
phosforea
my learning experience

# Introduction à la méthode EBIOS

EBIOS
Expression des Besoins et Identification des Objectifs de Sécurité

phosforea
my learning experience

# Objectif du cours

Etre capable de mener une analyse de risque et de définir un plan de traitement des risques.

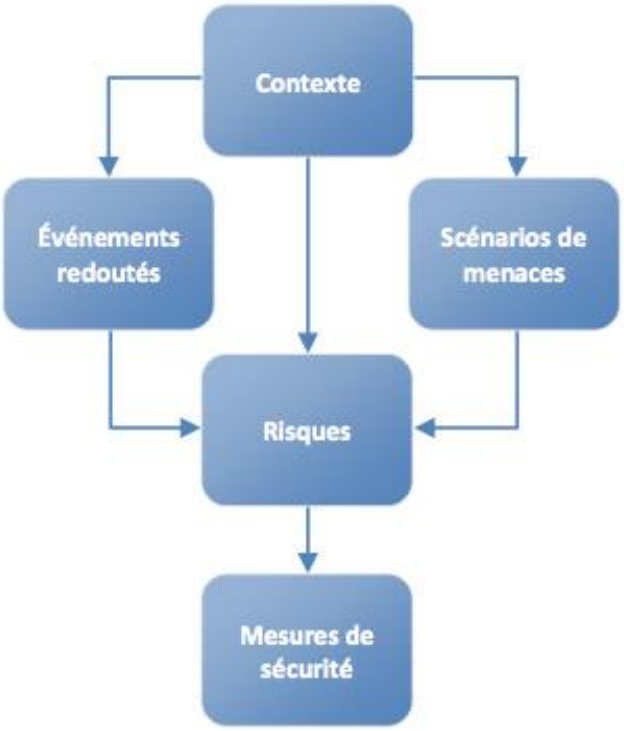
phosforea
my learning experience

# Introduction

- La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est un outil complet de gestion des risques SSI conforme au RGS et aux dernières normes ISO 27001, 27005 et 31000
- Elle a été créée en 1995 par l'ANSSI et elle est régulièrement mise à jour.
- Elle est assortie d'une base de connaissances cohérente avec le Référentiel Général de Sécurité et enrichie d'exemples  concrets permettant d'élaborer des scénarios de risque pertinents pour votre organisation.

# Principes généraux

- EBIOS est une démarche itérative en 5 modules permettant de répondre à 10 questions essentielles en gestion de risque




| | |
|---|---|
| **Contexte** | •Pourquoi et comment va-t-on gérer les risques ?<br>•Quel est le sujet de l'étude ? |
| **Evénements redoutés** | •Quels sont tous les événements craints ?<br>•Quels seraient les plus graves ? |
| **Scénarios de menaces** | •Quels sont tous les scénarios possibles ?<br>•Quels sont les plus vraisemblables ? |
| **Risques** | •Quelle est la cartographie des risques ?<br>•Comment choisit-on de les traiter ? |
| **Mesures de sécurité** | •Quelles mesures devrait-on appliquer ?<br>•Les risques résiduels sont-ils acceptables ? |

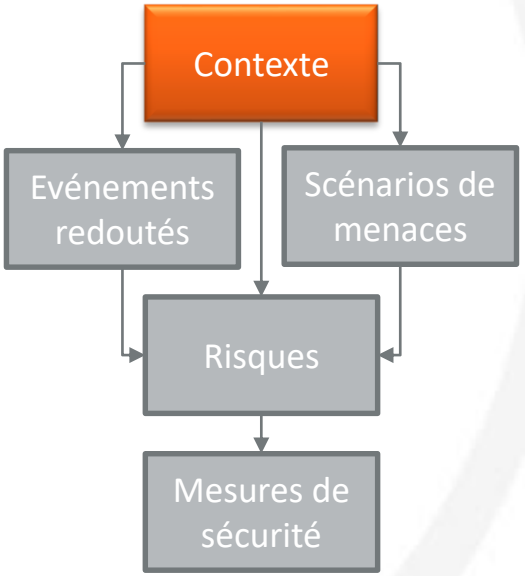
# Etude du contexte

phosforea
my learning experience

# Etude du contexte

Actions :

- Cadrer l'étude des risques
- Décrire le contexte général
- Délimiter le périmètre de l'étude
- Identifier les paramètres à prendre en compte
- Identifier les sources de menaces



