Étude des risques EBIOS

[NOM]

[NOM DU PROJET]

Document de travail du [DATE]

Historique des modifications

Date	Objet de la modification	Statut

Table des matières

1 Étude des risques

Étude du contexte

Le cadre de la gestion des risques

Objectif de l'étude

Plan d'action

Pour réaliser l'étude des risques SSI, la structure de travail prévue est la suivante :

Activités d'EBIOS	Responsable projet	Responsable Technique	Responsable de l'étude	Documents à produire	Ressources estimées (en h.j)	Durée (en jours)
1.1 – Définir le cadre de la gestion des risques				✓ Étude des risques		
1.2 – Préparer les métriques						
1.3 – Identifier les biens						
2.1 – Apprécier les événements redoutés						
3.1 – Apprécier les scénarios de menaces						
4.1 – Apprécier les risques						
4.2 – Identifier les objectifs de sécurité				✓ FEROS		
5.1 – Formaliser les mesures à mettre en œuvre				✓ PSSI		
5.2 – Mettre en œuvre les mesures de sécurité				✓ Décision d'homologation		

Légende : R = Réalisation ; A = Approbation ; C = Consultation ; I = Information

Sujet de l'étude

Enjeux

Paramètres à prendre en compte

Un ensemble de contraintes à prendre en compte a été identifié :

- ❑ Les références qui impacteront l'étude des risques de sécurité sont les suivantes :

- ❑ Les contraintes qui impacteront l'étude des risques de sécurité sont les suivantes :

- ❑ Les hypothèses qui impacteront l'étude des risques de sécurité sont les suivantes :

Les sources de menaces

Les sources de menaces contre lesquelles on souhaite s'opposer sont suivantes :

Types de sources de menaces	Retenu ou non	Exemples
Source humaine interne, malveillante, avec de faibles capacités	✓	
Source humaine interne, malveillante, avec des capacités importantes	✓	
Source humaine interne, malveillante, avec des capacités illimitées	✓	
Source humaine externe, malveillante, avec de faibles capacités	✓	
Source humaine externe, malveillante, avec des capacités importantes	✓	
Source humaine externe, malveillante, avec des capacités illimitées	✓	
Source humaine interne, sans intention de nuire, avec de faibles capacités	✓	
Source humaine interne, sans intention de nuire, avec des capacités importantes	✓	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	✓	
Source humaine externe, sans intention de nuire, avec de faibles capacités	✓	
Source humaine externe, sans intention de nuire, avec des capacités importantes	✓	
Source humaine externe, sans intention de nuire, avec des capacités illimitées	✓	
Code malveillant d'origine inconnue	✓	
Phénomène naturel	✓	
Catastrophe naturelle ou sanitaire	✓	
Activité animale	✓	
Événement interne	✓	

Les métriques utilisées

Les critères de sécurité retenus : disponibilité, intégrité et confidentialité

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.

Échelle de disponibilité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Journée	Le bien essentiel doit être disponible dans la journée
demi-journée	Le bien essentiel doit être disponible dans la demi-journée.
30 minutes	Le bien essentiel doit être disponible dans la demi-heure.

Échelle d'intégrité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	Description détaillée de l'échelle
Négligeable	Le bien essentiel peut ne pas être intègre.
Acceptable	Le bien essentiel peut ne pas être intègre, mais son altération doit être détectée ou suffisamment faible pour ne pas gêner les opérationnels.
Intègre	Le bien essentiel doit être parfaitement intègre.

Échelle de confidentialité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Restreint projet	Le bien essentiel ne doit être accessible qu'aux personnes du projet.
Confidentiel	Le bien essentiel ne doit être accessible qu'aux personnes dirigeantes.

Échelle de gravité

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
1. Négligeable	L'organisme surmontera les impacts sans aucune difficulté.
2. Limitée	L'organisme surmontera les impacts malgré quelques difficultés.
3. Importante	L'organisme surmontera les impacts avec de sérieuses difficultés.
4. Critique	L'organisme ne jouera pas sa survie mais sera impacté très fortement.

Échelle de vraisemblance

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
1. Minime	Cela ne s'est jamais produit et ne devrait pas se produire.
2. Significative	Cela ne s'est jamais produit, mais pourrait se produire.
3. Forte	Cela s'est rarement produit et pourrait se reproduire.
4. Maximale	Cela se produit régulièrement et devrait se reproduire prochainement.

