Appréciation et traitement des risques – EBIOS RM

EBIOS RISK MANAGER

1) Risque, gravité et vraisemblance
2) Qu'est-ce que EBIOS RM ?
3) Les ateliers
4) La matrice des scénarios
5) Les stratégies de traitement des risques
6) Un exemple

CLUBEBIOS

ANSSI | Agence nationale de la sécurité des systèmes d'information

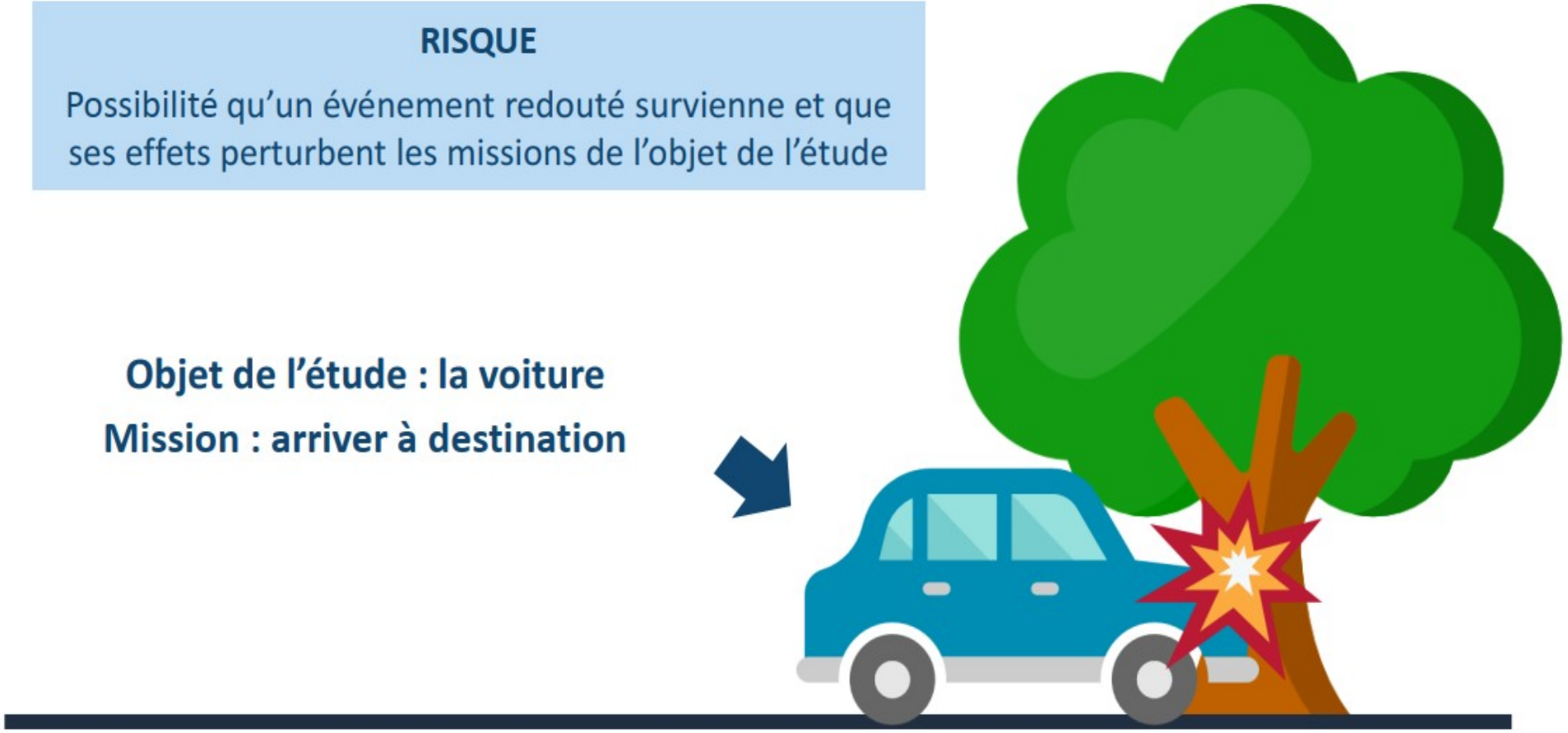
Qu'est-ce qu'un risque ?