# Etude du contexte

| | |
|---|---|
| Cadrer l'étude des risques | ▪ Qu'est-ce qui est à l'origine de l'étude (motif, événement…) ?<br>▪ Quel est l'objectif de l'étude (son but et les livrables attendus) ?<br>▪ Comment organiser le travail (actions, rôles, charges…) ? |
| Décrire le contexte général | ▪ Que sait-on du contexte (externe et interne) ?<br>▪ Comment les risques sont-ils gérés actuellement ? |
| Délimiter le périmètre de l'étude | ▪ Quelles sont les limites du périmètre étudié ?<br>▪ Qui doit participer à l'étude ? |
| Identifier les paramètres à prendre en compte | ▪ Quels sont les référentiels applicables ?<br>▪ Quelles sont les contraintes qui pourraient impacter l'étude ? |
| Identifier les sources de menaces | ▪ Contre quels types de sources de menaces décide-t-on de se protéger ?<br>▪ Quels sont les exemples illustratifs ? |

# Etude du contexte

- Les livrables attendus :
  1. Une proposition de métriques à valider
     - Besoins DIC, gravité, vraisemblance et critères de gestion des risques

*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. |

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

| Niveaux de l'échelle | Description détaillée de l'échelle |
|---|---|
| Plus de 72h | Le bien essentiel peut être indisponible plus de 72 heures. |
| Entre 24 et 72h | Le bien essentiel doit être disponible dans les 72 heures. |
| Entre 4 et 24h | Le bien essentiel doit être disponible dans les 24 heures. |
| Moins de 4h | Le bien essentiel doit être disponible dans les 4 heures. |

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

| Niveaux de l'échelle | Description détaillée de l'échelle |
|---|---|
| Détectable | Le bien essentiel peut ne pas être intègre si l'altération est identifiée. |
| Maîtrisé | Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée. |
| Intègre | Le bien essentiel doit être rigoureusement intègre. |

*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. |
| Limité | Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires. |
| Réservé | Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées. |
| Privé | Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître. |

*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 | @RCHIMED surmontera les impacts sans aucune difficulté. |
| 2. Limitée | @RCHIMED surmontera les impacts malgré quelques difficultés. |
| 3. Importante | @RCHIMED surmontera les impacts avec de sérieuses difficultés. |
| 4. Critique | @RCHIMED ne surmontera pas les impacts (sa survie est menacée). |

*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 devrait pas se (re)produire. |
| 2. Significative | Cela pourrait se (re)produire. |
| 3. Forte | Cela devrait se (re)produire un jour ou l'autre. |
| 4. Maximale | Cela va certainement se (re)produire prochainement. |

*Les critères de gestion des risques retenus sont les suivants :*

| Action | Critère de gestion des risques (règle choisie pour réaliser l'action) |
|---|---|
| Estimation des événements redoutés (module 2) | ❑ Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet. |
| Évaluation des événements redoutés (module 2) | ❑ Les événements redoutés sont classés par ordre décroissant de vraisemblance. |
| Estimation des risques (module 4) | ❑ La gravité d'un risque est égale à celle de l'événement redouté considéré.<br>❑ 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 (module 4) | ❑ Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme intolérables.<br>❑ Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale, sont jugés comme significatifs.<br>❑ Les autres risques sont jugés comme négligeables. |
| … | ❑ … |

# Etude du contexte

- Les livrables attendus :
  2. Les comptes rendus d'interviews
     - Le contexte général
     - Les mesures de sécurité existantes
     - Les vulnérabilités et/ou menaces existantes
     - Les incidents passés
     - Les constats de visites de sites
     - …

# Etude du contexte

- Les livrables attendus :
  3. L'inventaire des biens essentiels et support en regard du périmètre d'application.

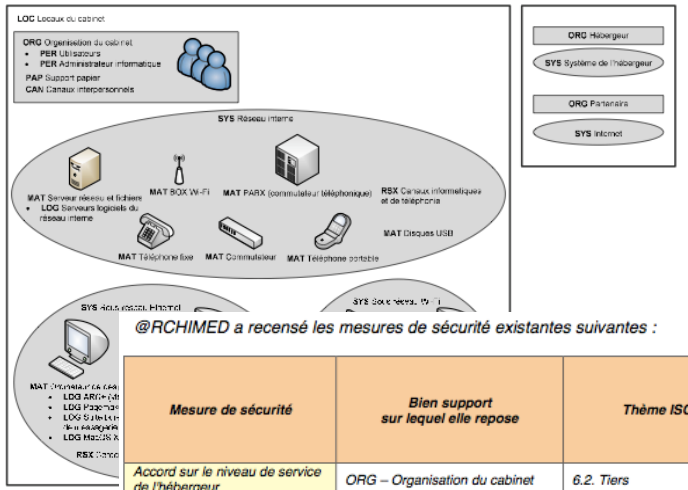
*Dans le cadre du sujet d'étude, le cabinet @RCHIMED a retenu les processus suivants en tant que biens essentiels :*

| Processus essentiels | Informations essentielles concernées | Dépositaires |
|---|---|---|
| *Établir les devis (estimation du coût global d'un projet, négociations avec les clients…)* | ✓ Cahier des charges<br>✓ Catalogues techniques<br>✓ Contrat (demande de réalisation)<br>✓ Devis | *Service commercial* |
| *Créer des plans et calculer les structures* | ✓ Dossier technique d'un projet<br>✓ Paramètres techniques (pour les calculs de structure)<br>✓ Plan technique<br>✓ Résultat de calcul de structure | *Bureau d'études* |
| *Créer des visualisations* | | |
| *Gérer le contenu du site* | | |

