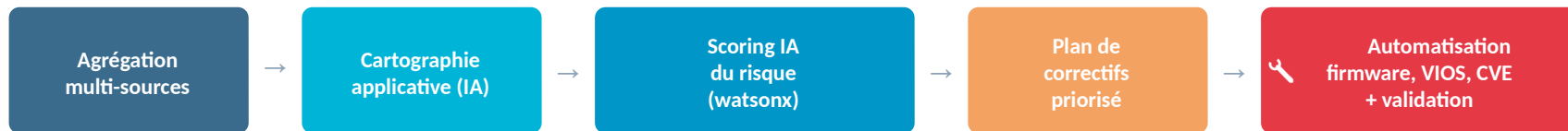
Au-delà du simple score CVSS

Concert calcule un **Risk Score unifié**, en croisant criticité métier, dépendances et fenêtres de maintenance, avec une **priorité aux vulnérabilités réellement exploitables (EPSS)** plutôt qu'un simple classement par sévérité technique.

Pourquoi aller au-delà du CVSS ?

- ✓ **Score de risque contextuel** : dépendances, criticité métier, topologie système, fenêtres de maintenance.
- ✓ **Exploitabilité réelle (EPSS)** : priorise les CVE vraiment exploitables, pas seulement les plus sévères.
- ✓ **Plans de correctifs optimisés** : équilibre entre vitesse de correction, risque et disponibilité de service.
- ✓ **Automatisation Power11** : firmware, VIOS et adaptateurs I/O orchestrés sans interruption (LPM).
- ✓ **Impact mesuré** : jusqu'à 90 % de réduction du délai de correction des CVE critiques.

Cycle de gestion intelligente des correctifs (IBM Concert)



Impact mesuré (données IBM Concert)

Réduction du bruit : jusqu'à 67 % d'alertes basse priorité en moins qu'une approche CVSS classique

Volumétrie CVE : +520 % de vulnérabilités référencées depuis 2016

Délai de correction : jusqu'à 90 % plus rapide sur les CVE critiques (auto-patching)

Correctifs en attente : 47 % des vulnérabilités encore non corrigées après 12 mois

Exploitation & Conformité

Monitoring, PCA/PRA, gouvernance, audit
et synthèse



22 — Monitoring, Alertes & Gouvernance des Sauvegardes

Indicateurs à surveiller

Taux de succès sauvegardes

Cible : $\geq 99\%$ 

Durée sauvegarde vs. fenêtre

Cible : $< 80\%$ 

Retard réplication (RPO)

Cible : $< 4h$ 

Taux déduplication DataDomain

Cible : $> 10:1$ 

Espace consommé / alerte

Cible : $< 80\%$ cap.

Restore test mensuel

Cible : 100% réussi



Stack de monitoring recommandé

BRMS Reports

Rapports natifs IBM i — logs job QBRM

DataDomain Mgr

Console Dell PowerProtect DD — supervise l'appliance cible BRMS (connectée à IBM i via FC, émule une librairie TS3500)

DD REST API

API DD OS — expose métriques DD (dédup, réplication, alertes) vers SIEM/Grafana ; indirecte à IBM i

SNMP/Syslog

Forwarding vers SOC/SIEM centralisé

Vérification Restore

Test restore mensuel documenté (NIS2/DORA)

23 — Synthèse & Feuille de route

T4 2026

Évaluation

Audit sécurité IBM i
Cartographie NIS2
Inventaire des sauvegardes
BIA (analyse d'impact)

T1 2027

Mise en œuvre

Déploiement GKLM
Chiffrement des sauvegardes
Renforcement des profils
Journalisation complète

T2-T3 2027

Consolidation

Tests PCA/PRA
Tests de restauration
Formation équipes
Documentation complète

2028+

Conformité continue

Audits réguliers
Amélioration continue
Déclaration des incidents de
sécurité à l'ANSSI
Exercices de crise

