FICHE DE RÉVISION

Module : Analyse et Évaluation des Risques

Formation : Pilotage et Animation de la Cybersécurité

🎯 1. Introduction à la Gestion des Risques Cyber

> **Objectif :** Comprendre les enjeux de la gestion des risques dans une organisation

▸ Définitions fondamentales

Concept	Définition (ISO 27005 / ISO 31000)
Risque	Combinaison de la vraisemblance d'un événement redouté et de la gravité de ses conséquences sur les objectifs de l'organisation
Menace	Cause potentielle d'un incident pouvant nuire à un système ou à une organisation (acteur malveillant, erreur humaine, catastrophe naturelle)
Vulnérabilité	Faiblesse d'un actif ou d'un contrôle pouvant être exploitée par une menace
Actif	Tout élément ayant de la valeur pour l'organisation : données, systèmes, processus, personnes, locaux
Impact	Conséquence d'un incident sur l'organisation : financière, opérationnelle, juridique, réputationnelle
Vraisemblance	Probabilité qu'une menace exploite une vulnérabilité et déclenche un incident
Risque résiduel	Risque subsistant après la mise en oeuvre des mesures de traitement
Appétit au risque	Niveau de risque qu'une organisation est prête à accepter pour atteindre ses objectifs (décision de gouvernance)

▸ La formule du risque

RISQUE = MENACE × VULNÉRABILITÉ × IMPACT

modulé par les mesures de sécurité existantes

Risque brut : avant toute mesure de sécurité
Risque net : après application des contrôles
Risque résiduel : après traitement, soumis à acceptation

▸ Enjeux de la gestion des risques pour l'organisation

Enjeu	Explication et bénéfice
Conformité réglementaire	RGPD Art. 32, NIS2 Art. 21, DORA, ISO 27001 : la gestion des risques est une exigence légale et normative
Priorisation des investissements	Allouer les ressources limitées (budget, RH) en priorité sur les risques les plus critiques
Protection de la valeur	Préserver la continuité d'activité, la réputation, les données et les actifs stratégiques de l'entreprise
Aide à la décision	Fournir à la direction une vision claire du niveau d'exposition pour arbitrer en connaissance de cause
Amélioration continue	Mesurer l'évolution du niveau de risque dans le temps et piloter l'efficacité des mesures mises en oeuvre

Communication interne	Sensibiliser les métiers aux risques qui les concernent directement et les impliquer dans le traitement

▸ Le cycle de gestion des risques (ISO 31000 / ISO 27005)

Phase	Étape	Actions principales
1	Établissement du contexte	Définir le périmètre, les critères d'évaluation, l'appétit au risque, les parties prenantes
2	Identification des risques	Recenser les actifs, les menaces, les vulnérabilités et les impacts potentiels
3	Estimation des risques	Évaluer la vraisemblance et l'impact de chaque risque identifié → calcul du niveau de risque
4	Évaluation des risques	Comparer les risques aux critères d'acceptation, prioriser le traitement
5	Traitement des risques	Choisir et mettre en oeuvre les options : Réduire / Accepter / Transférer / Éviter
6	Acceptation des risques résiduels	Validation formelle par la direction des risques non traités ou partiellement traités
7	Communication et surveillance	Reporting, réévaluation périodique, gestion des évènements déclencheurs

2. Cadres Normatifs et Méthodologies — ISO 27005 & EBIOS RM

> **Objectif :** Appliquer les principaux cadres normatifs et méthodologies de gestion des risques

▸ Comparatif des principales méthodologies

Méthode	Origine	Approche	Points forts	Limites
ISO 27005:2022	ISO / International	Processus générique, compatible ISO 27001	Universelle, flexible, reconnue mondialement	Ne prescrit pas de méthode précise
EBIOS Risk Manager	ANSSI / France	Scénarios d'attaque, approche par les parties prenantes	Opérationnelle, orientée métier, compatible NIS2	Complexe à mettre en oeuvre sans accompagnement
ISO 31000:2018	ISO / International	Cadre généraliste de management des risques (tous domaines)	Applicable à tout type de risque d'entreprise (ERM)	Trop générique pour la sécurité SI seule
MEHARI	CLUSIF / France	Évaluation quantitative des vulnérabilités et services de sécurité	Base de données de menaces riche, historique	Peu mise à jour, moins utilisée actuellement
FAIR	USA / OpenFAIR	Quantification financière du risque cyber	Permet de parler au langage de la direction financière	Complexe à calibrer, données d'entrée difficiles