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

| Biens supports / Biens essentiels | Établir les devis | Créer des plans et calculer les structures | Créer des visualisations | Gérer le contenu du site Internet |
|---|---|---|---|---|
| *Biens supports communs à @RCHIMED* | | | | |
| *SYS – Réseau interne* | X | X | X | X |
| *MAT – Serveur réseau et fichiers* | X | X | X | X |
| *LOG – Serveurs logiciels du réseau interne* | | X | X | |
| *MAT – Disque USB* | X | X | X | |
| *MAT – BOX Wifi* | X | X | X | X |
| *MAT – Commutateur* | X | X | X | X |
| *MAT – PABX (commutateur téléphonique)* | X | X | X | X |
| *MAT – Téléphone fixe* | X | X | X | X |
| *MAT – Téléphone portable* | X | X | X | X |
| *RSX – Canaux informatiques et de téléphonie* | X | X | X | X |
| *ORG – Organisation du cabinet* | X | X | X | X |
| *PER – Utilisateur* | X | X | X | |

*Le schéma suivant décompose ces biens supports et les positionne les uns par rapport aux autres :*




*@RCHIMED a recensé les mesures de sécurité existantes suivantes :*

| Mesure de sécurité | Bien support sur lequel elle repose | Thème ISO 27002 | Prévention | Protection | Récupération |
|---|---|---|---|---|---|
| *Accord sur le niveau de service de l'hébergeur* | *ORG – Organisation du cabinet* | *6.2. Tiers* | X | | X |
| *Activation d'une alarme anti-intrusion durant les heures de fermeture* | *LOC – Locaux du cabinet* | *9.1. Zones sécurisées* | X | | |
| *Consignes de fermeture à clef des locaux* | *LOC – Locaux du cabinet* | *9.1. Zones sécurisées* | | X | |
| *Dispositifs de lutte contre l'incendie* | *LOC – Locaux du cabinet* | *9.1. Zones sécurisées* | | X | |
| *Climatisation* | *LOC – Locaux du cabinet* | *9.2. Sécurité du matériel* | X | | |
| *Contrat de maintenance informatique (intervention sous 4h)* | *ORG – Organisation du cabinet* | *9.2. Sécurité du matériel* | X | | X |
| *Alimentation secourue* | *MAT – Serveur réseau et fichiers* | *9.2. Sécurité du matériel* | | X | |
| *Installation d'un antivirus sous Windows XP* | *LOG – Windows XP* | *10.4. Protection contre les codes malveillant et mobile* | | X | |
| *Sauvegarde hebdomadaire sur* | | | | | |

# Etude du contexte

- Les livrables attendus :
  4. Un planning de réalisation
     - L'organisation projet
     - Les échéances
     - Les risques projets

# Cas pratique

- Quelles sont les actions que vous feriez pour réaliser l'étude de contexte ?

*Le formateur joue le rôle du client et attend de vous que vous lui présentiez votre méthodologie de réalisation de la phase d'étude du contexte.*

phosforea
my learning experience

# Etude du contexte : Synthèse

- Les actions à entreprendre
  1. Reprise des informations des cahiers des charges
  2. Analyse de la documentation : organigramme, compte rendus de COPIL, charte, politiques, doc technique, …
  3. Planifier et mener des interviews
  4. Visiter le ou les sites
  5. Et parfois, mener des audits techniques

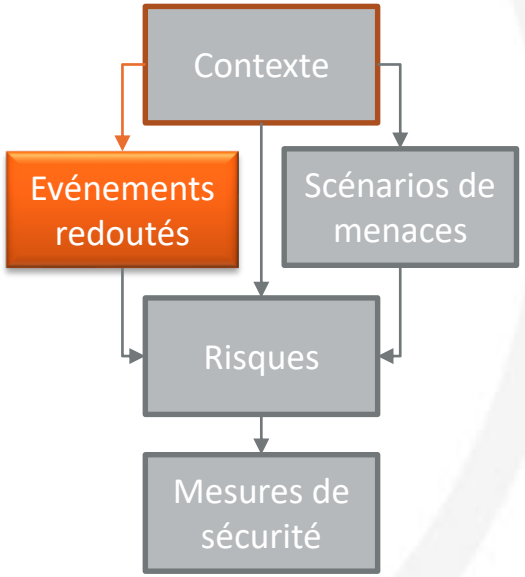
phosforea
my learning experience

# Evénements redoutés

# Evénements redoutés

Actions:

- Analyser les événements redoutés
- Evaluer les événements redoutés




phosforea
my learning experience

# Evénements redoutés

**Analyser tous les événements redoutés**

- Quels sont les besoins de sécurité de chaque bien essentiel ?
- Quelles sources de menaces peuvent les affecter ?
- Quels seraient les impacts si l'événement se produisait ?
- Quelle serait la gravité d'un tel événement ?