Points clés à retenir

- NIS2 est une obligation légale pour les EE et EI, pas une option — les systèmes IBM i critiques sont directement concernés
- La règle 3-2-1-1-0 est le socle de toute stratégie de sauvegarde robuste et conforme
- Le chiffrement matériel (GKLM + bandothèque) est la solution recommandée en production — zéro impact CPU, fenêtre préservée
- Les tests de restauration réguliers sont obligatoires : une sauvegarde non testée n'est pas une sauvegarde
- La gouvernance IBM i (profils, journalisation, audit) doit être intégrée dans la stratégie cyber globale de l'entreprise
- Le PCA/PRA doit être documenté, testé et maintenu — c'est une exigence NIS2 Article 21

Annexe 1



25 — Glossaire des acronymes

RÉGLEMENTATIONS

- NIS2** Network and Information Security 2 — Dir. UE 2022/2555
DORA Digital Operational Resilience Act — Règl. UE 2022/2554
REC Resilience of Critical Entities — Dir. UE 2022/2557
RGPD Règlement Général sur la Protection des Données (UE 2016/679)

ORGANISMES & RÔLES

- ANSSI** Agence Nationale de la Sécurité des Systèmes d'Information
SGDSN Secrétariat Général de la Défense et de la Sécurité Nationale
CERT-FR Centre Gouvernemental de Veille et de Réponse aux Attaques
OIV Opérateur d'Importance Vitale
EE / EI Entité Essentielle / Entité Importante (classification NIS2)

SÉCURITÉ & CONFORMITÉ

- PSSI** Politique de Sécurité des Systèmes d'Information
SIIV Système d'Information d'Importance Vitale
SAIV Secteur d'Activités d'Importance Vitale
MFA Multi-Factor Authentication — Authentification multi-facteurs
SIEM Security Information and Event Management
PAM Privileged Access Management — Accès privilégiés
CVE Common Vulnerabilities and Exposures — Référentiel vulnérabilités
PASSI Prestataire d'Audit SSI (qualifié ANSSI)
PDIS Prestataire de Détection des Incidents de Sécurité
PRIS Prestataire de Réponse aux Incidents de Sécurité
TOTP Time-based One-Time Password — MFA natif IBM i 7.6

CONTINUITÉ & SAUVEGARDE

- PCA** Plan de Continuité d'Activité (BCP)
PRA Plan de Reprise d'Activité (DRP)
BIA Business Impact Analysis — Analyse d'Impact Métier
RPO Recovery Point Objective — Perte de données max. admissible
RTO Recovery Time Objective — Durée max. d'interruption admissible
SLA Service Level Agreement — Accord de Niveau de Service
HA High Availability — Haute Disponibilité (clustering)
DR Disaster Recovery — Reprise après sinistre

IBM i & STOCKAGE

- GKLM** Guardium Key Lifecycle Manager — Gestion clés chiffrement
BRMS Backup, Recovery and Media Services
LME License Management Engine — Gestion des licences IBM
SGC Safeguarded Copy — snapshots immuables anti-ransomware (FlashSystem)
FCM FlashCore Module — module flash IBM, détection ransomware intégrée
VTL Virtual Tape Library — Bibliothèque de bandes virtuelles
WORM Write Once Read Many — Stockage immuable anti-falsification
LTO Linear Tape-Open — Standard bande magnétique haute densité
IFS Integrated File System — Système de fichiers natif IBM i
LPAR Logical PARTition — Partition logique isolée IBM i
PTF Program Temporary Fix — Correctif/patch sécurité IBM i
IPL Initial Program Load — Démarrage système IBM i

26 — L'ANSSI et les 20 objectifs de sécurité

Repères historiques de l'ANSSI

- **2001** Création de la DCSSI
- **2009** Création de l'ANSSI (ex-DCSSI)
- **2011** Devient autorité nationale SI
- **2015** Stratégie nationale numérique
- **2016** 1ère directive cyber européenne
- **2018** Transposition NIS 1 en France
- **2022** NIS2, DORA et REC adoptées
- **2023** Vincent Strubel nommé DG ANSSI
- **2025** Loi Résilience votée au Sénat
- **2026** Application attendue d'ici 2028