Les critères de gestion des risques : la liste des règles à utiliser dans l'étude

Les critères de gestion des risques retenus sont les suivants :

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Expression des besoins	❑ Les besoins de sécurité des biens essentiels sont exprimés à l'aide des échelles correspondantes, selon le critère de sécurité étudié. ❑ Les biens essentiels publics (dont le besoin en confidentialité est nul) n'engendrent pas d'événements redoutés en termes de confidentialité.
Estimation des événements redoutés	❑ Les événements redoutés sont estimés en termes de gravité et de vraisemblance à l'aide des échelles définies à cet effet.
Évaluation des événements redoutés	❑ Les événements redoutés sont classés selon leur gravité et leur vraisemblance. ❑ Les événements redoutés dont la gravité est négligeable ou la vraisemblance est invraisemblable sont jugés comme insignifiants. ❑ Ceux dont la gravité est importante ou critique et la vraisemblance est très vraisemblable ou certaine sont importants.
Estimation des scénarios de menaces	❑ Les scénarios de menaces sont estimés en termes de vraisemblance à l'aide de l'échelle définie à cet effet.
Évaluation des scénarios de menaces des risques	❑ Les scénarios de menaces sont classés par ordre décroissant de vraisemblance.
Estimation des risques	❑ La gravité d'un risque est égale à celle de l'événement redouté considéré. ❑ La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.
Évaluation des risques	❑ Les risques doivent être triés par ordre décroissant de leur gravité et de leur vraisemblance. ❑ Les risques les plus importants sont donc les premiers de la liste triée.
Choix de traitement des risques	❑ Les risques dont les niveaux sont maximums doivent être refusés ou réduits. ❑ Les autres peuvent être refusés, réduits ou transférés.
Validation du traitement des risques	❑ Le traitement des risques ne peut être validé que s'il est démontré que les risques résiduels sont acceptables et que les mesures de sécurité destinées à traiter les risques peuvent être mises en œuvre dans un délai raisonnable.

Les biens identifiés

Biens essentiels

Chaque métier sélectionné précédemment dans l'étude est lié à plusieurs processus. Ces processus sont des fonctions qui traitent des informations essentielles en entrée et en sortie.

Dans le cadre du sujet d'étude, les informations et fonctions suivantes ont été retenues en tant que biens essentiels :

Services	Informations concernées
	❑
	❑
	❑
	❑
	❑
	❑
	❑

Biens supports

Le schéma suivant présente les biens supports identifiés pour le sujet de l'étude :

Figure 1 - Schéma des biens supports

Note : les types de biens supports, sur lesquels ces biens essentiels reposent, sont les suivants :

- ❑ les locaux (LOC), qui hébergent/abritent/contiennent des :
  - ○ organisations (ORG), qui peuvent être décomposées en :
    - ▪ personnes (PER),
    - ▪ supports papier (SUP)
    - ▪ canaux interpersonnels (CAN) ;
  - ○ systèmes informatiques et de téléphonie (SYS), qui peuvent être décomposés en :
    - ▪ matériels (MAT),
      - • logiciels (LOG),
    - ▪ canaux informatique et de téléphonie (RSX)
- ❑ Etc …

Liens entre les biens essentiels et les biens supports

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Type	Biens essentiels			
Biens supports	**Image**	**Voix**	**Signalisation**	**Numéro de visioconférence**

Mesures de sécurité déjà mis en place sur les biens supports

Il a été recensé les mesures de sécurité existantes suivantes, bien support par bien support :

Biens supports	Image	Voix	Signalisation	Numéro de visioconférence	Mesures de sécurité portées par les biens supports
				❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑ ❑	

Étude des événements redoutés

Événements redoutés

Chaque ligne du tableau suivant représente un événement redouté (bien essentiel, critère de sécurité, besoin de sécurité selon les échelles de besoin, sources de menaces et impacts).

La gravité de chaque évènement redouté est estimée en ne tenant pas compte des mesures de sécurité existantes (cf. échelles de gravité).