**Évaluer chaque Événement redouté**

- Quelle est la hiérarchie des événements redoutés identifiés ?

# Evénements redoutés

- Les livrables attendus :

*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) :*

| Gravité | Événements redoutés |
|---|---|
| 4. Critique | ✓ Altération de plans ou de calculs de structures |
| 3. Importante | ✓ Altération de devis<br>✓ Compromission de plans ou calculs de structures<br>✓ Compromission de devis<br>✓ Altération du contenu du site Internet |
| 2. Limitée | ✓ Indisponibilité de devis<br>✓ Indisponibilité de visualisations<br>✓ Altération de visualisations<br>✓ Indisponibilité de plans ou de calculs de structures<br>✓ Indisponibilité du site Internet |
| 1. Négligeable | ✓ Compromission de visualisations<br>✓ Compromission du contenu du site Internet |

*Chaque ligne du tableau suivant représente un événement redouté par le cabinet @RCHIMED (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 (cf. échelle de gravité) sans tenir compte des mesures de sécurité existantes.*

| Événement redouté | Besoin de sécurité | Sources de menaces | Impacts | Gravité |
|---|---|---|---|---|
| Établir les devis | | | | |
| Indisponibilité de devis | 24-72h | ✓ Employé peu sérieux<br>✓ Incendie des locaux<br>✓ Panne électrique | ✓ Impossibilité de signer un contrat<br>✓ Perte d'un marché<br>✓ Perte de crédibilité | 2. Limitée |
| Altération de devis | Intégre | ✓ Employé peu sérieux | ✓ Impossibilité de signer un contrat<br>✓ Perte d'un marché<br>✓ Impossibilité de remplir les obligations légales<br>✓ Perte de crédibilité | 3. Importante |
| Compromission de devis | Limité | ✓ Employé peu sérieux<br>✓ Concurrent | ✓ Perte d'un marché<br>✓ Action en justice à l'encontre du cabinet<br>✓ Perte de crédibilité | 3. Importante |
| Créer des plans et calculer les structures | | | | |
| Indisponibilité de plans ou de calculs de structures | 24-72h | ✓ Employé peu sérieux<br>✓ Virus non ciblé<br>✓ Personnel de nettoyage (soudoyé)<br>✓ Personnels de maintenance<br>✓ Panne électrique | ✓ Perte de crédibilité | 2. Limitée |

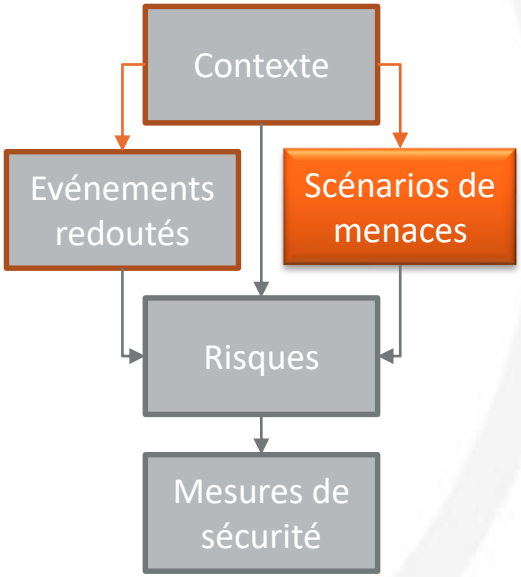
phosforea
my learning experience

# Scénarios de menaces

# Scénarios de menaces

Actions

- Analyser tous les scénarios de menaces
- Évaluer chaque scénario de menace



# Scénarios de menaces

**Analyser tous les scénarios de menaces**

- Quelles menaces peuvent s'exercer sur chaque bien support ?
- Quelles sources de menaces peuvent en être à l'origine ?
- Quelles sont les vulnérabilités potentiellement utilisables ?
- Y a-t-il des pré-requis pour que la menace se réalise ?
- Quelle est la vraisemblance des scénarios ?

**Évaluer chaque scénario de menace**

- Quelle est la hiérarchie des scénarios de menaces identifiés ?