20 objectifs stratégiques ANSSI pour NIS2

Référentiel qui encadrera la transposition NIS2 en France

- | | |
|---|--|
| 01 Gouvernance & risques cyber | 11 Continuité d'activité (PCA/PRA) |
| 02 Politique de sécurité (PSSI) | 12 Chaîne d'approvisionnement |
| 03 Sécurité des ressources humaines | 13 Communications & échanges |
| 04 Gestion des actifs & inventaire | 14 Acquisition & maintenance des SI |
| 05 Architecture & cloisonnement réseau | 15 Sécurité physique |
| 06 Contrôle d'accès & MFA | 16 Sauvegardes & restauration |
| 07 Chiffrement des données sensibles | 17 Journalisation & traçabilité |
| 08 Sécurité opérationnelle & surveillance | 18 Sensibilisation & formation |
| 09 Gestion des vulnérabilités & correctifs | 19 Audits & contrôles réguliers |
| 10 Gestion des incidents & notification | 20 Conformité & amélioration continue |

Missions de l'ANSSI : autorité nationale de cybersécurité (rattachée au SGDSN) ; accompagne les OIV et entités NIS2 ; opère le CERT-FR ; définit les règles, audite et qualifie les prestataires (PASSI/PDIS/PRIS). Portail : MonEspaceNIS2 (monespaceenis2.cyber.gouv.fr).

Annexe 2



28 — Architecture Globale — IBM i → VTL → Dell DataDomain → Site DR

SITE PRINCIPAL

IBM i
LPAR PROD 1

IBM i
LPAR PROD 2

IBM i
LPAR DEV

↓ BRMS / GO SAVE

VTL — Virtual Tape Library

IBM i classe les VTL comme périphériques TAPMLB • Cartouches virtuelles
*SAVE / *TAR

↓ VTL

Dell DataDomain — Site Principal

Déduplication inline • Compression • Chiffrement AES-256 • DIA ("Data
Invulnerability Architecture")

SITE DR / RÉPLICATION

IBM i LPAR DR
(Stand-by / Failover)

Restore
DR

Dell DataDomain — Site DR

Réplique synchrone/asynchrone • RPO configurable
Copies immuables (Air-gap logique)

Réplication
IP
over WAN

29 — Flux de Sauvegarde — De l'IBM i au Site DR

1

Déclenchement

BRMS planifie la sauvegarde (nuit, maintenance, planifiée)
GO SAVE 21/22 ou commande BRMS

2

Écriture VTL

IBM i écrit sur la VTL (TAPMLB virtuel via FC/iSCSI)
Débit natif Power Systems

3

VTL

VTL transmet à DataDomain via protocole VTL
Déduplication + compression inline

4

Retention Lock

Politique WORM appliquée
Copies immuables (SafeGuarded)
Protection anti-ransomware

5

Réplication WAN

DataDomain réplique vers le site DR
Seules les données déduplicuées passent sur le WAN (bande passante ↓)

6

Validation DR

Rapport de réplication vérifié
Test restore sur site DR planifié
Alertes en cas d'écart RPO/RTO

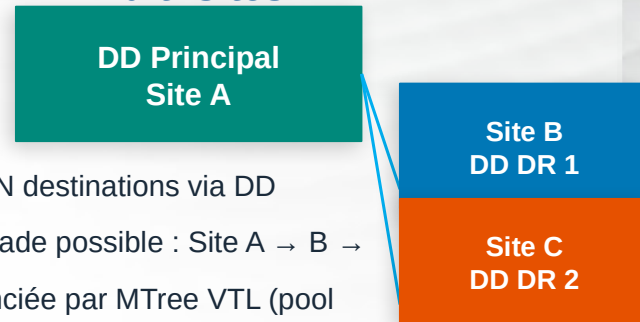
30 — Stratégies de Réplication DataDomain

Topologie 1:1 — Standard



- IBM i sauvegarde via BRMS vers VTL DataDomain (FC)
- Réplication DD → DD via DataDomain Replicator (WAN)
- Chiffrement WAN : TLS 1.3 + AES-256 (natif DD)
- Déduplication côté appliance DD (inline) — ~10% vol. source
- Idéal : 1 site principal IBM i / 1 site DR

Topologie 1:N — Multi-sites



- 1 DD source → N destinations via DD Replicator
- Réplication cascade possible : Site A → B → C
- Politique différenciée par MTree VTL (pool de bandes)
- Cas d'usage : multi-géographique, infogérance IBM i
- NIS2/DORA : données récupérables depuis