RISQUE

Possibilité qu'un événement redouté survienne et que ses effets perturbent les missions de l'objet de l'étude

Objet de l'étude : la voiture

Mission : arriver à destination

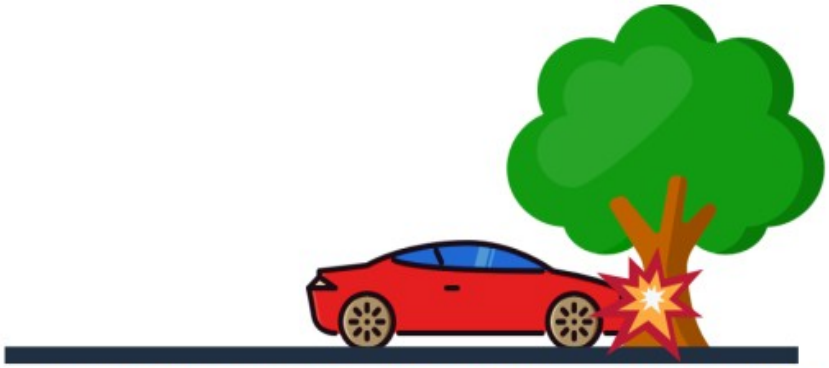


Événement redouté : la voiture percute un arbre

Quelle est la gravité de ce risque ?

La gravité varie selon la vitesse de la voiture

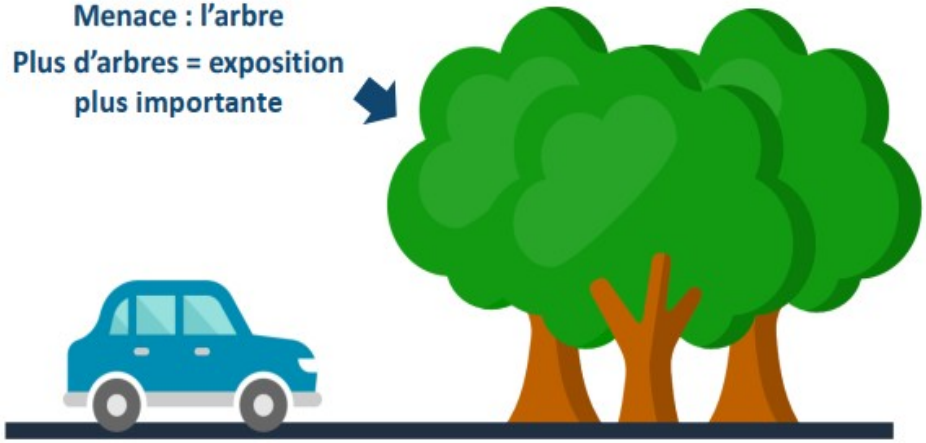
La gravité varie également selon la taille de l'arbre



La gravité varie selon la valeur (prix, robustesse) de la voiture

La gravité varie selon le nombre d'impacts et leur niveau mais aussi selon la valeur de l'objet étudié

Quelle est la vraisemblance de ce risque ?



La vraisemblance varie selon le nombre d'arbres

La vraisemblance varie selon le niveau d'attention du conducteur

La vraisemblance varie selon les panneaux de signalisation en place

La vraisemblance varie selon l'exposition aux menaces, le niveau de vulnérabilité et les mesures de sécurité

Comment évaluer le niveau d'un risque ?