# Scénarios de menaces

- Les livrables attendus :

*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 (menaces, vulnérabilités et pré-requis) est décrit dans les bases de connaissances de la méthode EBIOS.*

| Scénarios de menaces | Sources de menaces | Vraisemblance |
|---|---|---|
| SYS – Réseau interne | | |
| Menaces sur le réseau interne causant une indisponibilité | ✓ Employé peu sérieux<br>✓ Maintenance informatique<br>✓ Script-kiddies<br>✓ Virus non ciblé<br>✓ Incendie des locaux<br>✓ Panne électrique<br>✓ Phénomène naturel (foudre, usure…) | 3. Forte |
| Menaces sur le réseau interne causant une altération | ✓ Employé peu sérieux<br>✓ Maintenance informatique<br>✓ Script-kiddies<br>✓ Virus non ciblé | 2. Significative |
| Menaces sur le réseau interne causant une compromission | ✓ Employé peu sérieux<br>✓ Maintenance informatique<br>✓ Script-kiddies | 2. Significative |
| SYS – Sous réseau Ethernet | | |
| Menaces sur le sous réseau Ethernet causant une indisponibilité | ✓ Employé peu sérieux<br>✓ Maintenance informatique<br>✓ Script-kiddies<br>✓ Virus non ciblé<br>✓ Incendie des locaux<br>✓ Panne électrique<br>✓ Phénomène naturel (foudre, usure…) | 3. Forte |

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

| Vraisemblance | Scénarios de menaces |
|---|---|
| 4. Maximale | ✓ Menaces sur l'organisation d'@RCHIMED causant une compromission<br>✓ Menaces sur le système de l'hébergeur causant une indisponibilité<br>✓ Menaces sur le système de l'hébergeur causant une compromission<br>✓ Menaces sur un partenaire causant une compromission |
| 3. Forte | ✓ Menaces sur le réseau interne causant une indisponibilité<br>✓ Menaces sur le sous réseau Ethernet causant une indisponibilité<br>✓ Menaces sur le sous réseau Wifi causant une indisponibilité<br>✓ Menaces sur le sous réseau Wifi causant une altération<br>✓ Menaces sur le sous réseau Wifi causant une compromission<br>✓ Menaces sur le système de l'hébergeur causant une altération<br>✓ Menaces sur un partenaire causant une indisponibilité |

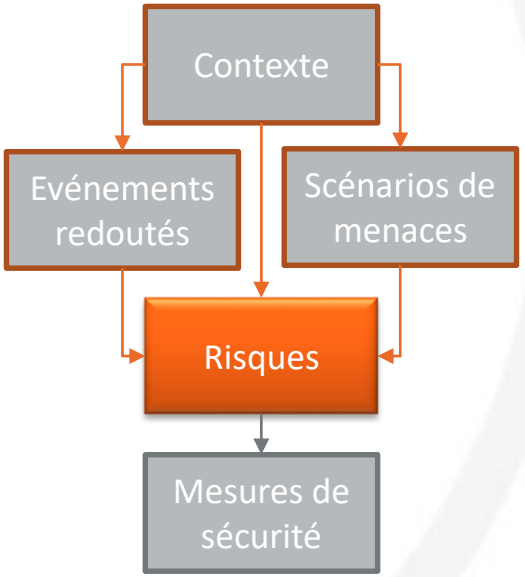
# Etude des risques

phosforea
my learning experience

# Etude des risques

Actions :

- Analyser les risques
- Evaluer les risques
- Identifier les objectifs de sécurité



# Etude des risques

| | |
|---|---|
| **Analyser les risques** | ▪ Quels scénarios s'appliquent aux événements redoutés ?<br>▪ Y a-t-il des mesures existantes pour traiter ces risques ?<br>▪ Quelle est la gravité des risques ?<br>▪ Quelle est la vraisemblance des risques ? |
| **Évaluer les risques** | ▪ Quelle est la hiérarchie des risques identifiés ? |
| **Identifier les obj. de sécurité** | ▪ Comment choisit-on de traiter chaque risque (réduire, transférer, éviter, prendre) ? |

# Etude des risques

- Analyser les risques
  - Mettre en évidence l'ensemble des risques qui pèsent réellement sur le périmètre de l'étude et déterminer leur gravité et leur vraisemblance :
    - Une première fois sans tenir compte des mesures de sécurité existantes : risque brut
    - Une seconde fois en les prenant en compte : risque actuel
  - Faire le lien entre les événements redoutés et les scénarios de menaces, c'est-à-dire entre ce que l'organisme craint et ce à quoi il est exposé

