ebios-risk-manager

```
    MARK RODERICK
```

EBIOS Risk Manager — Cours BTS SIO SISR

> **Source officielle :** Guide ANSSI — *EBIOS Risk Manager v1.5* (mise à jour 2024)
> **Norme associée :** ISO/IEC 27005:2022
> **Référentiel BTS SIO :** Bloc 3 — Cybersécurité des services informatiques
> **Compétences :** 3.4.1 Caractérisation des risques · 3.5.2 Sécurité projet

---

1. Qu'est-ce qu'EBIOS RM ?

EBIOS Risk Manager (EBIOS RM) est la **méthode française de référence** pour l'appréciation et le traitement des risques numériques. Elle est publiée par l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) avec le soutien du **Club EBIOS**.

EBIOS = **Expression des Besoins et Identification des Objectifs de Sécurité**

Objectifs de la méthode

- Mettre en place ou renforcer un **processus de management du risque numérique**
- Apprécier et traiter les risques relatifs à un **projet numérique** (ex : homologation de sécurité)
- Définir le **niveau de sécurité** à atteindre pour un produit ou service (certification, agrément)

À qui s'adresse-t-elle ?

- Organisations **publiques et privées**, toutes tailles et secteurs
- OIV (Opérateurs d'Importance Vitale)
- OSE (Opérateurs de Services Essentiels) — contexte NIS2
- Toute entité cherchant à structurer sa gestion des risques cyber

Trois caractéristiques distinctives

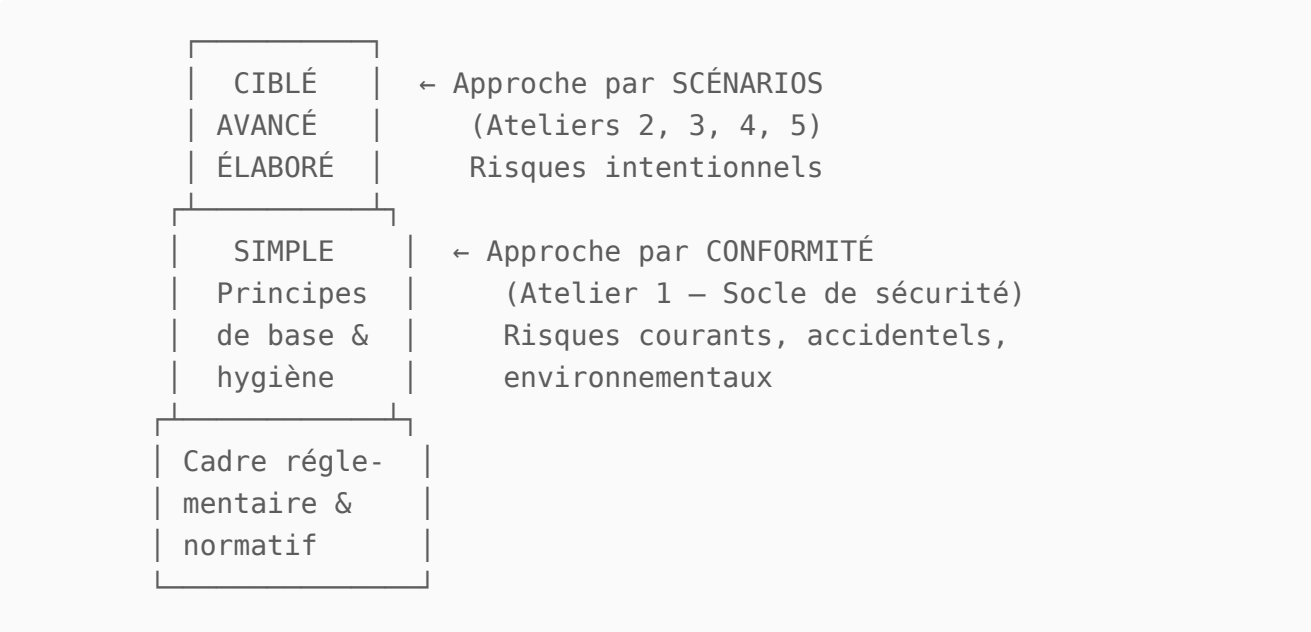
1. **Approche scénario-centrée** — construction de scénarios de risque réalistes, pas une simple liste de menaces génériques
2. **Synthèse conformité + scénarios** — le socle de sécurité (conformité) couvre les risques courants, les scénarios couvrent les menaces avancées et ciblées