NIVEAU DE RISQUE (EBIOS *RISK MANAGER*)

Mesure de l'importance du risque, exprimée par la combinaison de la gravité et de la vraisemblance

GRAVITÉ

Estimation du niveau et de l'intensité des effets d'un risque

VRAISEMBLANCE

Estimation de la faisabilité ou de la probabilité qu'un risque se réalise

L'estimation de la gravité et de la vraisemblance sont réalisées grâce à des échelles définies par l'organisation

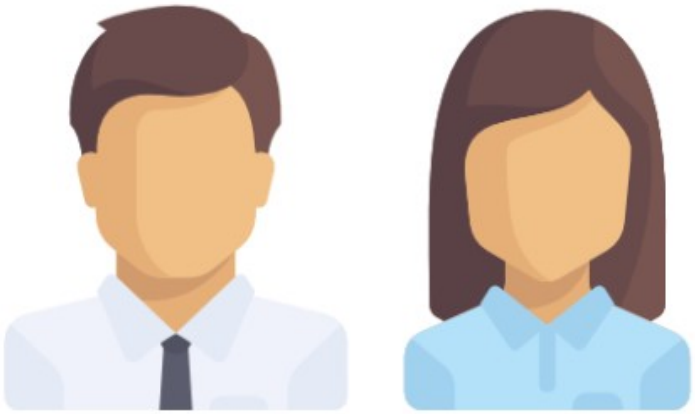
Quelques questions à se poser

Quel est mon degré d'exposition à ces risques ?

Comment maitriser ces risques pour les rendre tolérables ou acceptables ?

Quels sont les risques qui pèsent sur mon SI ou mon projet ?

Comment gérer les risques dans le temps ?



Qu’est-ce que EBIOS RM ?

EBIOS RM (**Expression des Besoins et Identification des Objectifs de Sécurité – *Risk Manager***) est une méthode d’appréciation et de traitement des risques numériques publiée par **l’ANSSI**. Elle permet **d’identifier les mesures de sécurité à mettre en œuvre pour les maîtriser et définir un niveau de sécurité à atteindre pour un service**.