		(pertes estimées en €)		

ISO 27005:2022 — Processus détaillé

Processus ISO 27005	Description et contenu clé
Établissement du contexte	Définir la portée, les limites, les contraintes légales, les critères de risque (vraisemblance et impact) et l'appétit au risque
Identification des risques	Recenser actifs (primaires et supports), identifier les menaces et vulnérabilités applicables, analyser les conséquences
Estimation des risques	Évaluer vraisemblance (probabilité) et impact (gravité) selon une échelle définie ; calculer le niveau de risque brut et net
Évaluation des risques	Comparer les niveaux de risque aux critères d'acceptation ; établir la liste priorisée des risques à traiter
Traitement des risques	Sélectionner les options (réduire, accepter, transférer, éviter), définir le plan de traitement, identifier les mesures de l'Annexe A ISO 27001
Acceptation du risque résiduel	Validation formelle et documentée de la direction pour chaque risque résiduel
Communication et revue	Partage des résultats avec les parties prenantes, réévaluation périodique, gestion des changements de contexte

EBIOS Risk Manager — Les 5 ateliers

EBIOS Risk Manager (ANSSI, 2018) est structurée en 5 ateliers séquentiels qui progressent du contexte général jusqu'aux scénarios d'attaque opérationnels.

Atelier	Nom	Objectif et livrables
1	Cadrage et socle de sécurité	Définir le périmètre, les missions critiques, les biens supports, identifier l'écart au socle de sécurité (ISO 27002, CIS)
2	Sources de risques	Identifier les sources de risques (SR) pertinentes et leurs objectifs visés (OV) : cybercriminels, États, initiés, concurrents
3	Scénarios stratégiques	Construire les chemins d'attaque de haut niveau (SR → OV → bien support) et évaluer l'impact métier de chaque scénario
4	Scénarios opérationnels	Décliner les scénarios stratégiques en chemins d'attaque techniques (MITRE ATT&CK) et évaluer leur vraisemblance
5	Traitement des risques	Définir les mesures de sécurité, construire le plan de traitement du risque (PTR), calculer les risques résiduels, valider avec la direction

Complémentarité ISO 27005 / EBIOS RM / MITRE ATT&CK

Outil / Cadre	Niveau	Apport dans la démarche risques
ISO 27005	Stratégique & organisationnel	Processus structurant, exigé pour ISO 27001, cadre d'ensemble de la gestion des risques
EBIOS Risk Manager	Stratégique & opérationnel	Scénarios d'attaque réalistes, implication des métiers, orienté NIS2 et LPM

MITRE ATT&CK	Opérationnel & technique	Base de connaissances des tactiques et techniques d'attaque réelles pour construire les scénarios opérationnels
CIS Controls v8	Opérationnel	Prioritisation des mesures de sécurité en 3 groupes d'implémentation (IG1, IG2, IG3)
CVSS	Technique	Scoring standardisé des vulnérabilités pour prioriser les correctifs (0 à 10)

3. Identification des Actifs et des Menaces

Objectif : Lister et qualifier les ressources critiques et les vecteurs d'attaque

▸ Classification des actifs (ISO 27005)

ISO 27005 distingue deux grandes catégories d'actifs : les actifs primaires (ce que l'on cherche à protéger) et les actifs supports (ce qui porte les actifs primaires et peut être exposé à des menaces).

Catégorie	Type d'actif	Exemples concrets
Actifs primaires	Informations / données	Base de données clients, données RH, brevets, contrats, données financières
Actifs primaires	Processus métier	Processus de prise de commande, facturation, paye, gestion de crise
Actifs supports	Matériels	Serveurs, postes de travail, équipements réseau, IoT, smartphones
Actifs supports	Logiciels	ERP, CRM, OS, applicatifs métier, middleware, hyperviseurs
Actifs supports	Réseaux et télécom	LAN, WAN, Internet, Wi-Fi, VPN, liaisons opérateur, DNS, DHCP
Actifs supports	Personnes	Administrateurs SI, RSSI, utilisateurs ayant accès à des données sensibles
Actifs supports	Sites / Locaux	Datacenters, salles serveurs, bureaux, locaux techniques
Actifs supports	Prestataires / Organisation	Hébergeurs, ESN, fournisseurs cloud, partenaires avec accès SI

▸ Évaluation de la criticité des actifs

Chaque actif est évalué selon les 3 critères DIC (Disponibilité, Intégrité, Confidentialité) sur une échelle de 1 à 4, afin d'obtenir un score de criticité global.