3. **Démarche collaborative et itérative** — inspirée des méthodes agiles, implique décideurs ET opérationnels

---

2. La pyramide du management du risque numérique

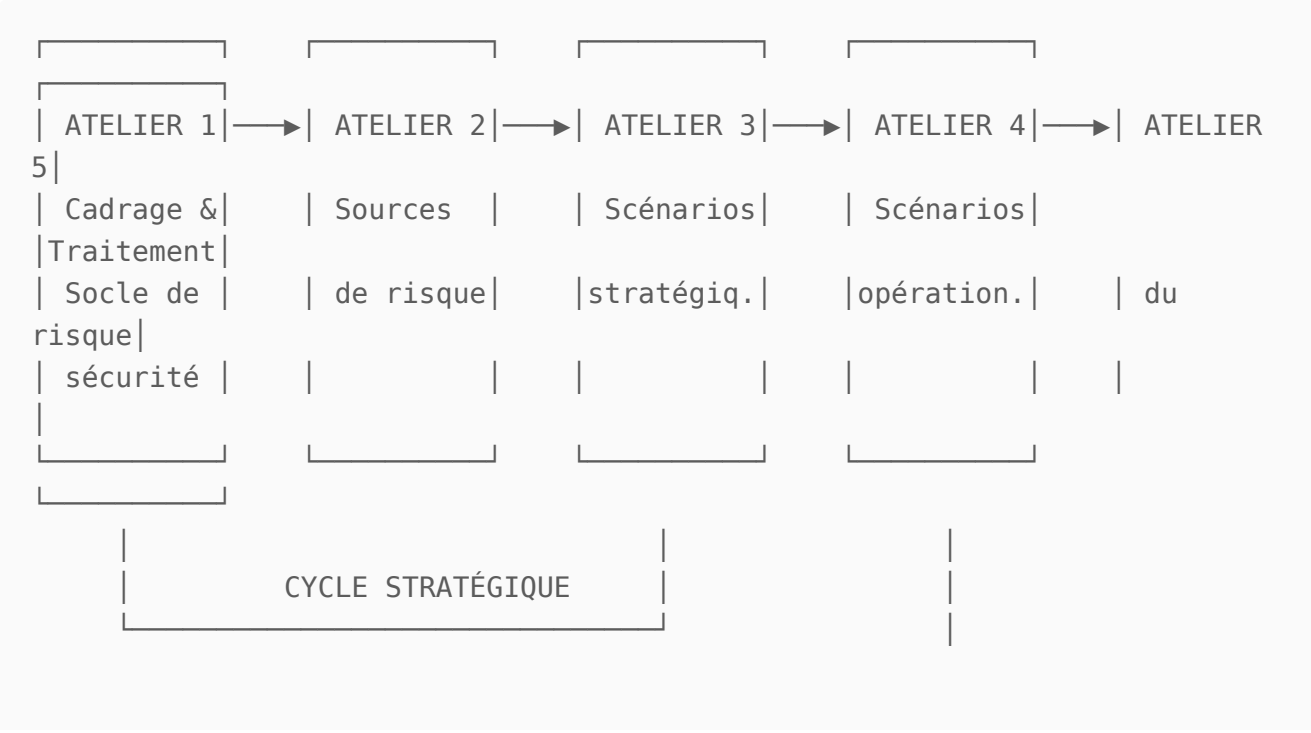
La méthode repose sur une vision en pyramide avec deux approches complémentaires :



Principe : Le socle de sécurité gère les cyberattaques simples par conformité aux référentiels. L'appréciation par scénarios cible les attaques élaborées, avancées et ciblées.