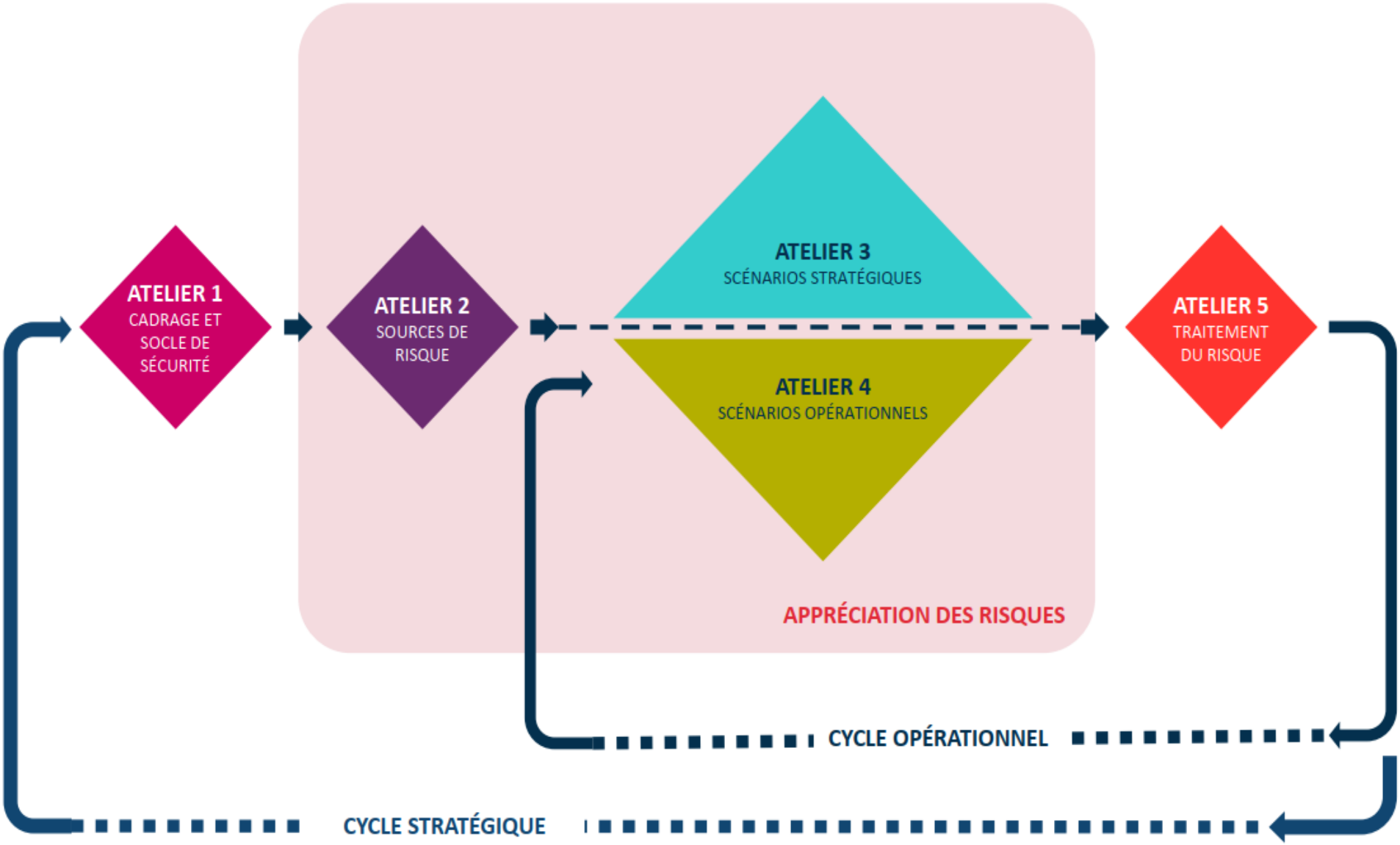
La **méthode de référence française** EBIOS accompagne les organisations pour identifier et comprendre les risques numériques qui leurs sont propres. Cependant, EBIOS RM n’est pas une norme, mais une méthode, surtout utilisée en France. La norme internationale est l’ISO 27005. EBIOS RM propose une solution de méthode dans la mise en œuvre d’une démarche ISO 27005.

EBIOS RM se base sur différents scénarios et se concentre sur les **menaces intentionnelles**.

Les ateliers

La méthode EBIOS RM est décomposée en **5 « ateliers »**

EBIOS *Risk Manager* : une méthode basée sur 5 ateliers



L'atelier 1 : Cadrage et socle de sécurité

Cette étape recense les **valeurs « métier »** (informations et processus importants) susceptibles d'être attaquées, les besoins de sécurité associés (en termes de disponibilité, confidentialité, intégrité, etc.) et les biens supports (éléments du SI sur lesquels les valeurs métier reposent) ; ensuite, les **évènements redoutés** sont identifiés et la **gravité** caractérisée.

Participants à l'atelier : Direction, Métiers, RSSI, DSI

Exemple partiel pour une mairie :

VALEUR MÉTIER	ÉVÈNEMENT REDOUTÉ	IMPACTS	GRAVITÉ
Fournir un service pour les actes d'état-civil (passeport, carte nationale d'identité, etc.)	Perte ou destruction des données concernant les usagers	▪ Impacts sur les missions et services de la mairie ▪ Impacts sur l'image et la confiance ▪ Impacts juridiques, etc.	**4/4**
Fournir un service de santé avec le centre municipal de santé	Perte ou destructions des données de santé des habitants	▪ Impacts sur les missions et services de la mairie ▪ Impacts sur l'image et la confiance ▪ Impacts juridiques, etc.	**4/4**

L'échelle de gravité

ÉCHELLE	DÉFINITION
G4 – CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée)
G3 – GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé)
G2 – SIGNIFICATIVE	Dégradation des performances de l'activité sans impacts sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé)
G1 – MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges)

L’atelier 2 : Sources de risque

Cette étape permet d’**identifier les sources de risques** les plus pertinentes et leurs objectifs visés.