Niveau	Label	Disponibilité	Intégrité	Confidentialité
1	Faible	Interruption tolérée plusieurs jours	Erreurs sans conséquence grave	Données publiques ou non sensibles
2	Modéré	Interruption tolérée quelques heures	Erreurs à impact limité et détectable	Données internes, non classifiées
3	Élevé	Interruption max. 1h, impact opérationnel fort	Erreurs à impact significatif sur le métier	Données confidentielles à diffusion restreinte

4	Critique	Temps réel, toute interruption inacceptable	Toute altération est inacceptable	Données sensibles, secret professionnel, brevets

▸ Identification des menaces — Catalogue de référence

Catégorie de menace	Source	Exemples de menaces
Malveillance externe	Cybercriminels, hacktivistes, États	Ransomware, phishing, DDoS, espionnage, APT, exploitation de CVE
Malveillance interne	Employés, prestataires mal intentionnés	Exfiltration de données, sabotage, fraude, abus de privilèges
Erreur humaine	Utilisateurs, administrateurs	Mauvaise configuration, envoi de données au mauvais destinataire, suppression accidentelle
Défaillance technique	Matériel, logiciel	Panne disque, bug logiciel, crash système, obsolescence non gérée
Accident physique	Environnement, infrastructure	Incendie, inondation, coupure électrique, dégâts des eaux, séisme
Dépendance fournisseur	Prestataires, cloud, chaîne d'approvisionnement	Faillite fournisseur, attaque supply chain, indisponibilité SaaS critique

▸ Sources de risques (EBIOS RM) — Profils des attaquants

Source de risque	Motivation principale	Capacité typique	Exemples d'objectifs visés
Cybercriminel / groupe organisé	Gain financier	Élevée (outils sophistiqués)	Rançon, vol de données bancaires, fraude au virement
État / APT	Espionnage, déstabilisation	Très élevée (ressources d'État)	Vol de propriété intellectuelle, sabotage infrastructures critiques
Hacktiviste	Idéologie, réputation	Modérée	Défacement, DDoS, fuite de données publiques (leak)
Concurrent / Intelligence économique	Avantage concurrentiel	Variable	Vol de savoir-faire, secrets de fabrication, offres commerciales
Initié malveillant	Vengeance, profit personnel	Faible à élevée (accès légitimes)	Sabotage, exfiltration, fraude, vente de données
Initié négligent	Inadvertance, manque de formation	N/A	Fuite accidentelle, erreur de configuration, perte de support

🔓 4. Évaluation des Vulnérabilités et Scénarios d'Attaque

> **Objectif :** Identifier les failles et construire les scénarios de risques

▸ Identification et qualification des vulnérabilités

Type de vulnérabilité	Source d'identification	Exemples
Techniques (systèmes et réseaux)	Scan de vulnérabilités (Nessus, Qualys), CVE/NVD, pentest	Port ouvert inutile, CVE non patchée, protocole obsolète (SMBv1, Telnet)
Applicatives (code et config)	Audit de code, DAST, SAST, OWASP Top 10	Injection SQL, XSS, mauvaise gestion des sessions, secrets en dur dans le code
Organisationnelles	Audit de conformité PSSI, entretiens, revue de processus	Absence de procédure de gestion des incidents, droits non revus, BYOD non encadré
Humaines	Campagnes de phishing simulé, quiz, observation	Mots de passe faibles, clic sur liens malveillants, partage d'identifiants
Physiques et environnementales	Inspection physique, audit datacenter	Accès aux baies serveurs non contrôlé, absence de groupe électrogène, caméras insuffisantes