# Etude des risques

- Evaluer les risques
  - En regard des critères de gestion des risques

*Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :*

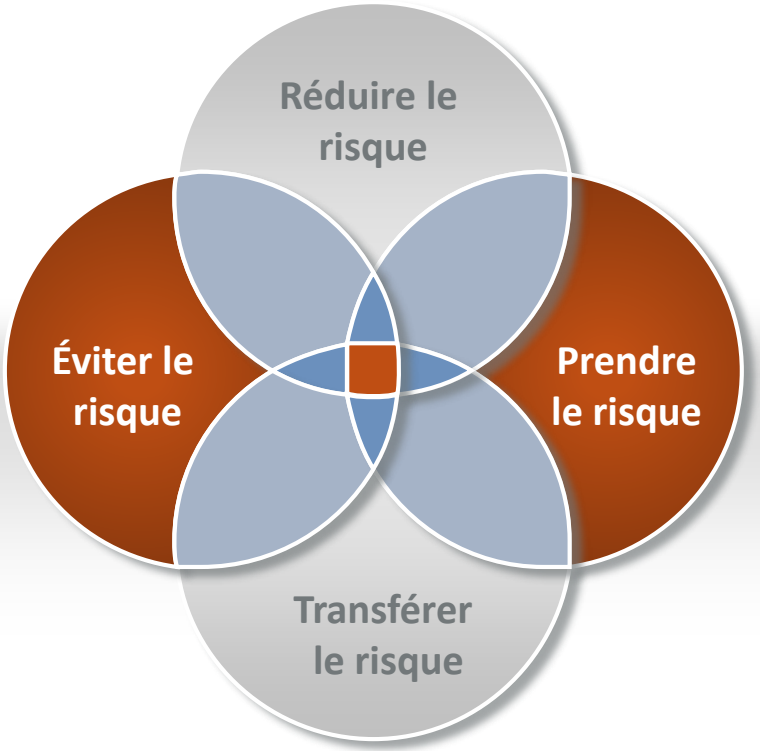
| Gravité | | | | | |
|---|---|---|---|---|---|
| | 4. Critique | | Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intégres | | |
| | 3. Importante | | Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver | Risque lié à l'altération d'un devis qui doit rester rigoureusement intégre<br>~~Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver~~ | Risque lié à la compromission d'un devis au-delà du personnel et des partenaires<br>Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires |
| | 2. Limitée | | Risque lié à l'indisponibilité d'un devis au-delà de 72h<br>Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h<br>Risque lié à l'indisponibilité de visualisations au-delà de 72h<br>Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h | ~~Risque lié à l'indisponibilité d'un devis au-delà de 72h~~<br>~~Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h~~<br>~~Risque lié à l'indisponibilité de visualisations au-delà de 72h~~<br>Risque lié à l'altération de visualisations sans pouvoir la détecter | ~~Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h~~ |
| | 1. Négligeable | | | | Risque lié à la compromission de visualisations, jugées comme publiques<br>Risque lié à la compromission du contenu du site Internet public |
| | | 1. Minime | 2. Significative | 3. Forte | 4. Maximale |
| | | Vraisemblance | | | |

Risques négligeables | Risques significatifs | Risques intolérables

phosforea
my learning experience

# Etude des risques

- Identifier les objectifs de sécurité




**Éviter (ou refuser) le risque**

Changer le contexte de telle sorte qu'on n'y soit plus exposé

**Réduire le risque**

Prendre des mesures de sécurité pour diminuer l'impact et/ou la vraisemblance

**Prendre (ou maintenir) le risque**

Assumer les conséquences sans prendre de mesure de sécurité supplémentaire

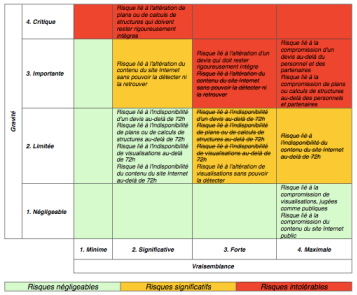
**Transférer (ou partager) le risque**

Partager les pertes occasionnées par un sinistre ou faire assumer la responsabilité à un(des) tiers

# Etude des risques

- Livrables attendus :

*Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :*




*Le tableau suivant présente les objectifs de sécurité identifiés (les croix correspondent aux premiers choix, les croix entre parenthèses correspondent aux autres possibilités acceptées) :*

| Risque | Évitement | Réduction | Prise | Transfert |
|---|---|---|---|---|
| Risque lié à l'indisponibilité d'un devis au-delà de 72h | | (X) | X | |
| Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre | (X) | X | X | (X) |
| Risque lié à la compromission d'un devis au-delà du personnel et des partenaires | (X) | X | X | (X) |
| Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h | | (X) | X | |
| Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres | (X) | X | X | (X) |
| Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires | (X) | X | X | (X) |
| Risque lié à l'indisponibilité de visualisations au-delà de 72h | | (X) | X | |

*@RCHIMED a établi la liste des risques 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 rayés correspondent aux valeurs avant application de ces mesures).*