Paramètres de réplication recommandés

Paramètre	Valeur recommandée	Remarque
Fréquence réplication	Selon schedule BRMS (ex. toutes les 4h)	DD Replicator recopie après chaque job BRMS
Chiffrement WAN	TLS 1.3 + AES-256	Natif DD Replicator — activer SSL Replication
Bande passante WAN	~10-20% du volume brut (dédup côté DD)	Throttle 70% WAN — dédup inline DD
Rétention DR	90 jours (DORA) / 5 ans (ANSSI critique)	Retention Lock WORM
Monitoring	DataDomain REST API + SNMP traps	Alertes sur retard > RPO

31 — IBM SafeGuarded Copy (SGC)

Qu'est-ce que SafeGuarded Copy ?

IBM SafeGuarded Copy (SGC) crée des snapshots point-in-time **immuables** et **logiquement isolés** de l'environnement de production sur les baies IBM FlashSystem.

Caractéristiques clés :

- Copies indestructibles : ne peuvent être modifiées, supprimées ni chiffrées, même par un administrateur compromis
- Isolation logique (air-gap virtuel) : stockées dans un child-pool protégé, inaccessibles aux hôtes
- Séparation des rôles : seul le Security Admin gère les politiques SGC (principe du double contrôle)
- Restauration instantanée : reverse FlashCopy en moins de 60 secondes (garantie IBM)
- Jusqu'à 256 SGC par volume source — jusqu'à 15 000 snapshots par système

Politique de snapshots automatisée

Exemple : politique SGC pour IBM i

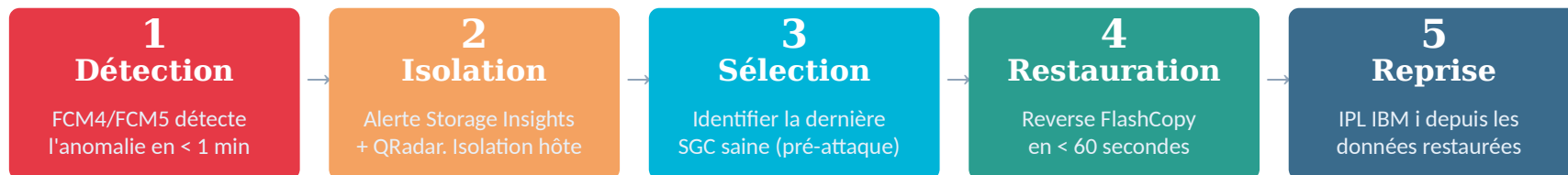
Fréquence : Toutes les 4 heures
Rétention : 72 heures (3 jours)
Démarrage : 00:00 chaque jour
Safeguarded : OUI (immuable)

→ 18 snapshots indestructibles sur 3 jours

→ RPO maximum de 4 heures

Jusqu'à 32 politiques SGC par système.
 Orchestration possible via IBM Copy Services Manager.
 Intégration QRadar pour déclenchement SGC sur alerte de sécurité.

⚡ Processus de restauration après attaque ransomware



32 — FlashCore Module & détection ransomware**FCM4 — FlashCore Module Gen 4 (2024)**

- FPGA + processeur ARM sur chaque module flash
- Analyse de chaque I/O en temps réel (2 secondes)
- Mesure de l'entropie, compressibilité et patterns d'écriture
- Modèles ML entraînés : ransomware vs activité normale
- Détection en < 1 minute (firmware FCM 4.1 + Virtualize 8.6.3+)
- Capacités : 4.8 à 38.4 TB — PCIe Gen 4 — QLC NAND
- Zéro impact perf. : traitement dans le module flash

FCM5 — FlashCore Module Gen 5 (fév. 2026)

- Format NVMe EDSFF — nouvelle génération de form factor
- Capacités : 6.6 à 105.6 TB (record industrie)
- QLC NAND, IP propriétaire IBM (perf. TLC, coût QLC)
- Modèle ransomware v3.3 — faux positifs < 1 %
- Chiffrement quantum-safe intégré au hardware
- Déduplication accélérée matériellement
- Disponibilité : 6 mars 2026 (FS 5600/7600/9600)