---

3. Les 5 ateliers — Vue d'ensemble



```
                                    CYCLE OPÉRATIONNEL    │
                                    ──────────────────────┘
```

Deux cycles de révision :

- **Cycle stratégique** : revisite l'ensemble de l'étude (ateliers 1–3)
- **Cycle opérationnel** : revisite les scénarios opérationnels à la lumière de nouveaux incidents, vulnérabilités et modes opératoires (ateliers 3–5)

---

4. Atelier 1 — Cadrage et socle de sécurité

> **Durée indicative :** 2 à 4 demi-journées
> **Participants :** Direction, équipes métiers, RSSI, DSI
> **Approche :** Conformité (défense)

Objectif

Définir le **cadre de l'étude**, son périmètre métier et technique, les événements redoutés et le socle de sécurité.

Activités

a) Définir le cadre

- Identifier l'**objet de l'étude** (système, projet, organisation)
- Identifier les **participants** aux ateliers et leurs rôles (matrice RACI)
- Définir le **cadre temporel** (durée de l'étude, cycles de révision)

b) Recenser les valeurs métier et biens supports

Concept	Définition	Exemple
Mission	Finalité de l'objet étudié	Fabriquer et distribuer des vaccins
Valeur métier	Processus ou information essentielle	Recherche & Développement
Bien support	Composant technique supportant la valeur métier	Serveur de base de données, ERP, réseau LAN

c) Identifier les événements redoutés

Pour chaque valeur métier, identifier les événements redoutés et estimer la **gravité des impacts** :

Niveau	Gravité	Description
G1	Négligeable	L'organisation surmonte sans difficulté
G2	Significative	L'organisation surmonte malgré quelques difficultés
G3	Grave	L'organisation surmonte avec de sérieuses difficultés
G4	Critique	L'organisation ne peut pas surmonter

d) Évaluer le socle de sécurité

- S'appuyer sur les **référentiels** : Guide d'hygiène ANSSI, ISO 27001, PSSI
- Pour chaque règle, évaluer : **Appliqué / Partiellement appliqué / Non appliqué**
- Les **écarts identifiés** alimentent directement le plan de traitement (Atelier 5)

Livrables

- Périmètre de l'étude documenté
- Liste des valeurs métier classées par criticité
- Événements redoutés avec cotation de gravité
- Évaluation du socle de sécurité avec écarts identifiés

---

5. Atelier 2 — Sources de risque

> **Durée indicative :** 1 à 2 demi-journées
> **Participants :** RSSI, DSI, experts cybersécurité, veille menaces

Objectif

Identifier **qui** peut attaquer l'organisation et **pourquoi**. EBIOS RM se distingue par son approche **adversaires**, pas uniquement menaces génériques.

Concepts clés

Concept	Définition	Exemple
Source de risque (SR)	Entité ou personne à l'origine du risque	Concurrent, hacktiviste, État, employé mécontent
Objectif visé (OV)	Motivation de haut niveau de la source	Voler la propriété intellectuelle, saboter la production
Couple SR/OV	Association source + objectif	Concurrent / Vol de données R&D

Activités

1. **Identifier les sources de risque** — lister les attaquants potentiels en s'aidant de :
   - Veille sur la menace (CERT-FR, MITRE ATT&CK)
   - Contexte géopolitique et sectoriel
   - Historique des incidents
2. **Définir les objectifs visés** — pour chaque source, quels objectifs poursuit-elle ?
3. **Former les couples SR/OV** — associer chaque source à ses objectifs
4. **Évaluer la pertinence** — un couple SR/OV est retenu si sa pertinence dépasse un seuil (motivation × ressources × activité connue)

Livrable

- **Cartographie des sources de risque** : tableau des couples SR/OV retenus pour les ateliers suivants

---

6. Atelier 3 — Scénarios stratégiques

> **Durée indicative :** 2 à 4 demi-journées
> **Participants :** RSSI, DSI, métiers, experts sécurité

Objectif

Construire des **scénarios de haut niveau** décrivant les chemins d'attaque à l'échelle de l'écosystème.