Participants à l’atelier : Métiers, RSSI, (spécialiste de la menace cyber), Direction

Exemple :

SOURCES DE RISQUE	OBJECTIFS VISÉS	MOTIVATION	RESSOURCES	ACTIVITÉ	PERTINENCE
Cyber-terroriste	Voler les informations personnelles des usagers dans un but financier	+ +	+ + +	+	**Moyenne**
Cyber-terroriste	Bloquer le SI avec demande de rançon sans exfiltrer les données	+ + +	+ + +	+ +	**Haute**
Usager malveillant	Accéder à des données sensibles sans autorisation en exploitant une faille	+	+	+	**Faible**

Évaluation de la pertinence

			RESSOURCES			
			Incluant les ressources financières, le niveau de compétences cyber, l'ouillage, le temps dont l'attaquant dispose pour réaliser l'attaque, etc.			
			Ressources limitées	Ressources significatives	Ressources importantes	Ressources illimitées
MOTIVATION	Intérêts, éléments qui poussent la source de risque à atteindre son objectif	Fortement motivé	**Moyennement pertinent**	**Plutôt pertinent**	**Très pertinent**	**Très pertinent**
		Assez motivé	**Moyennement pertinent**	**Plutôt pertinent**	**Plutôt pertinent**	**Très pertinent**
		Peu motivé	**Peu pertinent**	**Moyennement pertinent**	**Plutôt pertinent**	**Plutôt pertinent**
		Très peu motivé	**Peu pertinent**	**Peu pertinent**	**Moyennement pertinent**	**Moyennement pertinent**

L’atelier 3 : Scénarios stratégiques

Cette étape permet d’identifier les parties prenantes externes les plus vulnérables et de bâtir des scénarios stratégiques : **chemins d’attaques** que pourrait emprunter une source de risque pour atteindre son objectif.

Participants à l’atelier : Métiers, Architecte fonctionnel, Juristes, RSSI, (spécialiste de la menace cyber)

Exemple :

PARTIE PRENANTE	CHEMINS D’ATTAQUE STRATÉGIQUES	MESURES DE SECURITÉ	MENACE INITIALE	MENACE RÉSIDUELLE
Prestataire informatique	Vol d’informations en passant par le prestataire informatique	Accroître la maturité cyber du prestataire. Solutions à investiguer : audit de sécurité, etc.	2/5	1,2/5

L’atelier 4 : Scénarios opérationnels

Cette étape détaille les scénarios opérationnels, c’est-à-dire les **modes opératoires** que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques.

Participants à l’atelier : RSSI, DSI, Architecte SI, (spécialiste de la menace cyber)

Exemple :

CHEMINS D’ATTAQUES STRATÉGIQUES (ASSOCIÉS AUX SCÉNARIOS OPÉRATIONNELS)	VRAISEMBLANCE GLOBALE
Une personne malveillante (pirate) compromet un logiciel fourni par un prestataire et utilisé dans le SI de la mairie (vol de données par une porte dérobée)	Peu vraisemblable (1/4)
Un groupe de pirates envoie un courriel d’hameçonnage à un utilisateur du réseau et crée une porte dérobée pour exfiltrer des données	Très vraisemblable (3/4)
Un groupe de pirate envoie un courriel d’hameçonnage à un utilisateur du réseau et infecte un poste informatique avec un rançongiciel	Très vraisemblable (3/4)

Définir une échelle de vraisemblance

ÉCHELLE	DÉFINITION
V4 – CERTAIN OU DÉJÀ PRODUIT	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés OU un tel scénario s'est déjà produit au sein de l'organisation (historique d'incidents)
V3 – TRÈS VRAISEMBLABLE	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée
V2 – VRAISEMBLABLE	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative
V1 – PEU VRAISEMBLABLE	La source de risque a peu de chances d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible

L'atelier 5 : Traitement du risque

Cette dernière étape permet de définir une stratégie de traitement du risque avec une série de **mesures de sécurité à mettre en œuvre**.