*Risque lié à l'indisponibilité d'un devis au-delà de 72h*

| Événement redouté | Besoin de sécurité | Sources de menaces | Impacts | Gravité |
|---|---|---|---|---|
| Indisponibilité de devis | 24-72h | ✓ Employé peu sérieux<br>✓ Incendie des locaux<br>✓ Panne électrique | ✓ Impossibilité de signer un contrat<br>✓ Perte d'un marché<br>✓ Perte de crédibilité | 2. Limitée |

| Scénarios de menaces | Sources de menaces | Vraisemblance |
|---|---|---|
| Menaces sur le réseau interne causant une indisponibilité | ✓ Employé peu sérieux<br>✓ Maintenance informatique<br>✓ Script-kiddies<br>✓ Virus non ciblé<br>✓ Incendie des locaux<br>✓ Panne électrique<br>✓ Phénomène naturel (foudre, usure…) | 3. Forte |
| Menaces sur le sous réseau Wifi causant une indisponibilité | ✓ Employé peu sérieux<br>✓ Maintenance informatique<br>✓ Script-kiddies<br>✓ Virus non ciblé<br>✓ Incendie des locaux<br>✓ Panne électrique<br>✓ Phénomène naturel (foudre, usure…) | 3. Forte |
| Menaces sur l'organisation d'@RCHIMED causant une indisponibilité | ✓ Employé peu sérieux<br>✓ Personnel de nettoyage<br>✓ Maladie | 2. Significative |
| Menaces sur Internet causant une indisponibilité | ✓ Fournisseur d'accès Internet | 2. Significative |
| Menaces sur un partenaire causant une indisponibilité | ✓ Partenaire | 3. Forte |

| Mesure de sécurité existante | Bien support sur lequel elle repose | Prévention | Protection | Récupération |
|---|---|---|---|---|
| Activation du WPA2 | MAT – Commutateur | X | | |
| Assurance multirisque professionnelle et sur les matériels informatiques | ORG – Organisation du cabinet | | | X |
| Climatisation | LOC – Locaux du cabinet | X | | |
| Contrat de maintenance informatique (intervention sous 4h) | ORG – Organisation du cabinet | X | | X |
| Contrôle d'accès par mot de passe | LOG – Windows XP | X | | |
| Dispositifs de lutte contre l'incendie | LOC – Locaux du cabinet | | X | |
| Installation d'un antivirus | LOG – Windows XP | | X | |
| Alimentation secourue | MAT – Serveur réseau et fichiers | | X | |
| Accès restreint en entrée (messagerie, services WEB…) | MAT – Commutateur | X | | |
| Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef | MAT – Disque USB | | | X |

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | 1. Négligeable | **2. Limitée** | 3. Importante | 4. Critique |
| Vraisemblance | 1. Minime | **2. Significative** | 3. Forte | 4. Maximale |

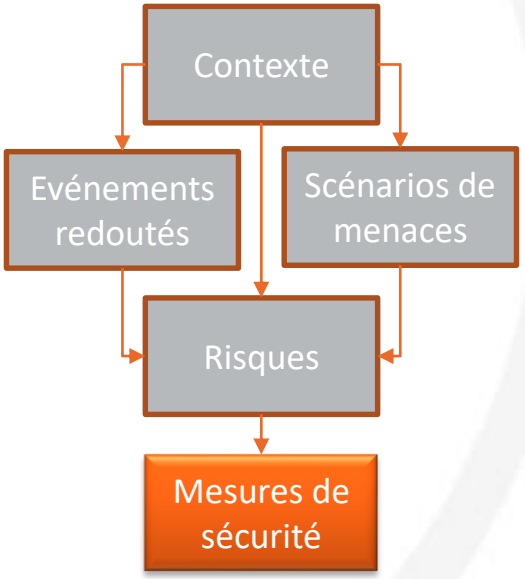
# Etude des mesures de sécurité

phosforea
my learning experience

# Etude des mesures de sécurité

Actions :

- Déterminer les mesures de sécurité
- Analyser les risques résiduels
- Établir une déclaration d'applicabilité



# Etude des mesures de sécurité

| | |
|---|---|
| **Déterminer les mesures de sécurité** | ▪ Quelles mesures doivent être mise en place ?<br>▪ Servent-elles à la prévention, la protection, ou à la récupération ?<br>▪ Sur quels biens supports reposent-elles ? |
| **Analyser les risques résiduels** | ▪ Quelles sont les nouvelles valeurs de gravité et vraisemblance ?<br>▪ Quels sont les scénarios toujours possibles ? |
| **Établir une déclaration d'applicabilité** | ▪ Les paramètres à prendre en compte ont-ils été bien traités ? |

# Etude des mesures de sécurité

- Déterminer les mesures de sécurité
  - Protectrice : bloquer, contenir et détecter l'apparition des incidents et des sinistres à l'aide de mesures de sécurité
  - Préventive : éviter l'apparition des incidents et des sinistres à l'aide de mesures de sécurité
  - Récupératrice : minimiser les conséquences des incidents et des sinistres et revenir à l'état initial, à l'aide de mesures de sécurité