▸ Scoring CVSS — Évaluation standardisée des vulnérabilités

Groupe de métriques CVSS v3.1	Critères évalués	Impact sur le score
Métriques de base (Base)	Vecteur d'attaque, complexité, privilèges requis, interaction utilisateur, impacts CIA	Score de base (0-10) — fixe et indépendant de l'environnement
Métriques temporelles (Temporal)	Maturité du code d'exploitation, disponibilité des correctifs, niveau de confiance	Ajuste le score à l'état actuel de la menace (peut diminuer ou augmenter)
Métriques environnementales (Environmental)	Exigences CIA spécifiques à l'organisation, présence de mesures compensatoires	Score final adapté au contexte de l'organisation — le plus pertinent pour prioriser

Score	Criticité	Délai de patch cible	Mesure intermédiaire	Exemple
9.0 – 10.0	🔴 Critique	Immédiat (< 24-72h)	Isolation du système si possible	Log4Shell (CVE-2021-44228, CVSS 10.0)
7.0 – 8.9	🟠 Élevée	< 7 jours	Surveillance renforcée, WAF, règles IPS	EternalBlue (CVE-2017-0144, CVSS 8.1)
4.0 – 6.9	🟡 Modérée	< 30 jours	Plan de patch planifié	Vulnérabilité XSS persistante

0.1 – 3.9	🟢 Faible	Prochaine fenêtre de maintenance	Surveillance normale	Divulgation d'informations non sensibles

▸ Construction des scénarios de risques

Un scénario de risque décrit de manière structurée comment une menace, exploitant une vulnérabilité sur un actif, peut produire un impact sur l'organisation.

Composante du scénario	Description et questions clés
Source de risque (Qui ?)	Quel acteur est à l'origine de l'attaque ? Quelle est sa motivation et sa capacité ?
Vecteur d'attaque (Comment ?)	Par quel chemin ou mécanisme l'attaque se déroule-t-elle ? (phishing, exploitation CVE, accès physique…)
Actif cible (Sur quoi ?)	Quel actif (primaire ou support) est visé par l'attaque ?
Vulnérabilité exploitée (Pourquoi ?)	Quelle faiblesse permet à la menace de se concrétiser ? (CVE, mauvaise config, erreur humaine…)
Impact redouté (Quelles conséquences ?)	Quelles sont les conséquences sur la disponibilité, l'intégrité, la confidentialité ? Sur le métier ?

Exemple de scénario de risque formalisé

Champ	Contenu du scénario
Identifiant	SCN-042 — Compromission du SI via phishing ciblé sur un compte administrateur
Source de risque	Groupe cybercriminel à motivation financière (capacité élevée)
Vecteur d'attaque	Email de spear phishing → vol de credentials → mouvement latéral → déploiement ransomware
Actif cible	Serveur Active Directory (actif support critique), données métier sur NAS (actif primaire)
Vulnérabilités exploitées	Absence de MFA sur les comptes admin, utilisateurs non sensibilisés au phishing, segmentation réseau insuffisante
Impact redouté	Chiffrement total du SI (D=4), altération des sauvegardes (I=3), exfiltration de données clients (C=4) — impact critique

5. Mesure et Hiérarchisation des Risques

> **Objectif :** Évaluer la vraisemblance et l'impact pour prioriser les actions

▸ Échelles d'évaluation — Vraisemblance et Impact

Niveau	Label	Vraisemblance (probabilité d'occurrence)	Impact (gravité des conséquences)
1	Faible / Négligeable	Scénario peu probable, menace faible capacité, vulnérabilité difficile à exploiter	Impact limité : perturbation mineure, perte financière

			négligeable, aucune fuite de données
2	Modéré / Limité	Scénario possible, menace opportuniste, vulnérabilité connue mais peu exposée	Impact modéré : interruption partielle, plaintes clients limitées, données peu sensibles exposées
3	Élevé / Significatif	Scénario probable, menace active, vulnérabilité exploitable facilement	Impact fort : interruption majeure, perte financière significative, données personnelles exposées
4	Critique / Maximal	Scénario très probable, menace hautement ciblée, actif très exposé	Impact catastrophique : arrêt total, sanction réglementaire, atteinte à la réputation irréversible