Événement redouté	Besoin de sécurité	Impacts	Sources de menaces	Gravité
		✓	✓	
		✓	✓	
		✓	✓	

Évaluation des événements

L'importance relative des événements redoutés précédemment analysés (identifiés et estimés) est évaluée à l'aide du tableau suivant (cf. critères de gestion des risques) :

Critique	✓
Importante	✓
Limitée	✓
Négligeable	✓

Étude des scénarios de menaces / menaces

Scénarios de menaces

Les pages suivantes présentent les scénarios de menaces potentiellement réalisables dans le cadre du sujet de l'étude. Les sources de menaces susceptibles d'en être à l'origine sont identifiées et la vraisemblance de chaque scénario de menace est estimée (cf. échelle de vraisemblance). Le détail des scénarios de menaces est présenté en annexe (bien support, critère de sécurité, sources de menaces, menaces, vulnérabilités et pré-requis).

Scénarii de menaces	Sources de menaces	Vraisemblance
	✓	
	✓	
	✓	

Évaluation des scénarios de menaces

L'importance relative des scénarios de menaces précédemment analysés (identifiés et estimés) est évaluée de la façon suivante (cf. critères de gestion des risques) :

4. Maximale	✓
3. Forte	✓
2. Significative	✓
1. Minime	✓

Étude des risques

Les risques

La liste des risques a été établie à partir des événements redoutés et des scénarios de menaces précédemment appréciés.

Les mesures de sécurité existantes, ayant un effet sur chaque risque, ont également été identifiées.
La gravité et la vraisemblance ont finalement été estimées, sans, puis avec, les mesures de sécurité (les niveaux sur fond gris correspondent aux valeurs avant application de ces mesures).

Risque XXX

	0	1	2	3	4
Gravité		**Négligeable**	Limitée	Importante	Critique
Vraisemblance		Minime	**Significative**	Forte	Maximale

Impacts :

- ❑

Scénarii de menaces :

Scénarii de menaces	Sources de menaces	Vraisemblance
	✓	
	✓	
	✓	
	✓	

Mesures existantes :

Mesures de sécurité	Biens supports	Prévention	Protection	Récupération

Justification de la ré-estimation :

Évaluation des risques :

Hiérarchie des risques avant application des mesures de sécurité existantes

	Risques	Gravité estimée	Vraisemblance estimée
1			

Hiérarchie des risques après application des mesures de sécurité existantes

	Risques	Gravité estimée	Vraisemblance estimée
1			

Les objectifs de sécurité :

Le tableau suivant présente les objectifs de sécurité retenus :

Risque	Évitement	Réduction	Prise	Transfert
1				

Étude des mesures de sécurité

Les mesures de sécurité : une défense en profondeur pour réduire les risques

Le tableau suivant présente la liste des mesures de sécurité destinées à réduire les risques :

Mesures de sécurité	Biens supports	Risque XXX	Risque XXX	ISO 27001	Prévention	Protection	Récupération

Risques résiduels

Si les mesures de sécurité précédemment identifiées sont mises en œuvre, alors le niveau des risques jugés comme intolérables ou significatifs peut être ré-estimé comme suit :

Risque XXX

	0	1	2	3	4
Gravité		**Négligeable**	**Limitée**	Importante	Critique
Vraisemblance		Minime	**Significative**	**Forte**	**Maximale**

En synthèse, les risques résiduels sont donc les suivants :

Risques résiduels	Gravité	Vraisemblance

Plan d’action

Les échelles de valeurs suivantes ont été utilisées pour élaborer le plan d'action :

Difficulté	Coût financier	Échéance	Avancement
1. Faible	1. Nul	1. Trimestre	1. Non démarré
2. Moyenne	2. Moins de 1000€	2. Année	2. En cours
3. Élevée	3. Plus de 1000€	3. 3 ans	3. Terminé

Le plan d'action est établi comme suit :

Mesure de sécurité	Responsable	Difficulté	Coût financier	Échéance	Avancement
Mesures du trimestre					

Homologation de sécurité

2 Livrables émanant de l’étude EBIOS

Fiche d’expression rationnelle des objectifs de sécurité (FEROS)

[Synthèse de l’étude EBIOS (quelques pages) jusqu’au niveau des objectifs de sécurité]

Politique de sécurité (PSSI)

[Organisation des mesures de sécurité de l’étude EBIOS sur la base des chapitres de l’ISO 27002]

Dossier des risques résiduels

[Émane de l’étude EBIOS]

Décision d’homologation

[Acceptation formelle des risques résiduels]

3 Annexe : liste détaillée des scénarii de menaces