➢ Guide pour la défense en profondeur

# Etude des mesures de sécurité

- Analyser les risques résiduels, pour chaque objectif de sécurité :
  - Réaliser un argumentaire justificatif, qui devrait démontrer que :
    - la combinaison des mesures de sécurité traite le risque conformément à l'objectif de sécurité identifié
    - l'ensemble des mesures de sécurité constitue un tout cohérent et dont les éléments se soutiennent mutuellement
    - le niveau de résistance des mesures de sécurité choisi est cohérent avec les sources de menaces retenues
  - Compléter la liste des risques résiduels au regard des mesures de sécurité identifiées et les estimer en termes de gravité et de vraisemblance
  - Estimer l'effet des mesures de sécurité sur la gravité et la vraisemblance du risque concerné en les ré-estimant

# Etude des mesures de sécurité

- Établir dossier de sécurité
  - expliquer comment les paramètres à prendre en compte (références applicables, contraintes et hypothèses) ont été pris en compte au sein de l'étude
  - justifier le fait de ne pas en avoir tenu compte, le cas échéant

# Etude des mesures de sécurité

- Livrables attendus :

*Le plan d'action d'@RCHIMED, trié par terme, avancement et coût financier, est établi comme suit :*

| Mesure de sécurité | Responsable | Difficulté | Coût financier | Terme | Avancement |
|---|---|---|---|---|---|
| Mesures du trimestre | | | | | |
| Activation d'une alarme anti-intrusion durant les heures de fermeture | Directeur | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Consignes de fermeture à clef des locaux | Directeur | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Dispositifs de lutte contre l'incendie | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Climatisation | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Contrôle d'accès par mot de passe sous MacOS X | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Contrôle d'accès par mot de passe sous Windows XP | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Accès restreint en entrée (messagerie, services WEB...) | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Activation du WPA2 | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Sauvegarde hebdomadaire sur des disques USB stockés dans un meuble fermant à clef | Directeur adjoint | 1. Faible | 1. Nul | 1. Trimestre | 3. Terminé |
| Installation d'un antivirus sous MacOS X | Directeur adjoint | 1. Faible | 2. Moins de 1000€ | 1. Trimestre | 3. Terminé |
| Installation d'un antivirus sous Windows XP | Directeur adjoint | 1. Faible | 2. Moins de 1000€ | 1. Trimestre | 3. Terminé |

*Le tableau suivant présente la liste des mesures de sécurité destinées à réduire ou transférer les risques prioritaires (elles traitent également les autres risques) :*

| Mesure de sécurité | R1 | R2 | R3 | R4 | R5 | R6 | Bien support sur lequel elle repose | Thème ISO 27002 | Prévention | Protection | Récupération |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques | | | | X | | | LOG – MacOS X | 7.1. Responsabilités relatives aux biens | | X | |
| Désactivation des composants inutiles sur le serveur | X | X | X | X | X | X | | | | | |
| Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures | X | | X | | X | X | | | | | |
| Accès restreint en entrée (messagerie, services WEB...) | X | X | X | X | X | X | | | | | |
| Rangement des supports amovibles dans un meuble fermant à clef | | X | | X | | | | | | | |

*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 lié à l'altération d'un devis qui doit rester rigoureusement intègre*

| Niveau de risque | | | | |
|---|---|---|---|---|
| Gravité | 1. Négligeable | 2. Limitée | **3. Importante** | 4. Critique |
| Vraisemblance | **1. Minime** | ~~2. Significative~~ | ~~3. Forte~~ | 4. Maximale |

*Risque lié à la compromission d'un devis au-delà du p*

| Niveau de risque | | |
|---|---|---|
| Gravité | 1. Négligeable | **2. Limitée** |
| Vraisemblance | 1. Minime | **2. Significative** |

*La prise en compte de chaque contrainte identifiée est explicitée comme suit :*

| Paramètre à prendre en compte | Explication / Justification |
|---|---|
| Le personnel est utilisateur de l'informatique, mais pas spécialiste | **Pris en compte** Les mesures de sécurité applicables par le personnel ne demandent pas une grande expertise |
| Le personnel de nettoyage intervient de 7h à 8h | **Non pris en compte** Les horaires doivent correspondrent à ceux du personnel |
| Aucun déménagement n'est planifié | **Pris en compte** Les mesures de sécurité formalisées ne demandent pas de déménagement |
| ... | ... |

# Plus d’informations

phosforea
my learning experience

# Outillage / Références

- Les différents documents relatifs à la méthode EBIOS (guide méthodologique, étude de cas, base de connaissance…) sont disponibles à l'adresse suivante :
  - http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

- Un logiciel permettant l'enregistrement de toutes les données d'analyse de risque est également disponible :
  - https://adullact.net/projects/ebios2010/

# Fin du module

Ce module est à présent terminé, vous pouvez retourner sur votre tableau de bord.

phosforea
my learning experience