▸ Calcul du niveau de risque

Approche	Description
Approche qualitative	Attribution d'un niveau sur une échelle descriptive (Faible / Modéré / Élevé / Critique) ; la plus courante en EBIOS RM
Approche semi-quantitative	Multiplication des scores (Vraisemblance × Impact) sur une grille numérique ; utilisée dans ISO 27005
Approche quantitative (FAIR)	Estimation des pertes financières en euros (esperance de perte annuelle — ALE) ; utile pour la direction financière

Exemple de calcul semi-quantitatif (échelle 1-4)

Scénario de risque	V	I	Score (V×I)	Niveau	Traitement prioritaire
Ransomware via phishing admin (SCN-042)	3	4	12	🔴 Critique	Immédiat : MFA + sensibilisation + segmentation
Fuite données clients via API exposée	2	4	8	🟠 Élevé	< 30j : revue des API, WAF, tests d'intrusion
Indisponibilité SI suite panne datacenter	2	3	6	🟠 Élevé	< 60j : PCA, redondance, sauvegarde hors site
Vol de poste non chiffré (télétravail)	2	2	4	🟡 Modéré	< 90j : chiffrement intégral, MDM
Erreur de configuration firewall	1	3	3	🟡 Modéré	Planifié : revue règles firewall, test semestriel
Accès non autorisé archive papier	1	1	1	🟢 Faible	Accepté : contrôle d'accès minimal suffisant

▸ Critères de hiérarchisation des risques

- Score V × I : priorité aux risques à score élevé, surtout si l'impact est maximal (I = 4)
- Réglementation : les risques entraînant une violation RGPD ou un incident NIS2 sont traités en priorité absolue
- Visibilité externe : les risques exposant des services publics (site web, API) sont prioritaires sur les risques internes

- Facilité d'exploitation : une vulnérabilité facile à exploiter (CVSS > 9, PoC public disponible) remonte automatiquement
- Coût du traitement : un risque élevé mais peu coûteux à traiter est priorisé par rapport à un risque similaire nécessitant un projet long

6. Élaboration de la Cartographie des Risques

> **Objectif :** Construire la matrice des risques cybersécurité

Définition et objectifs de la cartographie des risques

La cartographie des risques est une représentation visuelle et synthétique du portefeuille de risques d'une organisation. Elle permet d'identifier d'un coup d'oeil les risques prioritaires, de communiquer avec la direction et d'orienter les décisions d'investissement sécurité.

Objectif	Valeur ajoutée
Vision consolidée	Regrouper tous les risques identifiés dans un document de référence unique
Priorisation visuelle	Distinguer immédiatement les risques à traiter en urgence de ceux acceptables
Communication direction	Présenter le niveau d'exposition dans un format accessible pour les non-techniciens
Pilotage dans le temps	Suivre l'évolution du niveau de risque après mise en oeuvre des mesures
Conformité réglementaire	Répondre aux exigences de NIS2, DORA, ISO 27001 imposant une gestion formalisée des risques

Matrice des risques — Heat Map 4×4 (Vraisemblance × Impact)

V = Vraisemblance (1 à 4) | I = Impact (1 à 4) | Score = V × I | Les identifiants de scénarios sont placés dans leur case correspondante.

	V=1 Faible	V=2 Modérée	V=3 Élevée	V=4 Critique	Traitement
Impact 4 — Critique	**4** SCN-X12	**8** SCN-X15	**12** SCN-042 SCN-X07	**16** SCN-X01	Critique
Impact 3 — Élevé	**3** SCN-X20	**6** SCN-X08 SCN-X09	**9** SCN-X03	**12** SCN-X02	Élevé
Impact 2 — Modéré	**2**	**4** SCN-X16	**6** SCN-X11	**8** SCN-X05	Modéré
Impact 1 — Faible	**1** SCN-X18	**2**	**3** SCN-X17	**4**	Faible

Légende de la matrice

Couleur	Niveau de risque	Score (V × I)	Action recommandée

🔴	Critique	≥ 9 (ou I=4 + V≥2)	Traitement immédiat — escalade RSSI et direction, mesures d'urgence
🟠	Élevé	6 à 8	Traitement prioritaire — plan d'action sous 30 à 60 jours
🟡	Modéré	3 à 5	Traitement planifié — inclus dans le plan de sécurité annuel
🟢	Faible	1 à 2	Accepté ou surveillance — revue lors de la prochaine réévaluation