Concepts clés

Concept	Définition
Partie prenante	Tiers en interaction avec l'objet d'étude (fournisseur, prestataire, partenaire)
Écosystème	Ensemble des parties prenantes et de leurs relations avec l'objet d'étude
Scénario stratégique	Chemin d'attaque macro : SR → compromet partie prenante → compromet valeur métier

Activités

1. **Cartographier l'écosystème** — identifier toutes les parties prenantes et évaluer :
   - Niveau de **dépendance** (à quel point l'objet d'étude dépend de cette partie prenante)
   - Niveau de **pénétration** (à quel point la partie prenante a accès au SI)
   - Niveau de **maturité cyber** de la partie prenante
   - → Niveau de **dangerosité** résultant

2. **Construire les scénarios stratégiques** — pour chaque couple SR/OV retenu :
   - Identifier les chemins d'attaque passant par l'écosystème
   - Décrire la chaîne : SR → vecteur (partie prenante) → impact sur valeur métier
3. **Coter la gravité** — chaque scénario reçoit une cotation G1 à G4

> **Exemple :** *Concurrent → compromet le cabinet comptable externe (accès VPN) → accède à la base de données financières → exfiltration de données stratégiques* → Gravité G3

Livrables

- Cartographie de l'écosystème avec niveaux de dangerosité
- Scénarios stratégiques avec gravité estimée
- Premières mesures de sécurité sur l'écosystème

---

7. Atelier 4 — Scénarios opérationnels

> **Durée indicative :** 1 à 3 demi-journées
> **Participants :** Experts techniques, administrateurs systèmes et réseaux, RSSI

Objectif

Traduire les scénarios stratégiques en **scénarios techniques** décrivant les modes opératoires concrets des attaquants.

Lien avec l'Atelier 3

```
Couple SR/OV (Atelier 2)
    └─▶ Scénario stratégique (Atelier 3)  → GRAVITÉ
            └─▶ Chemin d'attaque 1
                    └─▶ Scénario opérationnel 1 (Atelier 4)  → VRAISEMBLANCE
            └─▶ Chemin d'attaque 2
                    └─▶ Scénario opérationnel 2 (Atelier 4)  → VRAISEMBLANCE
```

Activités

1. **Pour chaque scénario stratégique**, détailler les modes opératoires techniques :
   - Vecteur d'entrée (phishing, exploitation vulnérabilité, accès physique)
   - Méthode de compromission (élévation de privilèges, mouvement latéral)
   - Actions sur l'objectif (exfiltration, chiffrement, sabotage)
2. **S'appuyer sur le référentiel MITRE ATT&CK** pour identifier les tactiques et techniques réalistes
3. **Évaluer la vraisemblance** de chaque scénario opérationnel :

Niveau	Vraisemblance	Description
V1	Peu vraisemblable	Difficile à réaliser, nécessite des moyens très importants
V2	Possible	Réalisable avec des moyens modérés
V3	Vraisemblable	Facilement réalisable avec des moyens standards
V4	Quasi-certain	Trivial à réaliser, déjà observé dans des contextes similaires

Livrable

- Scénarios opérationnels documentés avec vraisemblance estimée

---

8. Atelier 5 — Traitement du risque

> **Durée indicative :** 2 à 4 demi-journées
> **Participants :** Direction, RSSI, DSI, métiers

Objectif

Synthétiser les risques et définir une **stratégie de traitement** concrète.

Le niveau de risque

Chaque **scénario de risque** = association d'un scénario stratégique (gravité) + scénario opérationnel (vraisemblance).

```
NIVEAU DE RISQUE = GRAVITÉ × VRAISEMBLANCE
```

Matrice de risque :

	V1 (Peu vraisemblable)	V2 (Possible)	V3 (Vraisemblable)	V4 (Quasi-certain)
G4 (Critique)	Moyen	Élevé	Élevé	Élevé
G3 (Grave)	Faible	Moyen	Élevé	Élevé
G2 (Significative)	Faible	Faible	Moyen	Élevé
G1 (Négligeable)	Faible	Faible	Faible	Moyen

Stratégies de traitement

Pour chaque risque, 4 options :

Stratégie	Description	Quand ?
Réduire	Mettre en œuvre des mesures de sécurité	Risque au-dessus du seuil d'acceptation
Transférer	Confier le risque à un tiers (assurance, sous-traitance)	Risque financier quantifiable
Éviter	Supprimer l'activité à l'origine du risque	Risque inacceptable, activité non essentielle
Accepter	Prendre le risque en connaissance de cause	Risque résiduel sous le seuil d'acceptation