Baies FlashSystem compatibles SGC + FCM**FlashSystem 5600**

2.5 PBe 2.6M IOPS

1U | FCM5

SGC ✓ Ransomware Detection ✓

FlashSystem 7600

7.2 PBe 4.3M IOPS

2U | FCM5

SGC ✓ Ransomware Detection ✓

FlashSystem 9600

11.8 PBe 6.3M IOPS

2U | FCM5

SGC ✓ Ransomware Detection ✓

🔒 SGC + FCM = défense en profondeur

Le FCM4/FCM5 détecte l'attaque en < 1 minute et déclenche automatiquement une SafeGuarded Copy via QRadar. Les SGC programmées (ex. 4h, rétention 72h) garantissent un point de restauration sain, restaurable par reverse FlashCopy en < 60 sec — reprise en minutes, pas en heures.

33 — Comparatif des deux méthodes de chiffrement

Critère	BRMS avec Chiffrement Software (CPU)	GKLM avec Chiffrement Hardware (Bandothèque)
Impact CPU serveur	Élevé — CPU IBM i sollicité	Aucun — chiffrement dans le drive
Fenêtre de sauvegarde	Potentiellement doublée	Préservée — vitesse native
Volume de bandes	×2 à ×3 (pas de compression)	Optimal (compression + chiffrement)
Algorithme	AES-128 ou AES-256	AES-256
Matériel requis	Tout lecteur de bande	Lecteur LTO-4+ ou TS11xx en bandothèque
Gestion des clés	Keystore IBM i (QUSRBRM)	GKLM (2 VM RHEL ou Windows) — KMIP
Coût additionnel	Options BRMS Advanced + SS1 Opt.44	Licence GKLM + 2 VM Linux ou Windows

 Recommandation

Pour les environnements de production IBM i avec des exigences NIS2 :

Privilégier le chiffrement matériel via GKLM + bandothèque IBM avec Library Managed Encryption. Cette solution garantit des sauvegardes chiffrées AES-256 sans impact sur les processeurs Power, préserve la fenêtre de sauvegarde, et permet une gestion centralisée des clés conforme aux exigences d'audit. Les 2 VM GKLM sous RHEL assurent la haute disponibilité du service de clés.

Annexe 3



35 — PCA & PRA sur IBM i

RPORecovery Point
ObjectivePerte de données
acceptable**RTO**Recovery Time
ObjectiveTemps de reprise
acceptable**Solutions IBM i par niveau de RTO**

- < 1 min → PowerHA + Stretched Cluster SVC
- < 15 min → PowerHA + réplication synchrone
- < 4h → Restauration FlashSystem snapshots
- < 24h → Restauration BRMS bandes locales
- > 24h → Restauration BRMS bandes externalisées

Exigences PCA/PRA dans le cadre NIS2**1 Analyse d'impact métier (BIA)**

Identifier les processus critiques, les dépendances IBM i, les RTOs/RPOs acceptables par application. Cartographier les flux de données.

2 Plan de Continuité (PCA)

Procédures de basculement documentées. Accords de service avec les fournisseurs. Tests annuels de basculement. Rôles et responsabilités clairs.

3 Plan de Reprise (PRA)

Procédures de restauration complètes. Recovery Report BRMS à jour. Séquence de restauration documentée (IPL, OS, données, applications, tests).

4 Tests & exercices

1 test PRA complet/an (NIS2 Art.21) : bascule site DR, validation apps IBM i, restauration SGC/bandes, failback. Tests PowerHA semestriels. BRMS mensuels. RTO/RPO documentés.

5 Amélioration continue

Revue post-incident. Mise à jour des procédures après chaque changement système. Audit annuel du PCA/PRA. Indicateurs RTO/RPO mesurés.

36 — Gouvernance & Audit IBM i



Journalisation complète

Activer la journalisation sur tous les objets critiques (fichiers DB, zones de données). Journal QAUDJRN pour l'audit système. Rétention des journaux conforme aux exigences légales (5 ans min. recommandé).



Gestion des profils & accès

Principe du moindre privilège. Suppression des profils *ALLOBJ inutiles. Revue trimestrielle des autorités. Politique de mots de passe renforcée (QPWDLVL 3+). Authentification multi-facteur (MFA) via Assure MFA ou équivalent.



Surveillance & détection

Monitoring temps réel des événements de sécurité. Alertes sur les tentatives d'accès échouées, les changements de profils *SECADM, les modifications de valeurs système critiques. Intégration SIEM (Splunk, QRadar).