▸ Étapes de construction de la cartographie

#	Étape	Contenu
1	Recenser les scénarios	Lister tous les scénarios de risques issus de l'analyse (EBIOS RM / ISO 27005) avec leur identifiant unique
2	Évaluer chaque scénario	Attribuer un score de vraisemblance (1-4) et d'impact (1-4) pour obtenir un score V × I
3	Positionner sur la matrice	Placer chaque scénario dans la case correspondante de la heat map (V en abscisse, I en ordonnée)
4	Définir les zones de traitement	Délimiter les zones rouge / orange / jaune / verte selon l'appétit au risque de l'organisation
5	Associer les traitements	Pour chaque risque en zone rouge/orange : affecter un responsable, des mesures et un délai de traitement
6	Mettre à jour et versionner	Réviser la cartographie après chaque audit, incident ou changement majeur du contexte ; archiver les versions précédentes

▸ Options de traitement et plan de traitement du risque (PTR)

Option	Condition d'application	Exemple concret
🔽 Réduire	Risque au-dessus du seuil d'acceptation, mesures de sécurité faisables et proportionnées	Déployer MFA, patcher les CVE critiques, segmenter le réseau
✅ Accepter	Risque sous le seuil d'acceptation, coût de traitement disproportionné	Accepter le risque de panne ponctuelle d'un système non critique — décision documentée et signée par la DG
🔄 Transférer	Risque résiduel élevé mais difficilement réductible, assurable ou externalisable	Assurance cyber, externalisation vers hébergeur SecNumCloud, clause contractuelle de responsabilité
🚫 Éviter	Activité génératrice du risque peut être supprimée sans impact métier majeur	Renoncer à connecter un SCADA à Internet, abandonner un usage BYOD non sécurisable

▸ Présentation de la cartographie à la direction

- Format synthétique : 1 page de heat map + 1 page de tableau des risques prioritaires (top 10)
- Langage métier : traduire les risques techniques en impacts business (continuité, réputation, finances, conformité)

- Tendance : comparer la cartographie actuelle avec la version N-1 pour montrer la progression des actions
- Décisions à valider : soumettre les risques résiduels à l'acceptation formelle et documentée de la direction
- Fréquence : revue annuelle minimum + revue ad hoc après incident significatif ou changement de périmètre

📌 Mémo Récapitulatif — À Retenir

🎯 Fondamentaux	📚 ISO 27005 & EBIOS	🗂️ Actifs & Menaces	🔓 Vulnérabilités	🔪 Hiérarchisation	🗺️ Cartographie
• Risque = Menace × Vulnérabilité × Impact • 7 étapes du cycle risques (ISO 31000) • Risque brut → net → résiduel • Appétit au risque : décision de la DG • Conformité : RGPD Art.32, NIS2 Art.21	• ISO 27005 : processus structurant (ISO 27001) • EBIOS RM : 5 ateliers, orienté scénarios • MITRE ATT&CK : TTPs pour scénarios opéra. • CVSS : scoring vulnérabilités 0-10 • CIS Controls : 3 groupes d'implémentation	• 2 catégories : actifs primaires / supports • Évaluation DIC : 1 (faible) à 4 (critique) • 6 catégories de menaces (malveillance, erreur…) • EBIOS RM : 6 profils de sources de risques • Menace + Vulnérabilité = risque potentiel	• 5 types de vulnérabilités (tech, orga, humaines…) • CVSS ≥ 9 → patch immédiat < 72h • CVSS 7-8.9 → patch < 7 jours • Scénario = SR + Vecteur + Actif + Vulnéra. + Impact • PoC public = criticité automatiquement majorée	• Échelle 1-4 : V × I = score risque • Score ≥ 9 ou I=4 → traitement immédiat • 3 approches : qualitative / semi-quant. / FAIR • 5 critères de hiérarchisation (réglementaire…) • Prioriser I=4 même si V faible	• Heat map 4×4 : V (abscisse) × I (ordonnée) • 4 zones : rouge / orange / jaune / vert • 4 options : Réduire / Accepter / Transférer / Éviter • Risque résiduel validé et signé par la DG • Revue annuelle + ad hoc après incident