Activités

1. **Synthétiser les risques** sur la matrice gravité × vraisemblance
2. **Définir le seuil d'acceptation** du risque avec la direction
3. **Choisir une stratégie** pour chaque risque au-dessus du seuil
4. **Élaborer le plan de traitement** — chaque mesure doit avoir :
   - Un **responsable** identifié
   - Une **échéance** claire
   - Un **budget** associé
5. **Évaluer les risques résiduels** après application des mesures
6. **Définir le cadre de suivi** (indicateurs, fréquence de révision)

Livrables

- Matrice des risques (cartographie gravité × vraisemblance)
- Plan de traitement du risque (PACS — Plan d'Amélioration Continue de la Sécurité)
- Risques résiduels documentés
- Cadre de suivi des risques

---

9. Synthèse — Tableau récapitulatif des 5 ateliers

Atelier	Nom	Question clé	Livrable principal	Durée
1	Cadrage & Socle de sécurité	Que protéger ? Quel est le niveau actuel ?	Périmètre + événements redoutés + socle	2–4 demi-journées

Atelier	Nom	Question clé	Livrable principal	Durée
2	Sources de risque	Qui peut attaquer et pourquoi ?	Cartographie des couples SR/OV	1–2 demi-journées
3	Scénarios stratégiques	Quels chemins d'attaque via l'écosystème ?	Scénarios stratégiques + gravité	2–4 demi-journées
4	Scénarios opérationnels	Comment techniquement ?	Scénarios opérationnels + vraisemblance	1–3 demi-journées
5	Traitement du risque	Que fait-on ?	Plan de traitement + risques résiduels	2–4 demi-journées

---

10. Vocabulaire essentiel à retenir

Terme	Définition
Valeur métier	Processus ou information essentielle à protéger (= bien essentiel EBIOS 2010)
Bien support	Composant technique supportant une valeur métier
Événement redouté	Scénario négatif associé à une valeur métier (perte de confidentialité, d'intégrité, de disponibilité)
Socle de sécurité	Niveau minimal de protection attendu (référentiels, bonnes pratiques)
Source de risque (SR)	Entité à l'origine du risque (attaquant)
Objectif visé (OV)	Motivation de la source de risque
Couple SR/OV	Association source + motivation
Partie prenante	Tiers en interaction avec l'objet d'étude (fournisseur, prestataire, etc.)
Scénario stratégique	Chemin d'attaque de haut niveau passant par l'écosystème
Scénario opérationnel	Description technique du mode opératoire de l'attaque
Gravité	Niveau d'impact d'un scénario (G1 à G4)
Vraisemblance	Probabilité de réalisation d'un scénario opérationnel (V1 à V4)
PACS	Plan d'Amélioration Continue de la Sécurité

---

11. Compatibilité et contexte réglementaire

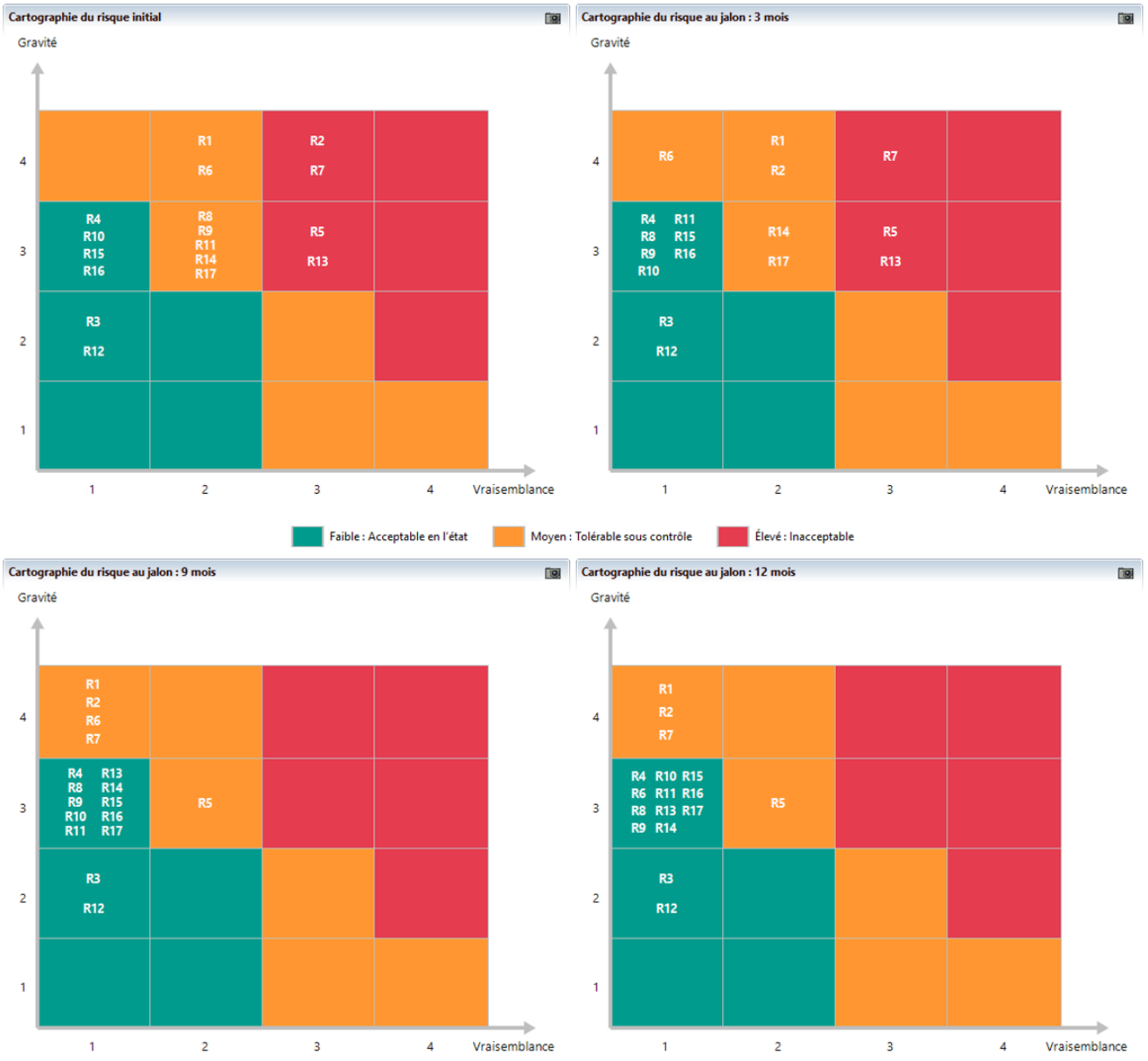
EBIOS RM est conforme et compatible avec :

- **ISO/IEC 27005:2022** — cadre international de gestion des risques SI
- **ISO 31000:2018** — management du risque (générique)
- **ISO 27001** — SMSI (Système de Management de la Sécurité de l'Information)
- **NIS2** — directive européenne sur la sécurité des réseaux et SI
- **DORA** — résilience opérationnelle numérique (secteur financier)
- **LPM** — Loi de Programmation Militaire (OIV)
- **RGPD** — l'AIPD peut s'appuyer sur EBIOS RM

---

12. Ressources

- Guide officiel ANSSI — EBIOS RM v1.5 (PDF)
- Page ANSSI — La méthode EBIOS Risk Manager
- Club EBIOS — Fiches méthodes et suppléments
- MITRE ATT&CK — Référentiel tactiques et techniques
- EBIOS RM Pro — Outil open source gratuit (GitHub)


Cartographie du risque initial
Gravité
4
3
2
1
R1
R6
R2
R7
R4
R10
R15
R16
R8
R9
R11
R14
R17
R5
R13
R3
R12
1
2
3
4
Vraisemblance
Cartographie du risque au jalon : 3 mois
Gravité
R6
R1
R2
R7
R4
R8
R9
R10
R11
R15
R16
R14
R17
R5
R13
R3
R12
Faible : Acceptable en l'état
Moyen : Tolérable sous contrôle
Élevé : Inacceptable
Cartographie du risque au jalon : 9 mois
Gravité
R1
R2
R6
R7
R4
R8
R9
R10
R11
R13
R14
R15
R16
R17
R5
R3
R12
Cartographie du risque au jalon : 12 mois
Gravité
R1
R2
R7
R4
R6
R8
R9
R10
R11
R13
R15
R16
R17
R14
R5
R3
R12