Audit & conformité continue

Audit annuel de la configuration de sécurité IBM i. Vérification des valeurs système (QSECURITY ≥ 40). Contrôle des exit points réseau. Rapport d'audit pour NIS2 et commissaires aux comptes. Outil recommandé : IBM Guardium, iSecurity, Powertech.

Indicateurs clés de conformité IBM i

QSECURITY : ≥ 40 (50 recommandé)	QPWDLVL : 3 ou 4 (mots de passe longs)	QAUDCTL : *AUDLVL *OBJAUD *NOQTEMP
QAUDLVL : Toutes valeurs d'audit actives	Exit points : Tous surveillés (FTP, ODBC, DDM...)	Profils *ALLOBJ : < 5 (inventaire documenté)



Prérequis SGC (Safeguarded Copy) — IBM FlashSystem



Matériel (Hardware)

Baie IBM FlashSystem 5600, 7600 ou 9600 | Microcode IBM Spectrum Virtualize ≥8.5.0 | Licence SGC Advanced (Spectrum Virtualize) | SAN Fibre Channel 16Gb/32Gb | Capacité dédiée SGC (≥30% de l'espace protégé selon rétention)



Logiciel (Software)

IBM Spectrum Virtualize ≥8.5.0 (SGC natif) | IBM Copy Services Manager (CSM) ≥6.3 (orchestration) | IBM i 7.3 TR minimum (7.5 TR6+ recommandé) | Environnement isolé (air-gap) pour restauration et validation | Politique de rétention définie (fréquence + durée)

37 — Check-up IBM i pour NIS2

Mesure ANSSI	Application IBM i	Commande / Valeur clé
 Intégrité du système	Détection des objets modifiés ou de programmes altérés (backdoors) par comparaison à une baseline de référence.	DSP0BJD, CHK0BJITG SAVCHGOBJ pour suivi delta
 Chiffrement des données sensibles	Chiffrement colonne des fichiers DB2 via Field Procedures — conformité RGPD/NIS2 pour les données personnelles et critiques.	Field Proc (FIELDPROC) AES-256 au niveau colonne RCACET pour politiques ligne/col.
 Hygiène des mots de passe	QPWDLVL 2 ou 3 pour activer les mots de passe longs (128 car.) : complexité, rotation et non-réutilisation imposées.	QPWDLVL 2 ou 3 QPWDMINLEN ≥ 12 QPWDEXPITVL ≤ 90 jours
 Maintenance & correctifs sécurité	CUM Packages et Group PTFs sécurité réguliers, veille PSIRT IBM sur les CVE, fenêtre de patching planifiée.	GO PTF → Option 8 Group PTFs : SF99V7R5 PSIRT : ibm.com/trust/security-psirt
 Journalisation & audit système	Audit journal complet : traçabilité des actions d'administration, connexions et modifications de profils/autorités.	QAUDCTL *AUDLVL *OBJAUD QAUDLVL toutes valeurs QAUDJRN actif
 Contrôle des accès réseau (Exit Points)	Exit Points sur chaque entrée réseau (ODBC, JDBC, FTP, REXEC, DDM) pour filtrer et journaliser les accès refusés.	WRKREGINF Exit Pts : QIBM_QTMF_*, QIBM_QZDA_*, QIBM_QTG_*
 Sauvegardes immuables	Règle 3-2-1-1-0 avec copie immuable (SGC + bandes WORM), sauvegardes AES-256 et tests de restauration mesurés.	BRMS + GKLM/LME SGC (FlashSystem) Bandes WORM en coffre
 Niveau de sécurité système	QSECURITY niveau 40 minimum (50 recommandé), protection des objets et validation des programmes activées.	QSECURITY 40 (ou 50) QALWOBJRST *NONE QFRCCVNRST 3



**Adoptons ensemble
des gestes responsables :**

**N'imprimons les documents
que si nécessaire.**



**Économisons
le papier**

Internal



**Préservons
les ressources**



**Protégeons
l'environnement**

RICOH | Cloud & Cyber



RICOH
imagine. change.

CORELIA
A RICOH Company

Merci de votre attention.
L'équipe Corelia reste à votre
disposition.