Participants à l'atelier : Direction, Métiers, RSSI, DSI

Exemples :

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN OEUVRE	COÛT / COMPLEXITÉ	ÉCHÉANCE	STATUT
Sensibilisation à l'hameçonnage	R2, R3	DSI, entreprise spécialisée		+	3 mois	Terminée
Audit de sécurité de l'ensemble du SI	Rx	DSI, pôle PSIR	Nécessite une cartographie complète et à jour	+ + +	6 mois	En cours
Surveillance renforcée des flux entrants et sortants	R2, R3	Pôle PSIR	Besoin de veille (signes d'infection - IOC à surveiller)	+	1 mois	En cours
Protection renforcée des données	R1, R2, R3	Pôle PIS		+	1 mois	À lancer
Analyse des journaux d'évènements à l'aide d'un outil	R1, R2, R3, R4	Pôle PSIR	Quantité de logs	+ +	2 mois	À lancer
Renforcement du PCA	Rx	DSI	Prévoir une solution cloud	+ + +	12 mois	À lancer
…	…	…	…	…	…	…

Rx = Tous les scénarios de risques

Source : d'après le « Guide EBIOS Risk Manager » de l'ANSSI

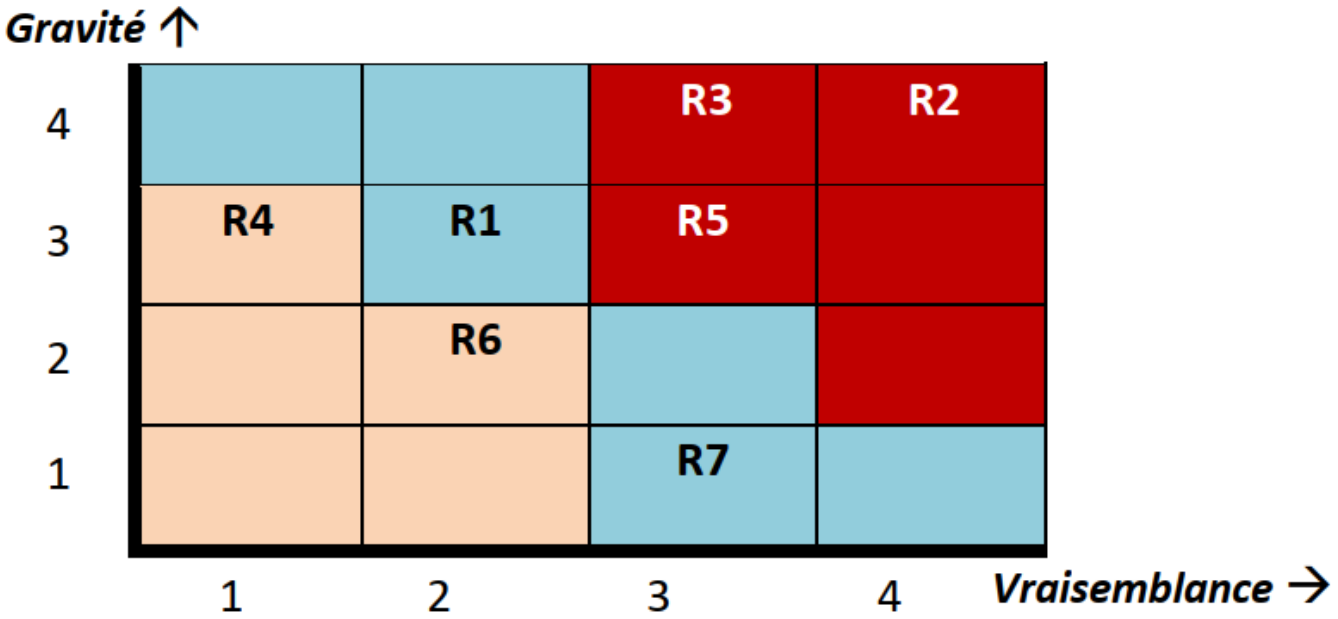
Bilan de l'analyse : matrice des scénarios de risques

Exemples :

- *R1 : un utilisateur du réseau tente d'accéder à des données sans autorisation*
- *R4 : un utilisateur ne respecte pas l'interdiction et se connecte au réseau de la ville avec sa*

propre machine (infectée par un virus)

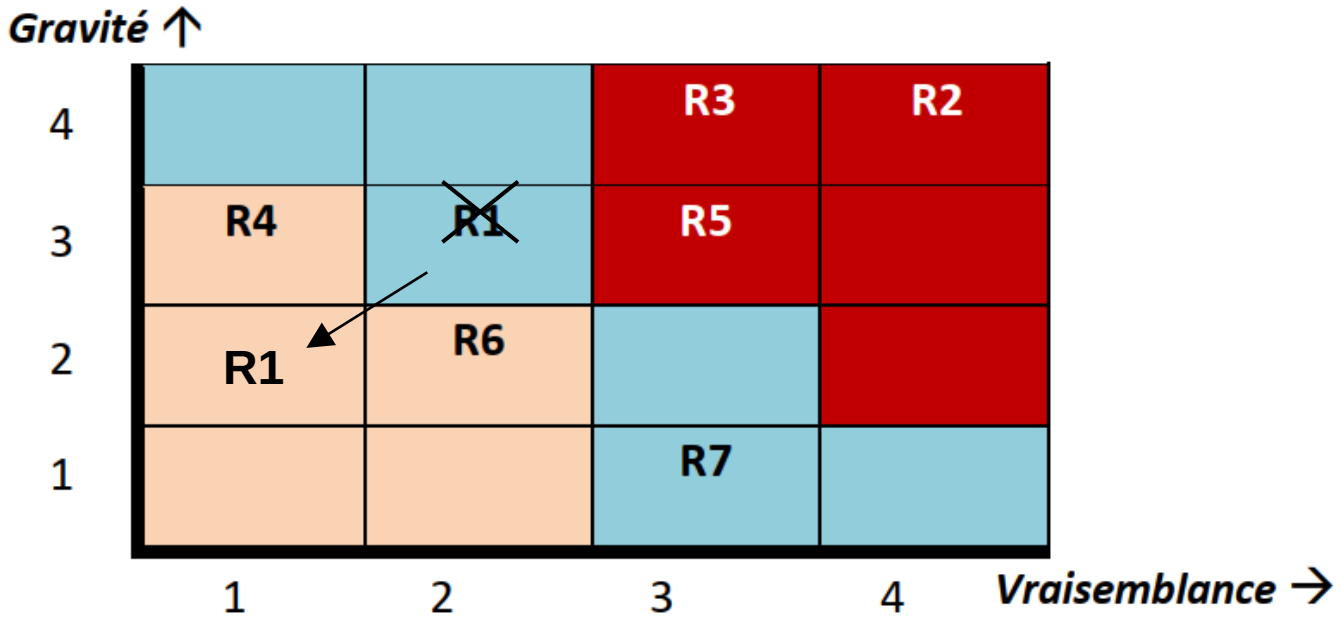
- *[…]*



Bilan de l'analyse : matrice des scénarios de risques

Après la mise en œuvre des nouvelles mesures de sécurité, la matrice évolue.

Exemple : après la mise en place d'un filtrage plus restrictifs de flux et le chiffrement des données stockées, le risque R1 évolue :



Sources

ANSSI : la méthode EBIOS RM

https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

ANSSI | Agence nationale de la sécurité des systèmes d'information

SUJET BTS E6 SISR 2023 : cas ville du Parc

U6 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES