# Management du Risque

Sécurité des Systèmes d'information
Concepts, Organisation, outils et Tendance

CPE LYON
ÉCOLE SUPÉRIEURE DE CHIMIE PHYSIQUE ÉLECTRONIQUE DE LYON

# Plan

- Introduction
- Méthode de mangement du risque: EBIOS
- Méthode de gouvernance des SI: COBIT

# Qu'est ce que le management de risque ?

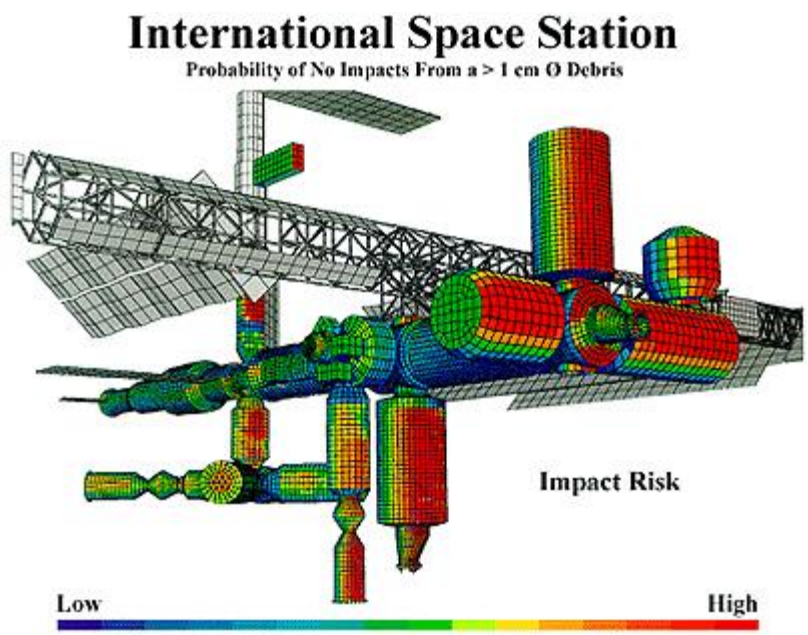
# Qu'est ce qu'un risque ?

- Un risque est un danger auquel est exposée une entreprise, une institution, plus ou moins probable, directement liée à la nature de l'activité de l'entreprise.

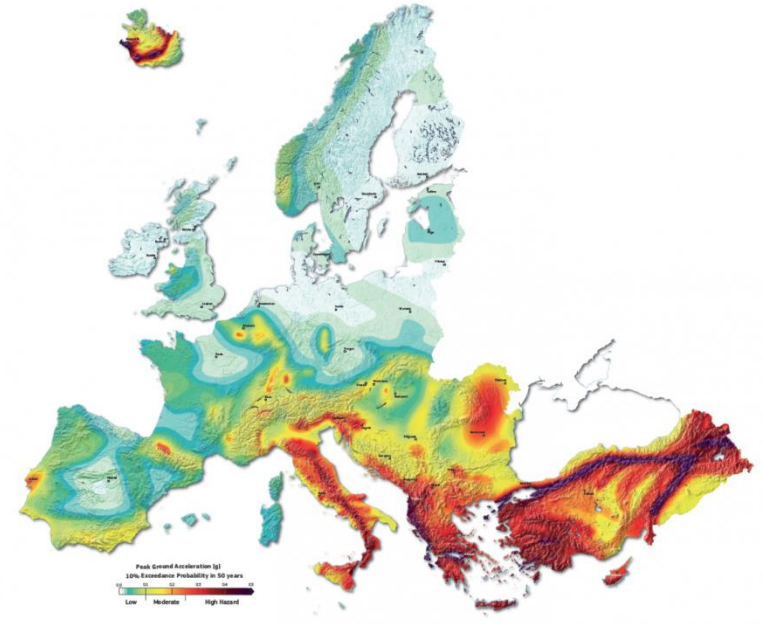
" *éventualité d'un évènement futur, incertain ou d'un terme indéterminé, ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage* "

droit français

# Qu'est ce qu'un risque ?




https://upload.wikimedia.org/wikipedia/commons/c/ca/ISS_impact_risk.jpg



http://horizon-magazine.eu/sites/default/files/SHARE-map.png

# Qu'est ce qu'un risque ?

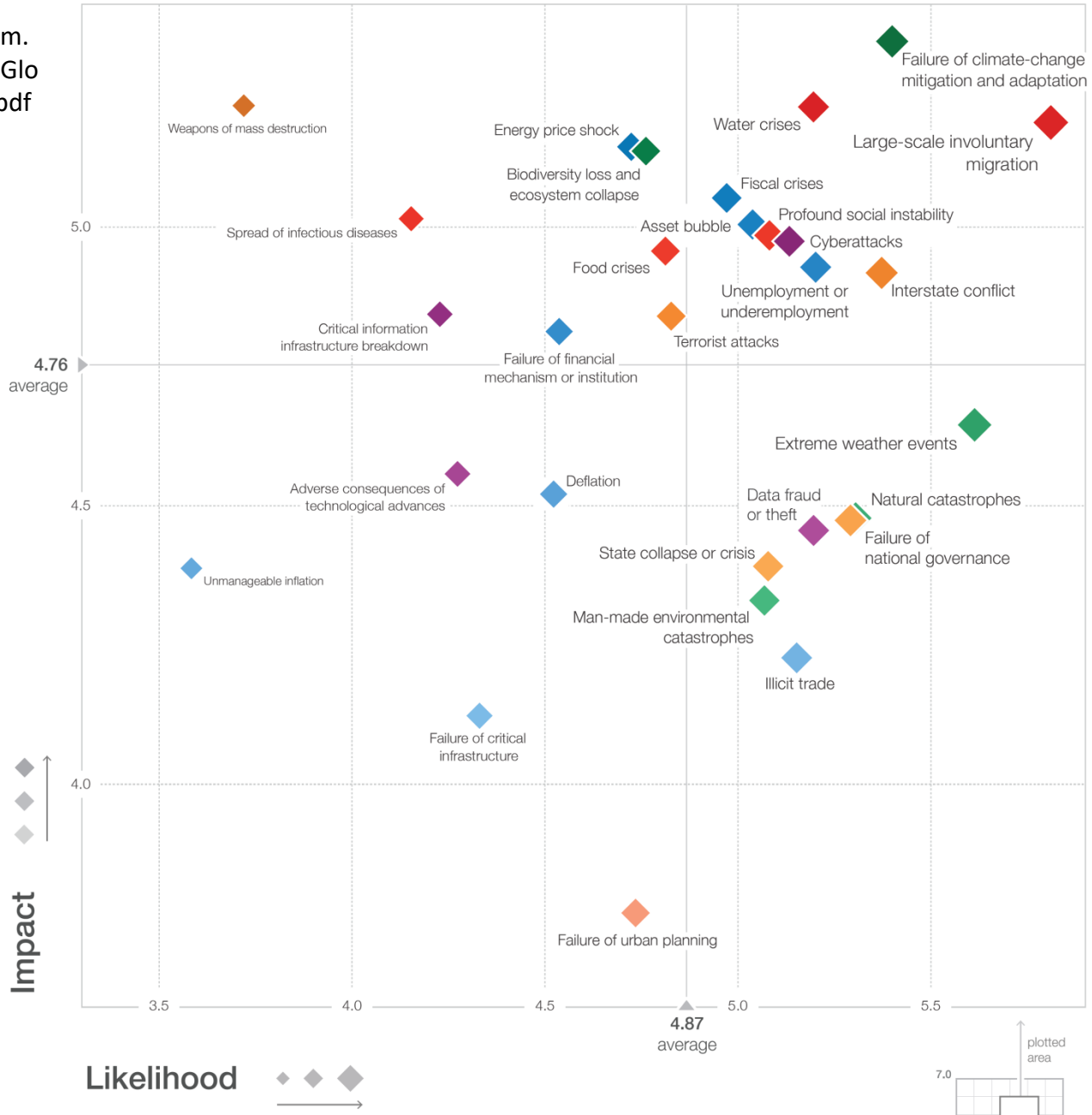
- 3 critères:
  - Nature d'un évènement
  - Probabilité de l'évènement
  - Impact de l'évènement

**Évènement**: Impact d'un astéroïde (>10km) avec la Terre
**Nature**: Risque naturel
**Probabilité**: < 1/ 1 000 000
**Impact**: Plutôt critique

**Évènement**: ne pas attraper le pokemon Crefollet (1/100PV) avec une pokeball
**Nature**: Risque naturel et humain
**Probabilité**: 98,83%
**Impact**: Plutôt insignifiant

CPE LYON
ÉCOLE SUPÉRIEURE DE CHIMIE PHYSIQUE ÉLECTRONIQUE DE LYON

http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf




Top 10 risks in terms of **Likelihood**

Top 10 risks in terms of **Impact**

# Différents types de risque

**(exemple)**

- Risques externes
  - Liés à l'environnement de l'entreprise, son activité, son marché ses concurrents, les réglementations
- Risques internes
  - Liés à l'organisation de l'entreprise, son management , ses processus, son système d'information
- Risque de pilotage
  - Liés aux informations nécessaires pour prendre des bonnes décisions (reporting financier, tableau de bord, étude de marché)

# Qu'est ce que la gestion de risque?

- La gestion des risques est la discipline qui s'attache à **identifier**, **évaluer** et **prioriser** les risques relatifs aux activités d'une organisation suivant une approche méthodique afin de **réduire** et **contrôler** la probabilité des événements redoutés, et **réduire** l'impact éventuel de ces événements.
- Eléments constituant
  - Etude de contexte
  - Appréciation des risques
  - Traitement des risques
  - Validation du traitement des risques
  - Communication relative aux risques
  - Suivre les risques

# Qu'est ce que la gestion de risque?

- Norme ou méthode ? (Clusir Rhône Alpes)

**Une norme** est un document de référence basé sur un consensus couvrant un large intérêt industriel ou économique et établi par un processus volontaire

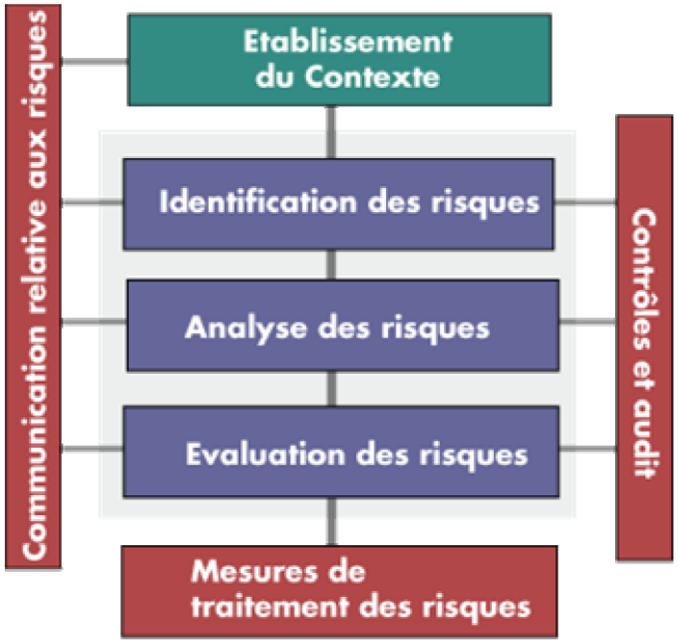
**Une méthode** est un moyen d'arriver à un résultat visé, elle ne comprend pas la notion de document de référence ni la notion de consensus

Norme et méthode doivent être associées afin que **l'outil méthode puisse être utilisé pour satisfaire une norme.**

# Pourquoi utiliser une méthode de gestion des risques ?

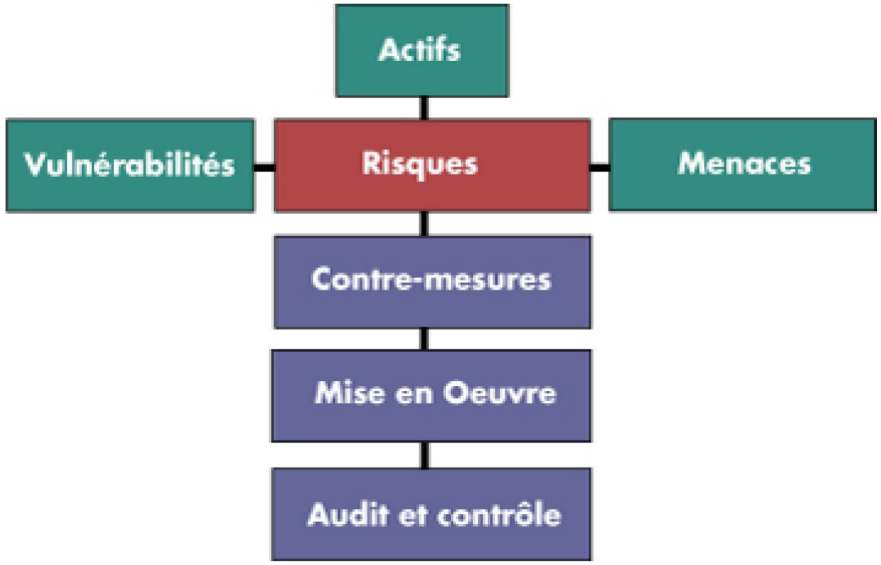
- Approche globale et complète
- Uniformité
- Rapidité / Efficacité
- Pas uniquement technique
- Implication de la chaine de décision

# Champs à couvrir par une méthode de management du risque



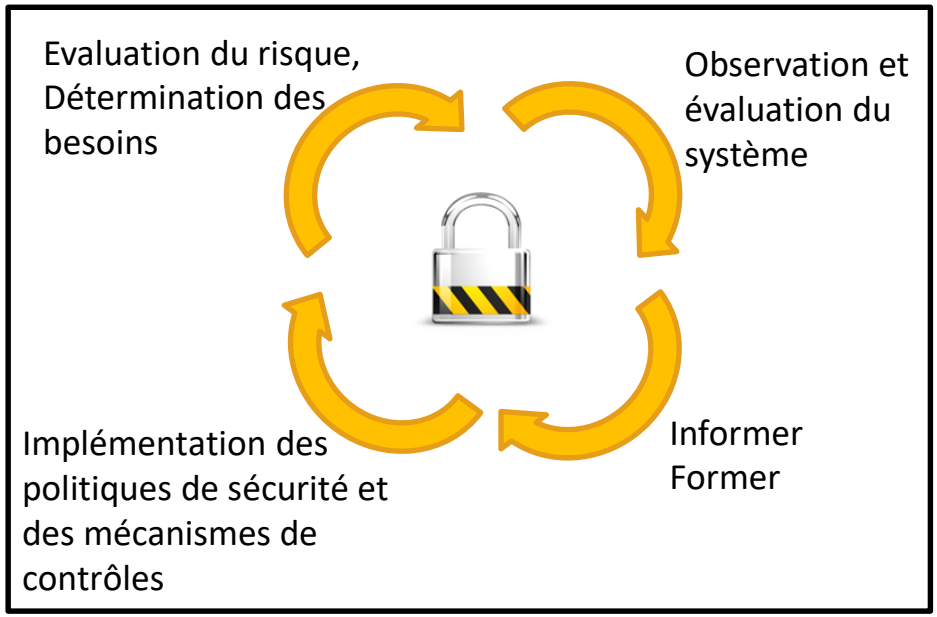

Synthèse du processus de management du risque (ISO 13335-2)





# Management de la sécurité

- Management du risque
- Politique de sécurité de l'information
- Procédures, Standard, Guideline, Baseline
- Classification des Informations
- L'organisation de la sécurité
- La formation à la sécurité

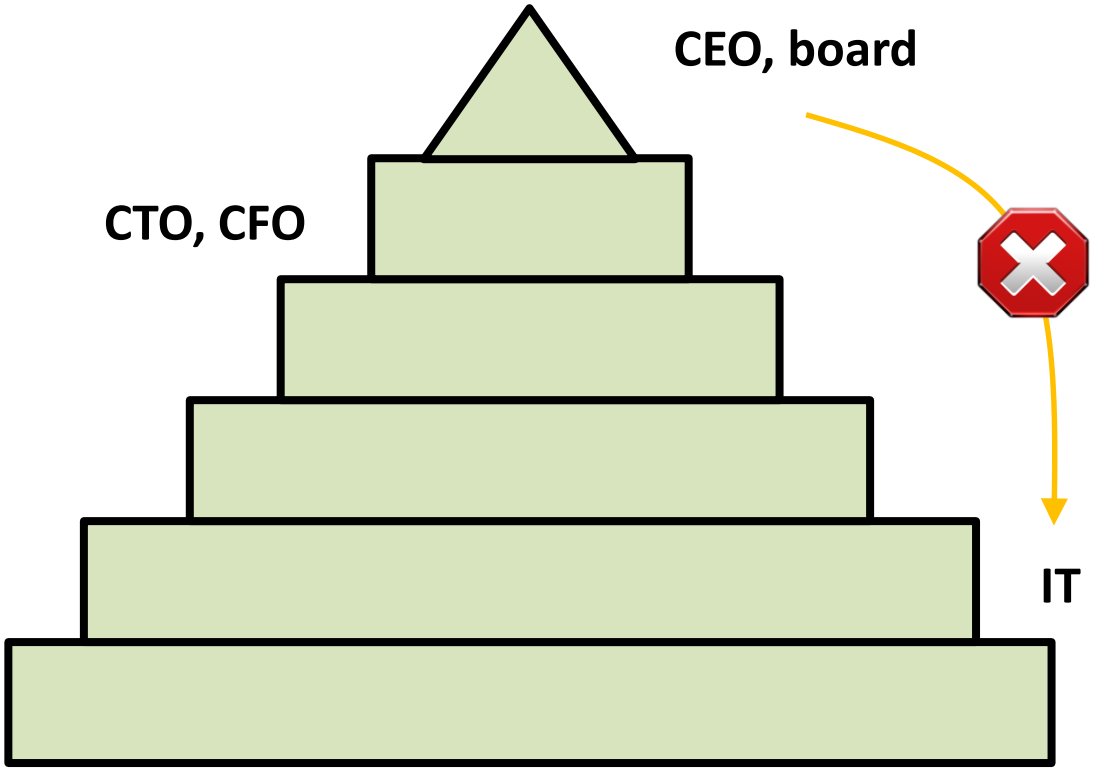



→Procédure circulaire

# Responsabilité

- Fonctions allouées:
  - Définir des objectifs
  - Définir le périmètre d'action
  - Définir les politiques
  - Définir les priorités
  - Définir les stratégies
- Evaluations requises:
  - Les objectifs business
  - Les risques
  - La productivité des utilisateurs
  - Les besoins fonctionnels

# Responsabilité



# Approche Top-Down

- Vision haut niveau nécessaire
  - Connaitre les enjeux avant de lancer un projet
  - Etre en adéquation avec les besoins stratégiques
  - Assurée une cohérence d'action
  - Définir des politiques homogènes et non ad hoc

- Risques liées à une approche Bottom-up
  - Solutions ad hocs hétérogènes
  - Complexité
  - Politiques incohérentes
  - Maintenance difficile

# Administration et contrôle

- Information Owner vs Security Team
- Contrôles nécessaires pour suivre les directives:
  - Contrôles Administratifs
  - Contrôles Techniques
  - Contrôles Physiques


**Figure 3-1** Administrative, technical, and physical controls should work in a synergistic manner to protect a company's assets.

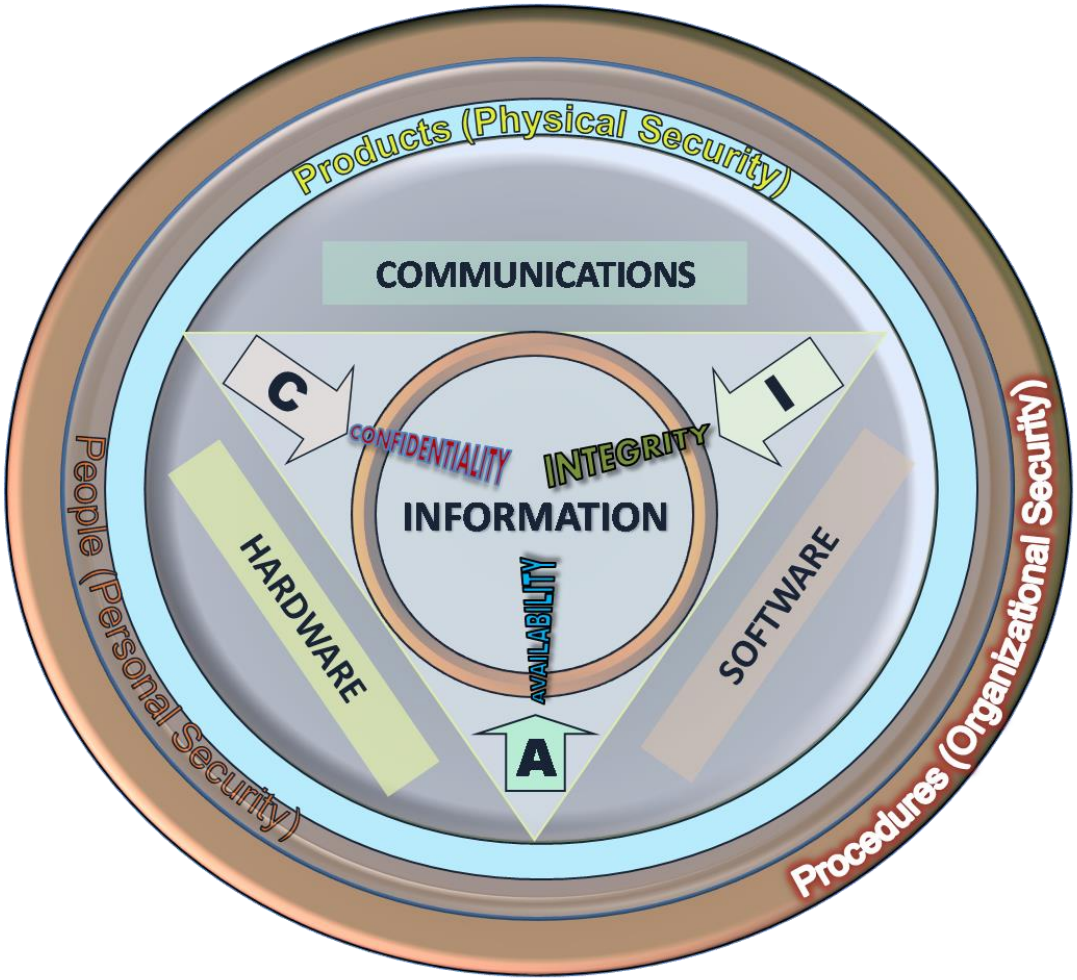
# Administration et contrôle

Sécurité

Accessibilité,
Facilité
d'utilisation

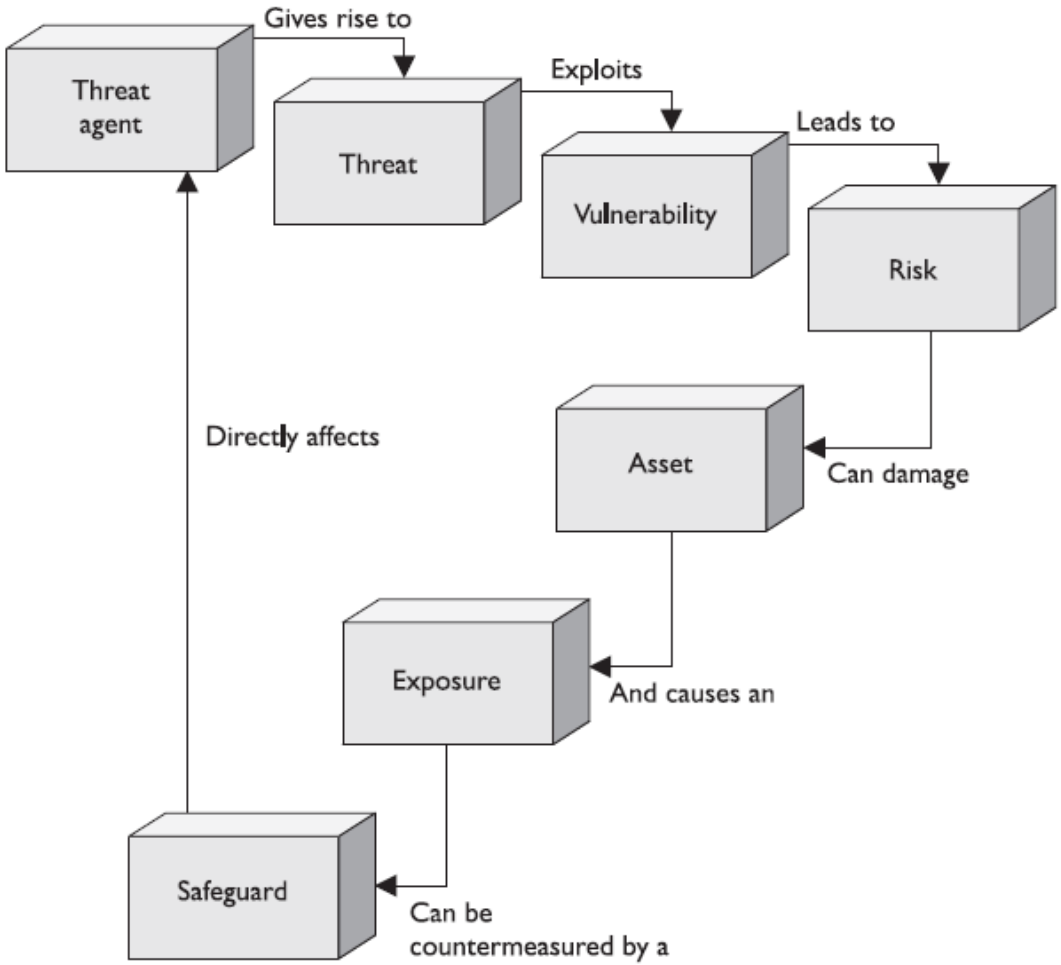
Attention à l'équilibre

# Rappel les enjeux de la sécurité




**JohnManuel** http://en.wikipedia.org/wiki/File:CIAJMK1209.png

# Rappel les enjeux de la sécurité



# Normes internationales

## ISO 27000

Aide les organisations à assurer la sécurité de leurs informations.

**ISO 27005:** décrit les grandes lignes d'une gestion des risques dans une perspective de mise en place d'un système de management de la sécurité des informations

**ISO 27001:** expose les exigences relatives aux systèmes de management de la sécurité des informations

## ISO 17000

Aide les organisations à assurer la sécurité de leurs informations.

**ISO 17799:** établit des lignes directrices et des principes généraux pour préparer, mettre en oeuvre, entretenir et améliorer la gestion de la sécurité de l'information au sein d'un organisme.

## ISO 31000

Fournit un cadre et des lignes directrices pour gérer toutes formes de risques.

# Méthode de management du risque: EBIOS

# Plusieurs méthodes !

- BDS Risk Assessor
- BDSS (Bayesian Decision Support System)
- Buddy Systel
- COBRA
- CRAMM (CCTA Risk Analysis And Management Method)
- **EBIOS**
- LAVA (Los Alamos Vulnerability Analysis)
- MARION
- **Mehari**
- MELISA
- OCTAVE
- RiskPac
- RiskWatch
- Security By Analysis (SBA)
- SISSI
- XRM (eXpert Risk Management)

Beaucoup de méthodes confidentielles
Seulement un sous ensemble est réellement utilisé

# Plusieurs méthodes !

- Sélection des méthodes en fonction du **cœur d'activité** (norme dans l'activité)

  **l'interopérabilité** des méthodes, capacité **d'usage en interne**, de la **pérennité** et de la **réglementation.**

| Méthode | Création | Popularité | Auteur | Soutenue par | Pays | Outils disponibles | Etat |
|---|---|---|---|---|---|---|---|
| **EBIOS** | 1995 | *** | DCSSI | gouvernement | France | logiciel gratuit | |
| **Melisa** | | ** | DGA | armement | France | | abandonnée |
| **Marion** | 1980 | ** | CLUSIF | association | France | | abandonnée |
| **Mehari** | 1995 | *** | CLUSIF | association | France | logiciel Risicare | |
| **Octave** | 1999 | ** | Université de Carnegie Mellon | universitaire | Etats-Unis | logiciel payant | |
| **Cramm** | 1986 | ** | Siemens | gouvernement | Angleterre | logiciel payant | |
| **SPRINT** | 1995 | * | ISF | association | Angleterre | logiciel payant | |
| **BS 7799** | | *** | | gouvernement | Angleterre | | |
| **ISO 17799** | | *** | | international | | | |
| **ISO 13335** | | | | international | | | |
| **ISO 15408** | | | | international | | | |
| **SCORE** | 2004 | | Ageris Consulting | secteur privé | France | logiciel payant | |
| **CALLIO** | 2001 | | CALLIO Technologies | secteur privé | Canada | logiciel payant | |
| **COBRA** | 2001 | | C & A Systems Security Limited | secteur privé | Angleterre | logiciel payant | |
| **ISAMM** | 2002 | | Evosec | secteur privé | Belgique | | |
| **RA2** | 2000 | | aexis | secteur privé | Allemagne | logiciel payant | |

http://cyberzoide.developpez.com/securite/methodes-analyse-risques/

# EBIOS

- **E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité
- Création 1995 DCSSI
- Objectifs:
  - Satisfaire les exigences de la gestion des risques d'un système de management de la sécurité informatique (ISO 27001)
  - Définir une démarche méthodologique (ISO 31000 et 27005)
  - Etablir une référence pour la certification de compétences relatives à la gestion du risque
- Référence dans les administrations Françaises

# EBIOS: Comment sont gérés les risques

1. Etablissement du contexte
2. Appréciation des risques
3. Traitement des risques
4. Validation du traitement des risques
5. Communications relatives aux risques
6. Surveillance des risques

# EBIOS: Comment sont gérés les risques

1. Etablissement du contexte

2. Appréciation des risques

Source de Menace

Menace


Vulnérabilité

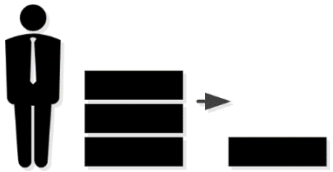
impact

=

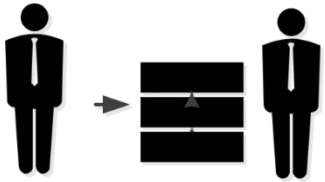
Risque

# EBIOS: Comment sont gérés les risques

3. Traitement des risques

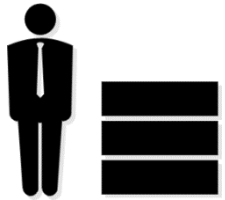


Réduire



Transférer

Eviter



Prendre

4. Validation des risques 

5. Communications relatives au risque 

6. Surveillance des risques 

# EBIOS:

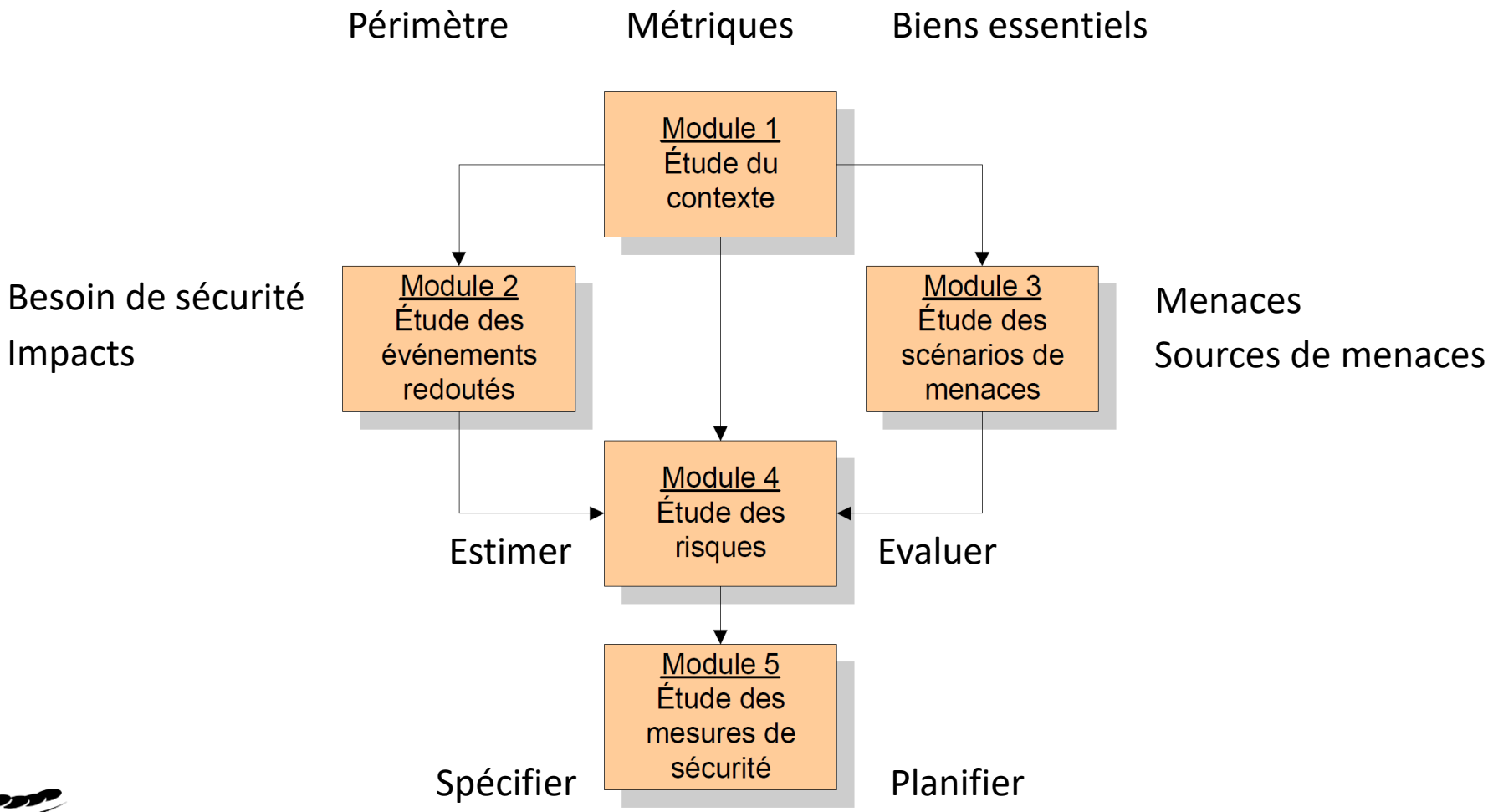
## Avantages

- Un outil de négociation et d'arbitrage
- Un outil de sensibilisation
- Une méthode rapide
- Une approche exhaustive
- Un référentiel complet
- De nombreux utilisateurs

## Inconvénients

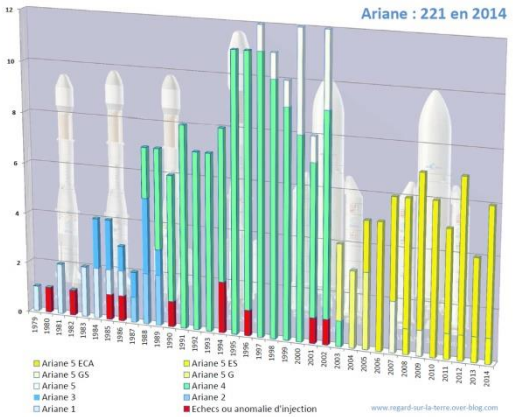
- Principalement utilisé en France (dans les administrations)
- Reconnaissance internationale limitée
- Peu d'outils fonctionnels

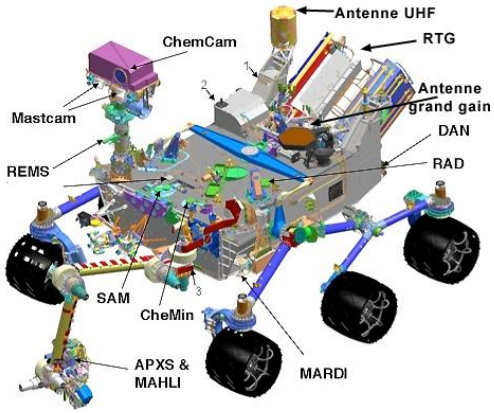
# EBIOS: Démarche itérative



# EBIOS: Différents usages

## Macro vs Micro




**Biens essentiels:** grandes activités du groupes
**Bien support:** ensemble des logiciels

**Biens essentiels:** Champs base de données spatiale
**Bien support:** Embedded VxWorks 4.21

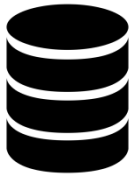
# EBIOS: Pré-requis

Décomposition du périmètre en sous périmètre

Itération de la méthode

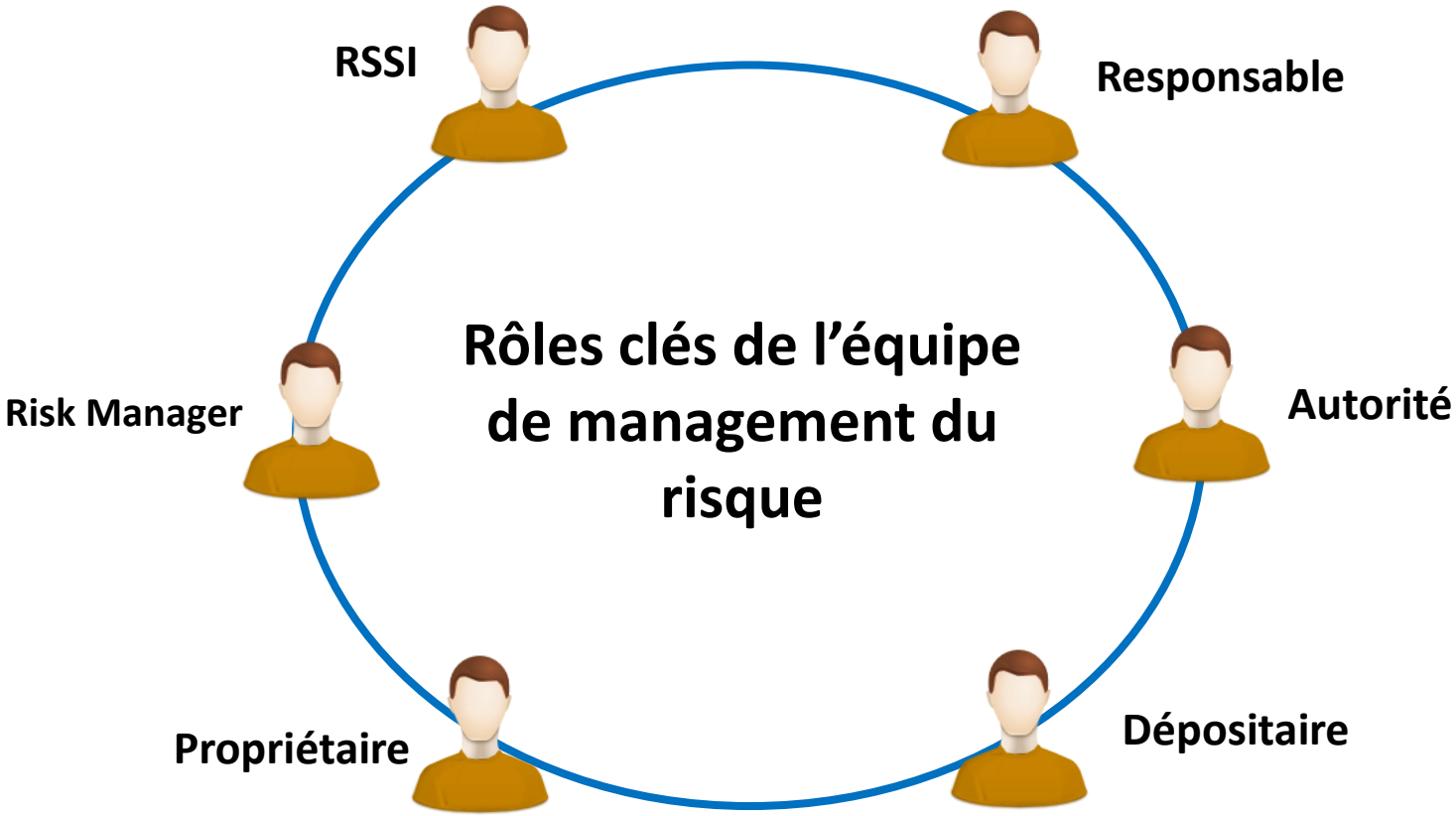
Choix d'activités pertinentes

Niveau de détail approprié



Ajustement base de connaissances

# EBIOS: les interlocuteurs

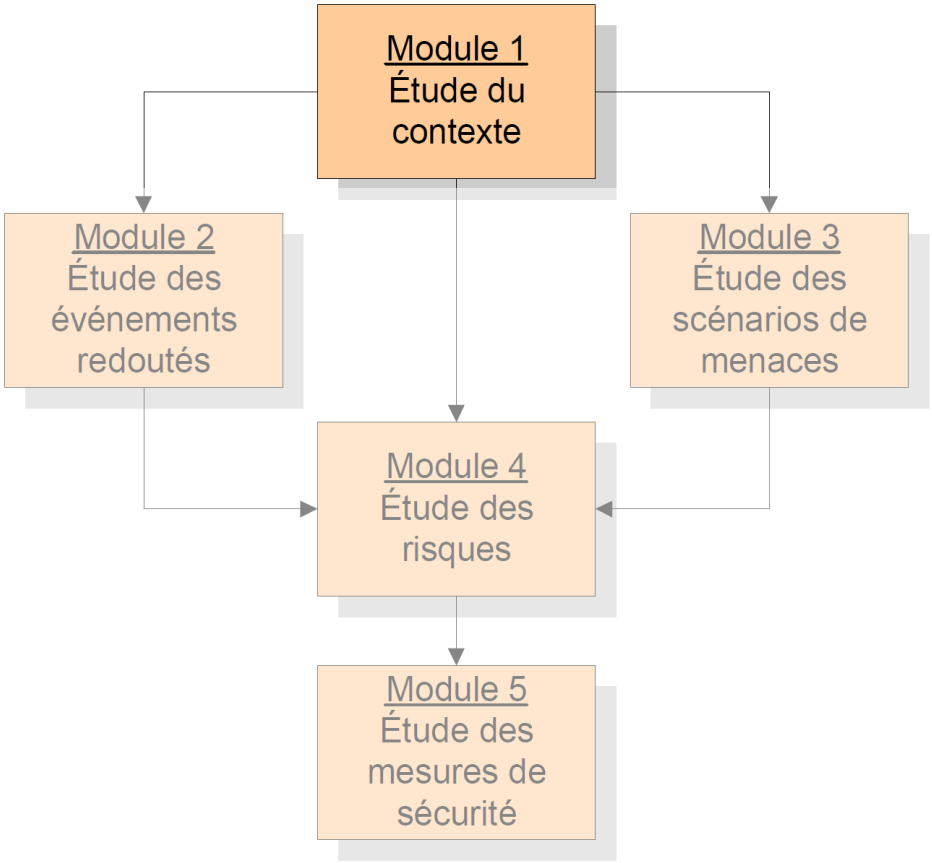


# EBIOS: Création d'une entreprise

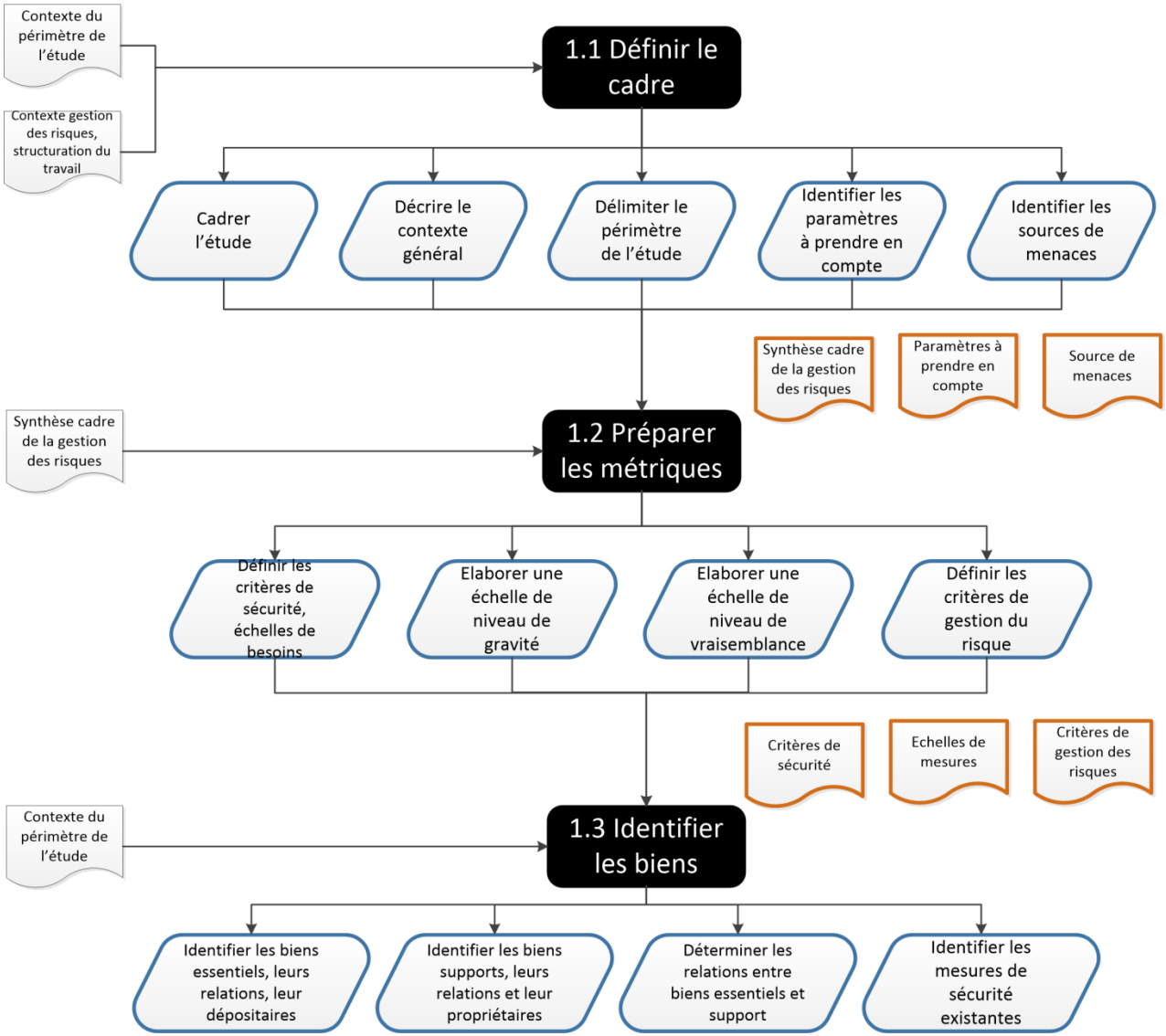
- Nature de l'activité
- Taille de l'entreprise
- Situation (leader, candidat, startup)
- Partenaires extérieurs
- Si (architecture macro)
- Objectifs : moyen terme, long terme

# EBIOS:

Périmètre Métriques Biens essentiels



# EBIOS: Etude du contexte



# EBIOS: Etude du contexte

## Activité 1.1 – Définir le cadre de la gestion des risques

**Objectif**

Cette activité fait partie de l'établissement du contexte. Elle a pour but de circonscrire le périmètre d'étude et de définir le cadre dans lequel la gestion des risques va être réalisée.

**Avantages**

- Permet de circonscrire objectivement le périmètre de l'étude
- Permet de s'assurer de la légitimité et de la faisabilité des réflexions qui vont être menées
- Permet d'orienter les travaux et les livrables en fonction des objectifs réels

**Données d'entrée**

- Données concernant le contexte du périmètre de l'étude (documents stratégiques, documents relatifs aux missions, les attributions et l'organisation, politique de gestion des risques…).
- Données concernant le contexte de la gestion des risques et la structure de travail

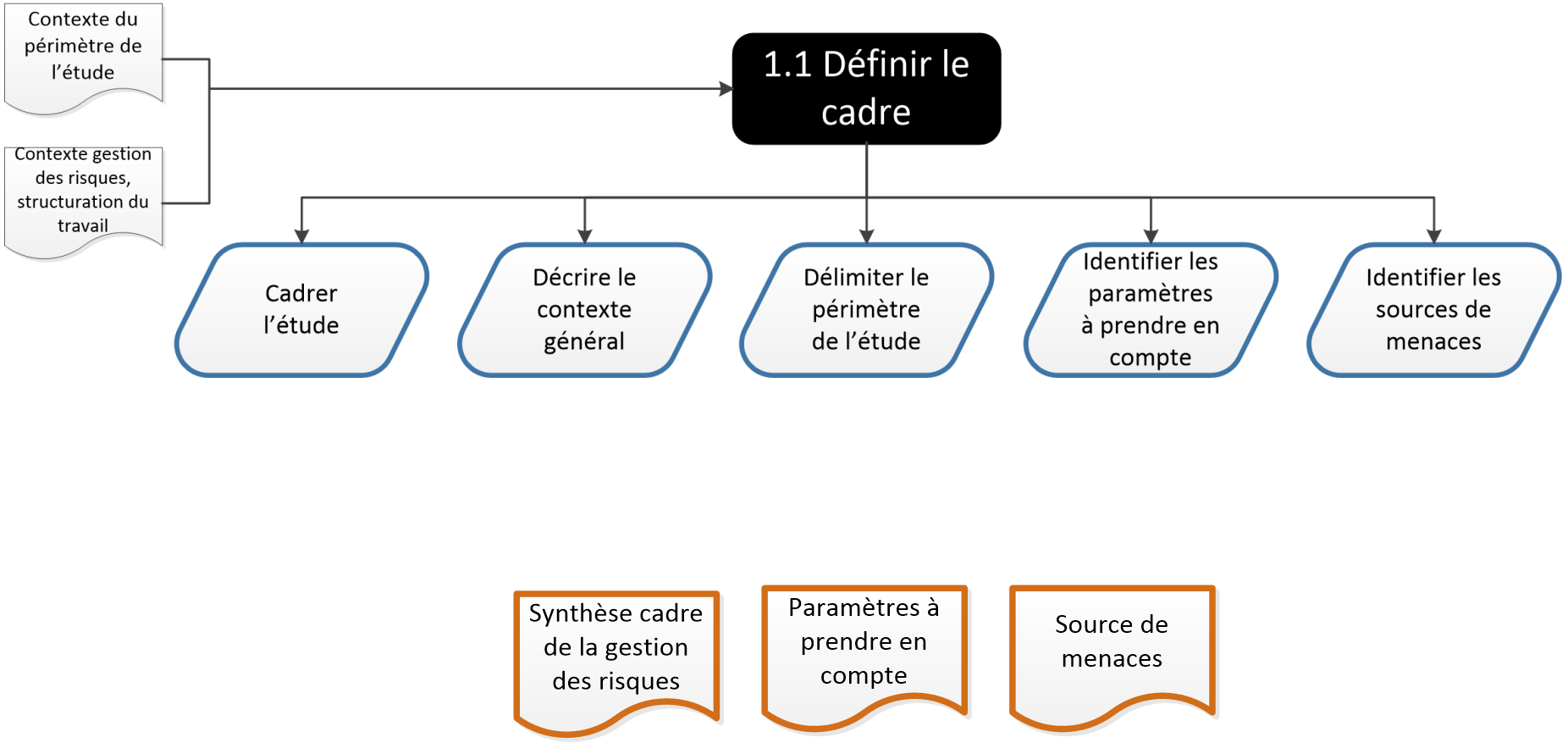
**Actions préconisées et rôle des parties prenantes**

| Actions : \ Parties prenantes : | Responsable | RSSI | *Risk manager* | Autorité | Dépositaire | Propriétaire |
|---|---|---|---|---|---|---|
| Action 1.1.1. Cadrer l'étude des risques | R | C | C | I | | |
| Action 1.1.2. Décrire le contexte général | R | | | I | | |
| Action 1.1.3. Délimiter le périmètre de l'étude | R | | | A | | |
| Action 1.1.4. Identifier les paramètres à prendre en compte | R | | | I | | |
| Action 1.1.5. Identifier les sources de menaces | R | C | C | I | | |

**Données produites**

- Synthèse relative au cadre de la gestion des risques
- Paramètres à prendre en compte
- Sources de menaces

# EBIOS: Etude du contexte



# EBIOS: Etude du contexte

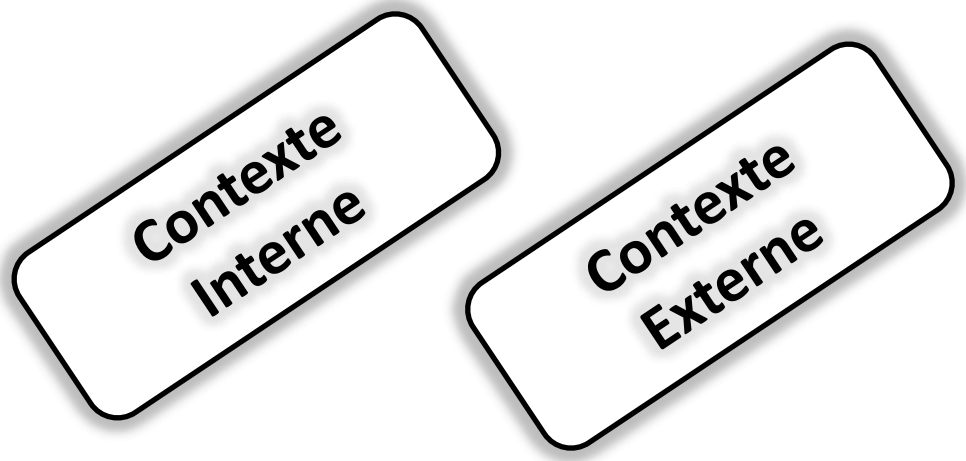
Cadrer l'étude

L'objectif de l'étude est **d'identifier les risques** liés à **l'utilisation** d'un **service de cloud computing de type IaaS** (Infrastructure as a Service) pour effectuer **un traitement de données**. Seront identifiés **les scénarios de menaces sur les biens supports de la société**, les évènements redoutés sur les biens essentiels ainsi que le détail des menaces et vulnérabilités. **L'étude doit permettre de faire ressortir des mesures de sécurité visant à réduire au maximum les risques identifiés.**

# EBIOS: Etude du contexte

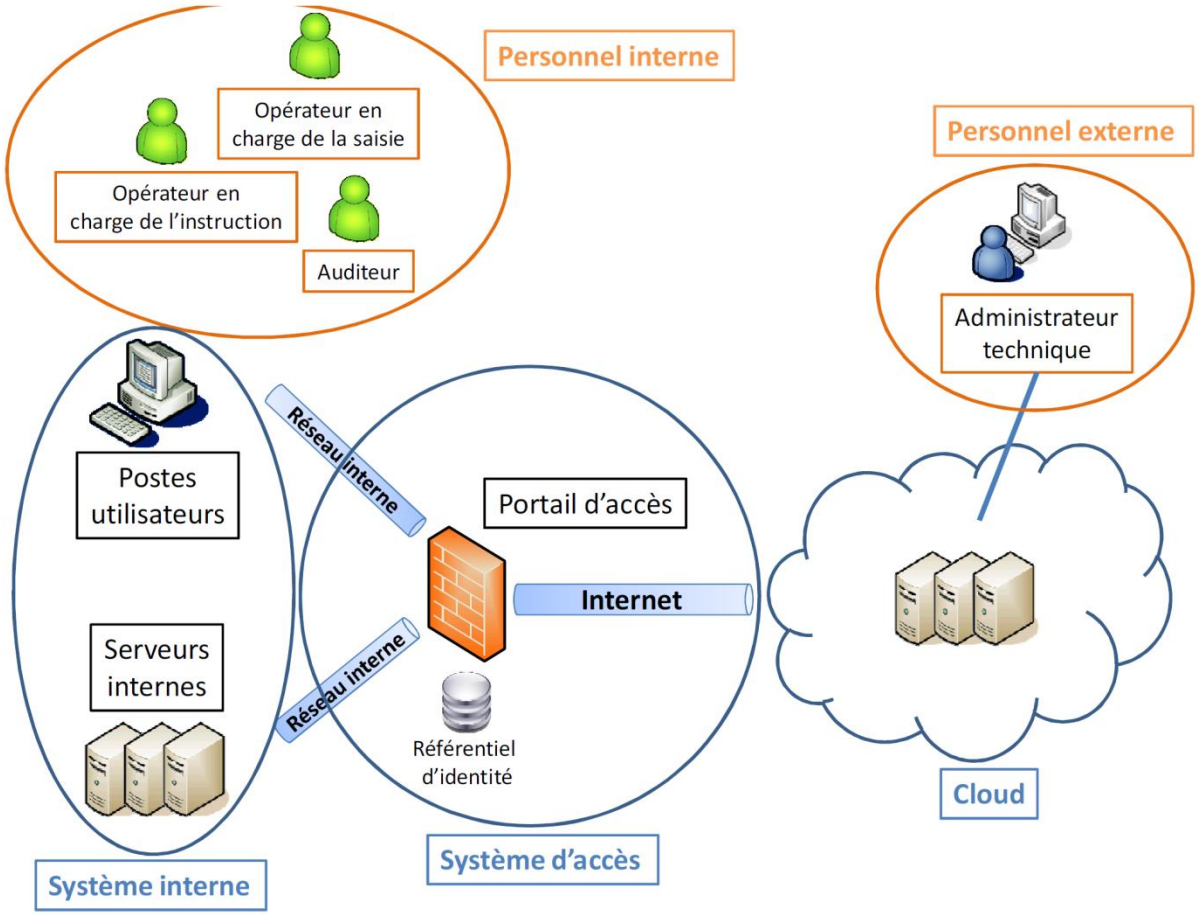
Décrire le contexte général

Un assureur s'attend à un **pic de déclaration en cas d'évènements catastrophiques**. Il fait **appel à un service de type IAAS** pour héberger et traiter les données de déclaration de sinistre. Ces **données sont rapatriées dans son SI** une fois instruites par les experts d'assurance.



# EBIOS: Etude du contexte

Décrire le contexte général



# EBIOS: Etude du contexte

Délimiter le périmètre de l'étude

L'étude se situe **au niveau du système d'information de l'assureur**, qui est interconnecté avec le système du cloud provider. Un portail d'accès permet l'administration et l'exploitation de la fonction de traitement des données de déclaration de sinistre ainsi que des données elles-mêmes.
Le schéma ci-dessous illustre le périmètre restreint de cette étude.

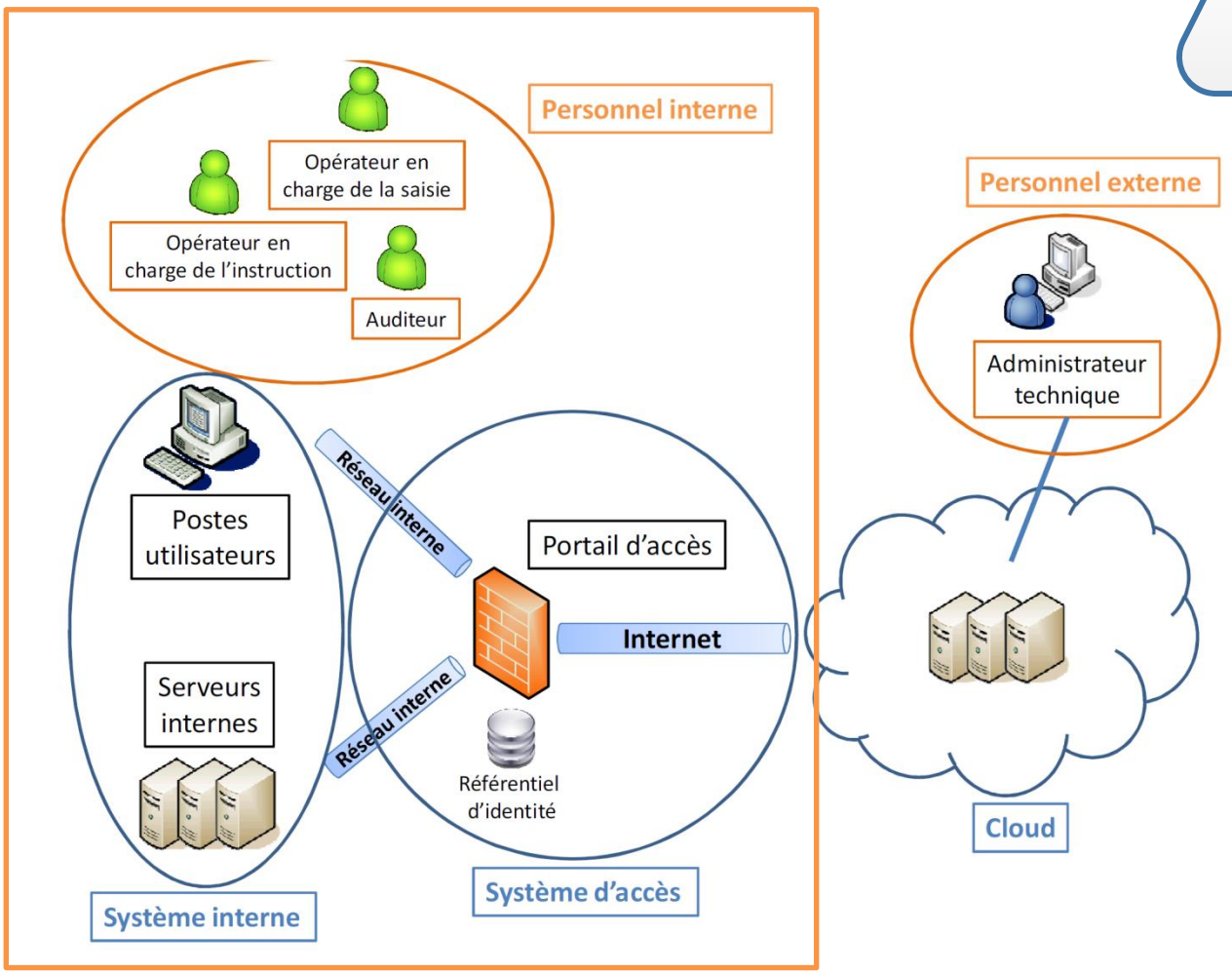
Découpage en sous périmètre

Mode d'exploitation de sécurté

Participants de l'étude

# EBIOS: Etude du contexte

Délimiter le périmètre de l'étude



# EBIOS: Etude du contexte

Identifier les paramètres à prendre en compte

- Sur l'organisme
  - contraintes relatives au personnel
  - contraintes d'ordre calendaire
  - contraintes relatives aux méthodes
  - contraintes d'ordre culturel
  - contraintes d'ordre budgétaire
  - contraintes d'ordre politique
  - contraintes d'ordre stratégique
  - contraintes territoriales
  - contraintes conjoncturelles
  - contraintes structurelle
  - contraintes fonctionnelle

- Spécifique sur le périmètre
  - contraintes d'antériorité
  - contraintes technique
  - contraintes financières
  - contraintes d'environnement
  - contraintes de temps
  - contraintes relatives aux méthodes
  - contraintes organisationnelles

# EBIOS: Etude du contexte

Identifier les paramètres à prendre en compte

| | |
|---|---|
| Le datacenter du prestataire comporte toutes les mesures de sécurités nécessaires (accès physique contrôlé, matériel non soumis aux menaces environnementales, réseau électrique de secours, réseau de communication protégé...) | Hypothèses |
| Les postes de travail du prestataire sont sécurisés et ne présentent pas de vulnérabilité. Ils ne sont pas retenus comme bien support. | Hypothèses |
| Les postes de travail internes sont sécurisés et ne présentent pas de vulnérabilité. Ils ne sont pas retenus comme bien support. | Hypothèses |
| Respect des règles fixées par la CNIL relative à la protection des données à caractère personnel. | Références communautaires, légales et réglementaires à appliquer |

# EBIOS: Etude du contexte

Identifier les sources de menaces

- Origines des risques
- Typologies de sources de menaces
- Connaitre son exposition face à ces menaces
- Connaitre le potentiel de ces menaces
  - Motivation
  - Facilité d'accès
  - Temps disponible à l'action
  - Compétences techniques disponibles
  - Ressources financières ou matérielles

# EBIOS: Etude du contexte

Identifier les sources de menaces

- Sources humaines agissant de manière délibérée
  - 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

# EBIOS: Etude du contexte

Identifier les sources de menaces

- Sources humaines agissant de manière accidentelle

- 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 des capacités importantes
- Source humaine externe, sans intention de nuire, avec des capacités illimitées

# EBIOS: Etude du contexte

Identifier les sources de menaces

- Sources non humaines
  - Phénomène naturel
  - Catastrophe naturelle ou sanitaire
  - Activité animale
  - Code malveillant d'origine inconnue
  - Événement interne

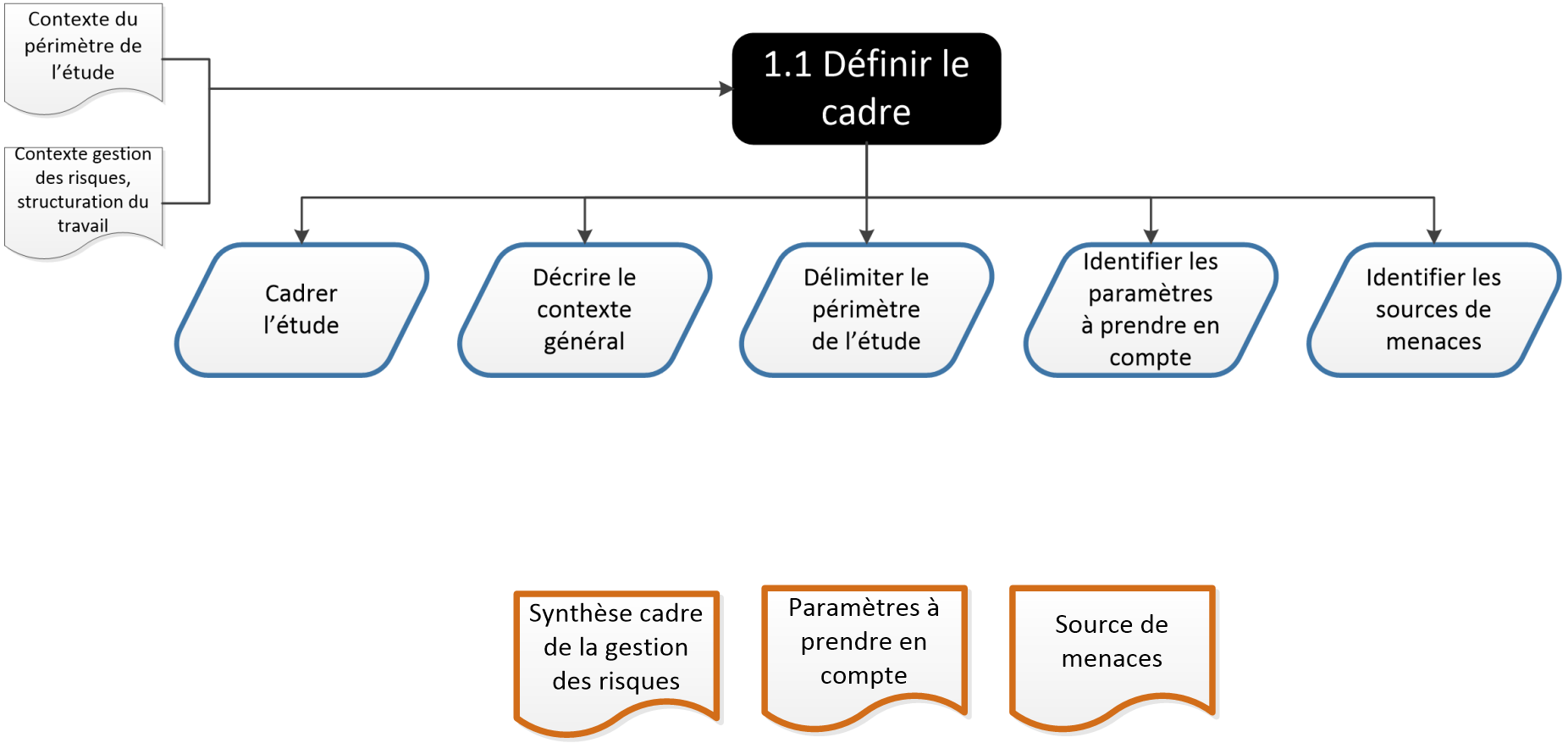
# EBIOS: Etude du contexte

Identifier les sources de menaces

**Liste des sources de menace - 29 élément(s)**

| Source de menace | Type de source de menace | Description |
|---|---|---|
| Employé malveillant | Source humaine interne, malveillante, avec de | Un employé de la société voulant causer des torts à la so |
| Employé du prestataire malveillant | Source humaine interne, malveillante, avec de | Un employé du cloud provider qui cause des torts à sa so |
| Source humaine interne, malveillante, avec de faibles capacités | Sources humaines agissant de manière délibér | |
| Source humaine interne, malveillante, avec des capacités importa | Sources humaines agissant de manière délibér | |
| Source humaine interne, malveillante, avec des capacités illimitée | Sources humaines agissant de manière délibér | |
| Source humaine externe, malveillante, avec de faibles capacités | | |
| Source humaine externe, malveillante, avec des capacités importa | Sources humaines agissant de manière délibér | |
| Source humaine externe, malveillante, avec des capacités illimité | | |
| Administrateur malveillant | Source humaine interne, malveillante, avec des | Un administrateur de la société qui cause des torts à sa s |
| Administrateur du prestataire malveillant | Source humaine interne, malveillante, avec des | Un administrateur du cloud provider qui cause des torts à |
| Pirate | Source humaine externe, malveillante, avec de | Un pirate souhaitant causer des torts à la société et qui p |
| Concurrent | Source humaine externe, malveillante, avec de | Un concurrent qui souhaite soutirer des informations ou c |

# EBIOS: Etude du contexte



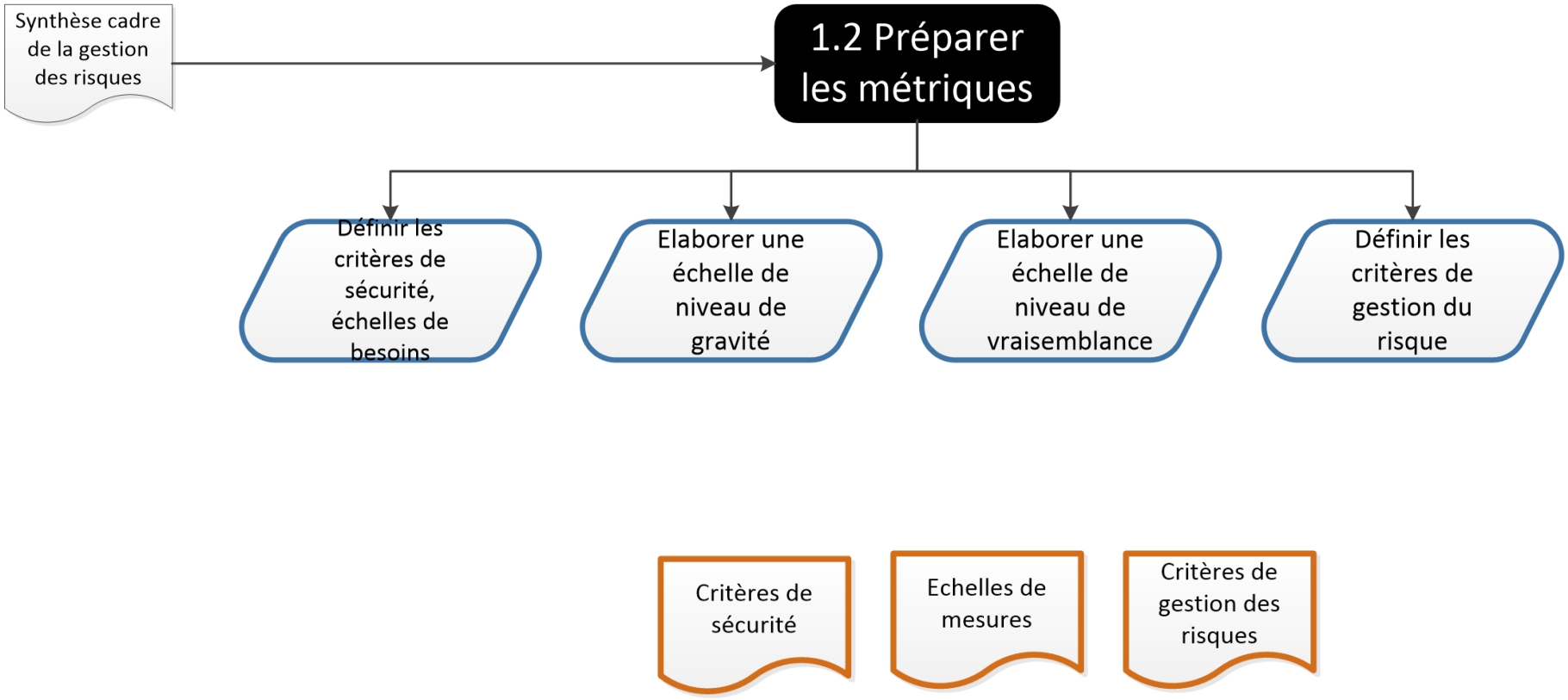
# EBIOS: Analyse de risque

1.1 Définir le cadre

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

https://adullact.net/frs/?group_id=737&release_id=4324#logiciel-ebios-2010-complet-ebios_2010_complet_20111023-title-content

# EBIOS: Etude du contexte



# EBIOS: Etude du contexte

## Activité 1.2 – Préparer les métriques

**Objectif**

Cette activité fait partie de l'établissement du contexte. Elle a pour but de fixer l'ensemble des paramètres et des échelles qui serviront à gérer les risques. Elle peut être commune à plusieurs études.

**Avantages**

- Permet de garantir l'homogénéité des estimations
- Permet la répétabilité dans le temps des activités de gestion des risques

**Données d'entrée**

- Synthèse relative au cadre de la gestion des risques

**Actions préconisées et rôle des parties prenantes**

| Actions : \ Parties prenantes : | Responsable | RSSI | *Risk manager* | Autorité | Dépositaire | Propriétaire |
|---|---|---|---|---|---|---|
| Action 1.2.1. Définir les critères de sécurité et élaborer les échelles de besoins | R | C | | A | | |
| Action 1.2.2. Élaborer une échelle de niveaux de gravité | R | C | C | A | | |
| Action 1.2.3. Élaborer une échelle de niveaux de vraisemblance | R | C | C | A | | |
| Action 1.2.4. Définir les critères de gestion des risques | R | C | C | A | | |

**Données produites**

- Critères de sécurité
- Échelles de mesures
- Critères de gestion des risques

CPE LYON
ÉCOLE SUPÉRIEURE DE CHIMIE PHYSIQUE ÉLECTRONIQUE DE LYON

# EBIOS: Etude du contexte

Définir les critères de sécurité, échelles de besoins

| Liste des critères de sécurité - 3 élément(s) | |
|---|---|
| Critère de sécurité | Niveau échelle |
| Confidentialité | 1. Public<br>2. Limité<br>3. Réservé<br>4. Privé |
| Disponibilité | 1. Plus de 48h<br>2. Entre 24h et 48h<br>3. Entre 4h et 24h<br>4. Moins de 4h |
| Intégrité | 1. Détectable<br>2. Maîtrisé<br>3. Intègre |

# EBIOS: Etude du contexte

Elaborer une échelle de niveau de gravité

| Niveau de l'échelle | Description détaillée de l'échelle |
|---|---|
| 0. Insignifiant | L'évènement redouté n'est pas retenu dans le contexte de cette étude |
| 1. Négligeable | La société surmontera les impacts sans aucune difficulté |
| 2. Limitée | La société surmontera les impacts malgré quelques difficultés |
| 3. Importante | La société surmontera les impacts avec de sérieuses difficultés |
| 4. Critique | La société surmontera les impacts avec de très sérieuses difficultés et sur une très longue période |

# EBIOS: Etude du contexte

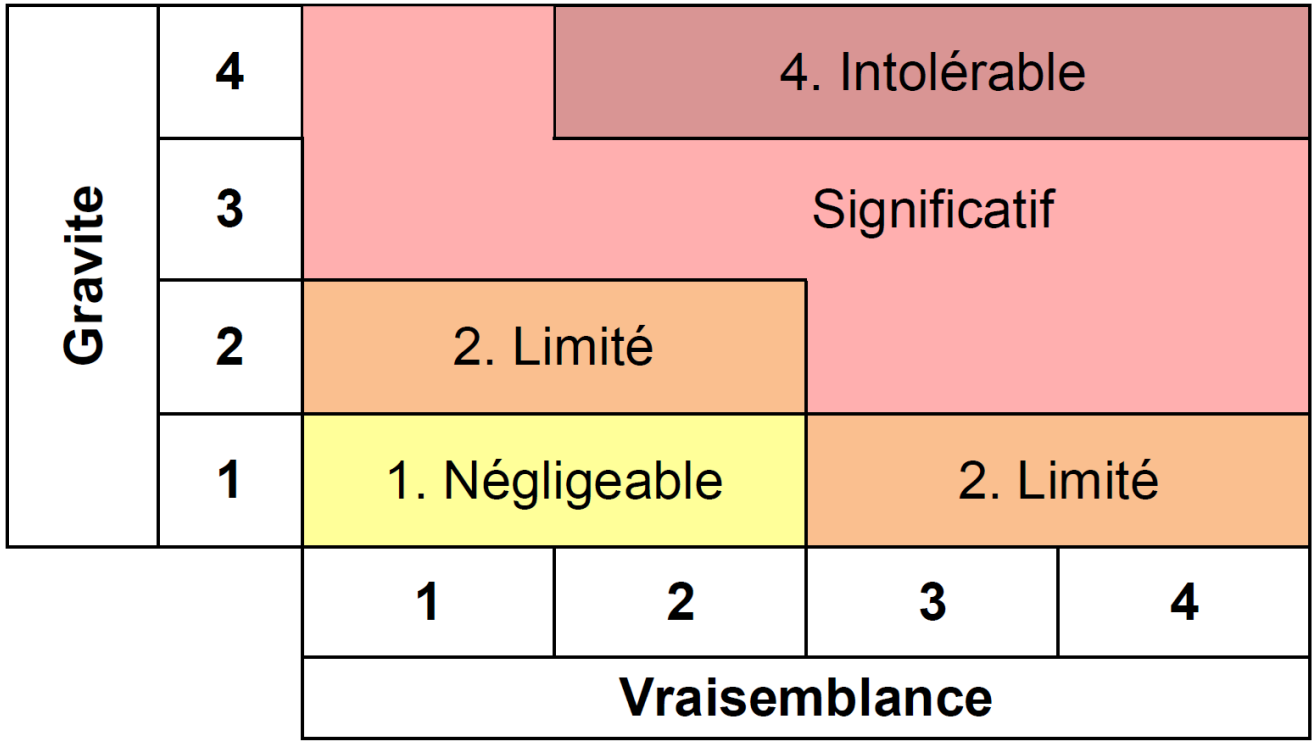
Elaborer une échelle de niveau de vraisemblance

| Niveau de l'échelle | Description détaillée de l'échelle |
|---|---|
| 1. Minime | Cela ne devrait pas se (re)produire dans les 3 ans / Besoin des privilèges d'administrateur |
| 2. Significative | Cela pourrait se (re)produire dans les 3 ans / Besoin de connaissances et d'un accès aux utilisateurs |
| 3. Forte | Cela devrait se (re)produire dans l'année / Sans besoin de connaissances et avec un besoin d'accès aux utilisateurs |
| 4. Maximale | Cela va certainement se (re)produire plusieurs fois dans l'année / Sans besoin de connaissances ni d'accès aux utilisateurs |

# EBIOS: Etude du contexte

Définir les critères de gestion du risque

Echelle de niveau des risques



# EBIOS: Etude du contexte

Définir les critères de gestion du risque

| | |
|---|---|
| 1.3.4 Identifier les mesures de sécurité existantes | |
| 2.1.1 Analyser tous les événements redoutés | Les évènements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet. |
| 2.1.2 Évaluer chaque événement redouté | Les évènements redoutés sont classés par ordre décroissant de gravité. |
| 3.1.1 Analyser tous les scénarios de menaces | Les scénarios de menaces sont estimés en termes de vraisemblance à l'aide de l'échelle définie à cet effet. |
| 3.1.2 Évaluer chaque scénario de menace | Les scénarios de menaces sont classés par ordre décroissant de vraisemblance. |
| 4.1.1 Analyser les risques | La gravité d'un risque est égale à celle de l'évènement redouté considéré. La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'évènement redouté considéré. |
| 4.1.2 Évaluer les risques | Sont jugés comme intolérables les risques dont la gravité est critique et la vraisemblance significative ou plus, ou les risques dont la gravité est importante et la vraisemblance maximale. Sont jugés comme significatifs les risques dont la gravité est critique et la vraisemblance négligeable, les risques dont la gravité est importante et la vraisemblance néglideable, significative ou forte, et les risques dont la gravité est limitée et la vraisemblance au moins significative. Les autres risques sont jugés comme négligeables. |
| 4.2.1 Choisir les options de traitement des risques | On cherchera à réduire tous les risques. |
| 4.2.2 Analyser les risques résiduels | |
| 5.1.1 Déterminer les mesures de sécurité | Les mesures de sécurité sont fixées en fonction du contexte pour éliminer au maximum les scénarios de menaces en corrigeant une vulnérabilité ou en cherchant à limiter l'impact. |
| 5.1.2 Analyser les risques résiduels | |
| 5.1.3 Établir une déclaration d'applicabilité | |
| 5.2.1 Élaborer le plan d'action et suivre la réalisation des mesures de sécurité | |
| 5.2.2 Analyser les risques résiduels | |

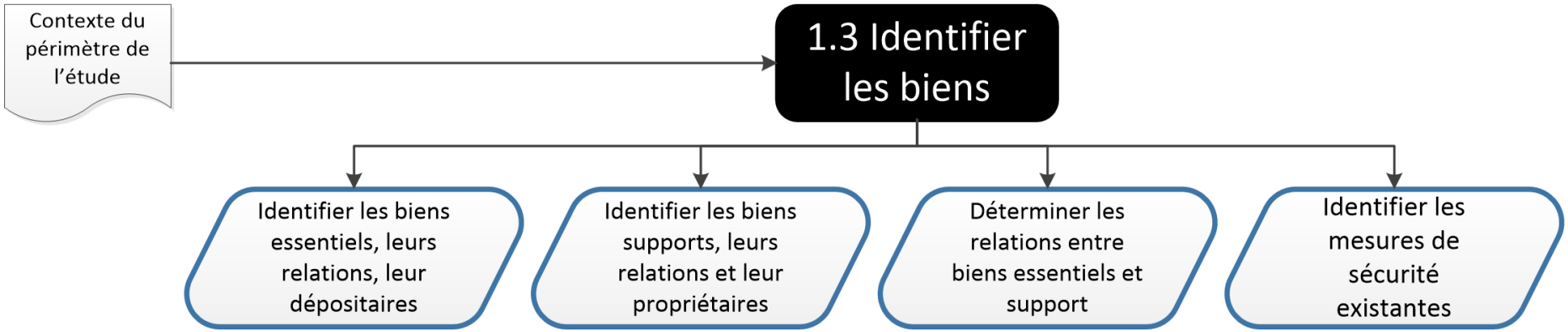
CPE LYON
ÉCOLE SUPÉRIEURE DE CHIMIE PHYSIQUE ÉLECTRONIQUE DE LYON

# EBIOS: Analyse de risque

**1.2 Préparer les métriques**

- Définir les critères de sécurité, échelles de besoins
- Elaborer une échelle de niveau de gravité
- Elaborer une échelle de niveau de vraisemblance
- Définir les critères de gestion du risque

# EBIOS: Etude du contexte



# EBIOS: Etude du contexte

## Activité 1.3 – Identifier les biens

**Objectif**

Cette activité fait partie de l'établissement du contexte. Elle a pour but d'identifier les biens au sein du périmètre de l'étude et ainsi de mettre en évidence les éléments nécessaires aux autres activités.

**Avantages**

- Permet de comprendre le fonctionnement du périmètre de l'étude
- Permet de prendre en compte les mesures de sécurité existantes (que celles-ci soient formalisées ou non) pour valoriser le travail déjà effectué et ne pas le remettre en cause

**Données d'entrée**

- Données concernant le contexte du périmètre de l'étude (documents concernant le système d'information, synthèses d'entretiens avec des responsables de l'organisme…).

**Actions préconisées et rôle des parties prenantes**

| Actions : \ Parties prenantes : | Responsable | RSSI | *Risk manager* | Autorité | Dépositaire | Propriétaire |
|---|---|---|---|---|---|---|
| Action 1.3.1. Identifier les biens essentiels, leurs relations et leurs dépositaires | A | C | I | | R | |
| Action 1.3.2. Identifier les biens supports, leurs relations et leurs propriétaires | A | C | | | | R |
| Action 1.3.3. Déterminer le lien entre les biens essentiels et les biens supports | A | C | | | | R |
| Action 1.3.4. Identifier les mesures de sécurité existantes | A | C | | | | R |

**Données produites**

- Biens essentiels
- Biens supports
- Tableau croisé biens essentiels / biens supports
- Mesures de sécurité existantes

# EBIOS: Etude du contexte

Identifier les biens essentiels, leurs relations, leur dépositaires

| Groupe | Infos essentielles | Dépositaire |
|---|---|---|
| Système d'information externalisé | Données de déclaration de sinistre | DSI |
| | Données de sécurité (Clés de chiffrement, logs, référentiel d'identité et des droits) | DSI |
| Fonctions externalisées | Traitement des données | DSI |

# EBIOS: Etude du contexte

Identifier les biens supports, leurs relations et leur propriétaires

| Biens supports | Détails |
|---|---|
| Système d'accès (SYS_AIN) | Réseau de l'organisme |
| | Réseau internet |
| Système externalisé (SYS_EXT) | Serveurs du prestataire |
| | Postes de travail du prestataire |
| | Logiciel d'administration du prestataire |
| | Portail d'accès |
| Système d'accès du prestataire (SYS_APR) | Réseau du prestataire |
| Organisation interne (ORG_INT) | Utilisateurs (opérateurs en charge de la saisie, opérateurs en charge de l'instruction, auditeurs) |
| | Administrateurs fonctionnels |
| | Administrateurs techniques |
| Organisation du prestataire (ORG_PRE) | Administrateurs du cloud |
| | Sous-traitants du Cloud Provider |

# EBIOS: Etude du contexte

Identifier les biens supports, leurs relations et leur propriétaires

- **SYS** - Système Informatique et de Téléphonie
  - **MAT** – Matériels
  - **LOG** – Logiciels
  - **RSX** – Canaux info. Et de téléphonie

- **ORG** Les organisations
  - **PER** – Personnes
  - **PAP** – Supports papier
  - **CAN** – Canaux interpersonnels

- **LOC** Les locaux

# EBIOS: Etude du contexte

Déterminer les relations entre biens essentiels et support

| Bien essentiels<br>Biens supports | Données de déclaration de sinistre | Données de sécurité | Traitement des données |
|---|---|---|---|
| Système d'accès (SYS_AIN) | X | X | |
| Système externalisé (SYS_EXT) | X | | X |
| Système d'accès du prestataire (SYS_APR) | X | X | |
| Organisation interne (ORG_INT) | X | X | |
| Organisation du prestataire (ORG_PRE) | X | X | |

# EBIOS: Etude du contexte

Identifier les mesures de sécurité existantes

**Liste des mesures de sécurité - 13 élément(s)**

| Etat ( | Libellé | Type de mesure | BS associé | Prévention | Protection | Récupération |
|---|---|---|---|---|---|---|
| E | Périmètre de sécurité physique | Mesures de l'étude | Système du prestataire (SYS_EXT) | X | X | |
| E | Contrôle physique des accès | Mesures de l'étude | Système du prestataire (SYS_EXT) | X | X | |
| E | Protection contre les menaces extérieures et environnementales | Mesures de l'étude | Système du prestataire (SYS_EXT) | X | X | |
| E | Services généraux | Mesures de l'étude | Système du prestataire (SYS_EXT) | X | X | X |
| E | Sécurité du câblage | Mesures de l'étude | Système d'accès du prestataire (SYS_APR) | | X | |
| E | Sécurité de la documentation système | Mesures de l'étude | Organisation interne (ORG_INT)<br>Organisation du prestataire (ORG_PRE) | | X | |
| E | Gestion des privilèges | Mesures de l'étude | Organisation interne (ORG_INT) | X | X | |
| E | Enregistrement des utilisateurs | Mesures de l'étude | Organisation interne (ORG_INT) | X | X | |
| E | Gestion du mot de passe utilisateur | Mesures de l'étude | Système d'accès (SYS_AIN)<br>Organisation interne (ORG_INT) | | X | |
| E | Utilisation du mot de passe | Mesures de l'étude | Système d'accès (SYS_AIN)<br>Organisation interne (ORG_INT) | X | X | |
| E | Authentification des administrateurs | Mesures de l'étude | Système du prestataire (SYS_EXT) | | X | |
| E | Authentification des utilisateurs | Mesures de l'étude | Système du prestataire (SYS_EXT) | | X | |
| E | Plan de continuité de l'activité du prestataire | Mesures de l'étude | Système du prestataire (SYS_EXT) | X | | X |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 9.1 Zones sécurisée | Contrôle physique des accès | Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels. | X | x | | Système d prestatair |

# EBIOS: Analyse de risque

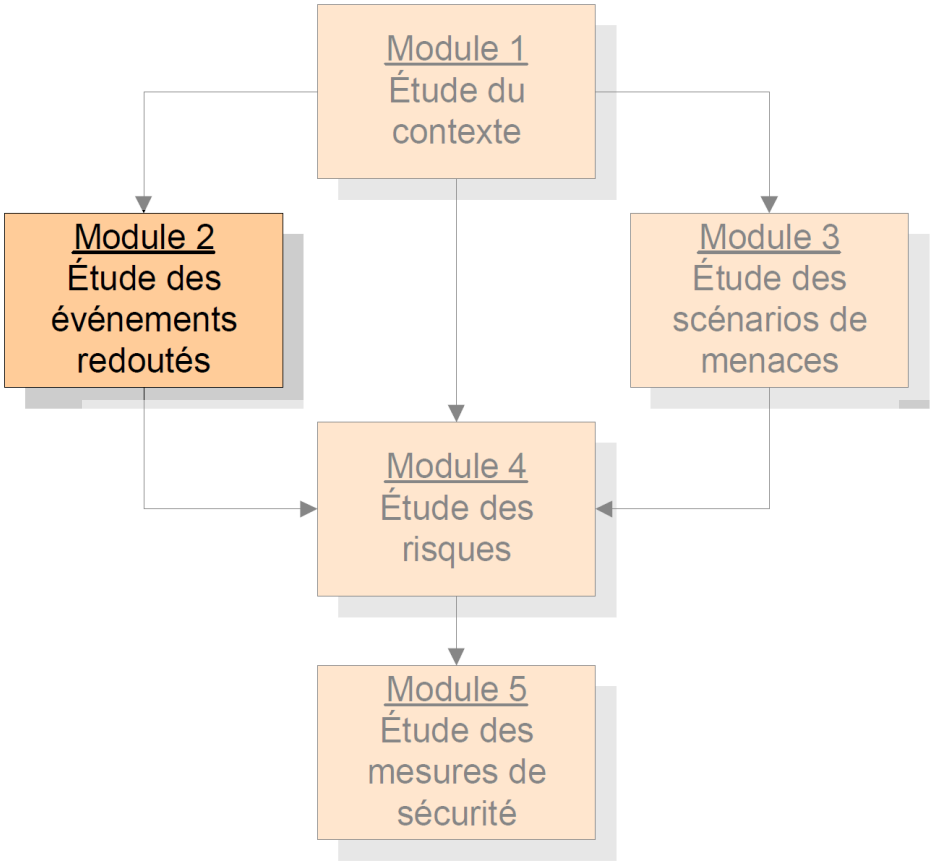
**1.3 Identifier les biens**

- Identifier les biens essentiels, leurs relations, leur dépositaires
- Identifier les biens supports, leurs relations et leur propriétaires
- Déterminer les relations entre biens essentiels et support
- Identifier les mesures de sécurité existantes

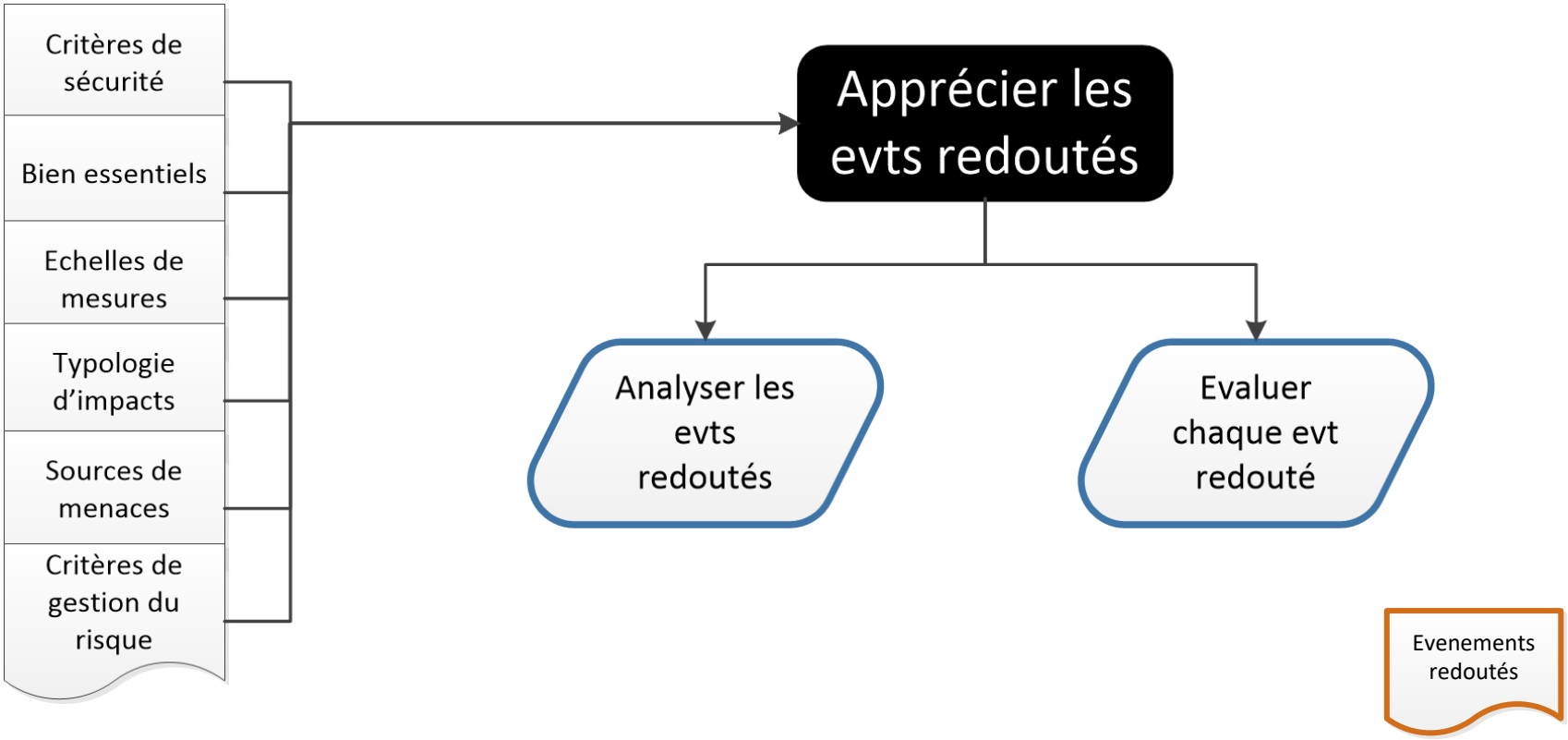
# EBIOS:

Besoin de sécurité

Impacts



# EBIOS: Etude des Evts Redoutés



# EBIOS: Etude des Evts Redoutés

## Activité 2.1 – Apprécier les événements redoutés

**Objectif**

Cette activité fait partie de l'appréciation des risques. Elle a pour but de faire émerger et de caractériser les événements liés à la sécurité de l'information que l'organisme redoute, sans étudier la manière dont ceux-ci peuvent arriver. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.

**Avantages**

- Permet aux parties prenantes de comparer objectivement l'importance des biens essentiels et de prendre conscience des véritables enjeux de sécurité
- Permet d'étudier un périmètre sans détailler les biens supports et les scénarios envisageables
- Permet de hiérarchiser les événements redoutés, voire d'en écarter de la suite de l'étude

**Données d'entrée**

- Critères de sécurité
- Biens essentiels
- Échelles de mesures
- Typologie d'impacts
- Sources de menaces
- Critères de gestion des risques

**Actions préconisées et rôle des parties prenantes**

| Actions : \ Parties prenantes : | Responsable | RSSI | *Risk manager* | Autorité | Dépositaire | Propriétaire |
|---|---|---|---|---|---|---|
| Action 2.1.1. Analyser tous les événements redoutés | A | C | | | R | |
| Action 2.1.2. Évaluer chaque événement redouté | R | C | I | A | C | |

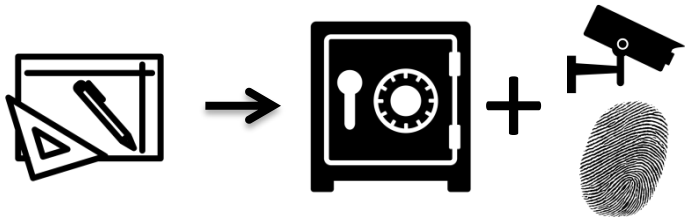
**Données produites**

- Événements redoutés

# EBIOS: Etude des Evts Redoutés

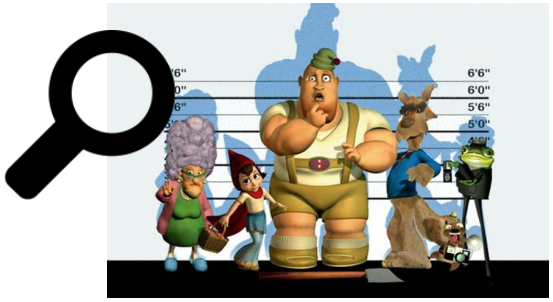
Analyser les evts redoutés

- Besoins de sécurité ET bien essentiel



- Besoin de sécurité ET Impact (en cas de non respect)

- Identifier les sources de menaces (à l'origine du non respect des besoins de sécurité)



# EBIOS: Etude des Evts Redoutés

Analyser les evts redoutés

| N° | Evènement Redouté | Besoin | Sources de menaces | Impacts | Gravité |
|---|---|---|---|---|---|
| Données de déclaration de sinistre | | | | | |
| ER1 | Divulgation des données | Privé | • Pirate<br>• Employé du prestataire peu sérieux<br>• Employé du prestataire malveillant<br>• Bogue logiciel<br>• Hébergeur/Faille dans l'application<br>• Employé peu sérieux | • Perte de notoriété<br>• Perte de confiance vis-à-vis des clients<br>• Impossibilité de remplir des obligations légales<br>• Action en justice à l'encontre de la société<br>• Non-conformité aux labels de sécurité<br>• Chute de valeur en bourse | 4. Critique |
| ER2 | Altération des données | Intègre | • Pirate<br>• Employé du prestataire peu sérieux<br>• Employé peu sérieux<br>• Hébergeur/Faille dans l'application | • Impossibilité de remplir les obligations légales<br>• Impossibilité d'assurer le traitement<br>• Perte de confiance vis-à-vis des clients<br>• Non-conformité aux labels de sécurité | 3. Importante |
| ER3 | Indisponibilité des données | 24h | • Pirate<br>• Employé du prestataire peu sérieux<br>• Employé du prestataire malveillant<br>• Hébergeur/Faille dans l'application<br>• Entreprise tierce<br>• Changement de juridiction<br>• Panne de serveur<br>• Bogue logiciel<br>• Catastrophe naturelle | • Impossibilité d'assurer le traitement<br>• Perte de confiance vis-à-vis des clients | 2. Limitée |
| Données de sécurité | | | | | |
| ER4 | Divulgation des données de sécurité | Privé | • Pirate | • Mise en péril du système d'information externalisé<br>• Impossibilité de remplir les obligations légales<br>• Non-conformité aux labels de sécurité<br>• Perte de notoriété | 4. Critique |

# EBIOS: Etude des Evts Redoutés

Evaluer chaque evt redouté

| Gravité | Evénements redoutés |
|---|---|
| 4. Critique | • ER1 Divulgation des données<br>• ER4 Divulgation des données de sécurité |
| 3. Importante | • ER2 Altération des données<br>• ER5 Altération des données de sécurité<br>• ER9 Indisponibilité de la fonction de traitement |
| 2. Limitée | • ER3 Indisponibilité des données<br>• ER6 Indisponibilité des données de sécurité |
| 1. Négligeable | |
| 0. Insignifiant | • ER7 Divulgation de la fonction de traitement<br>• ER8 Altération de la fonction de traitement |

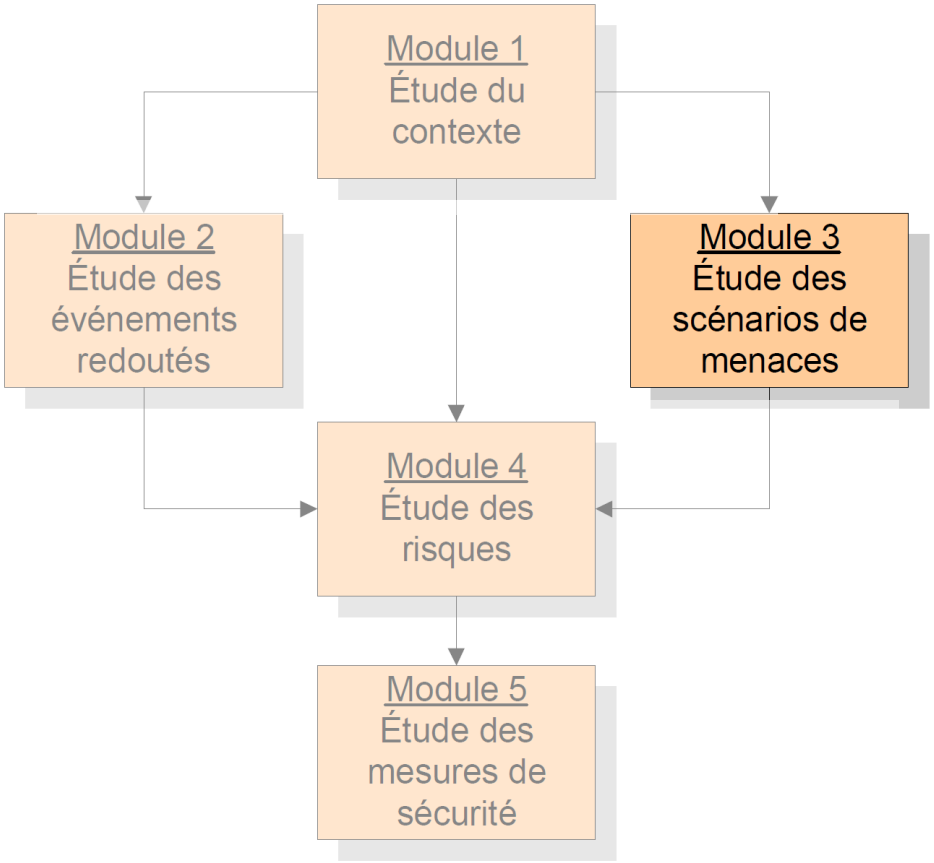
# EBIOS: Analyse de risque

Apprécier les evts redoutés

Analyser les evts redoutés

Evaluer chaque evt redouté

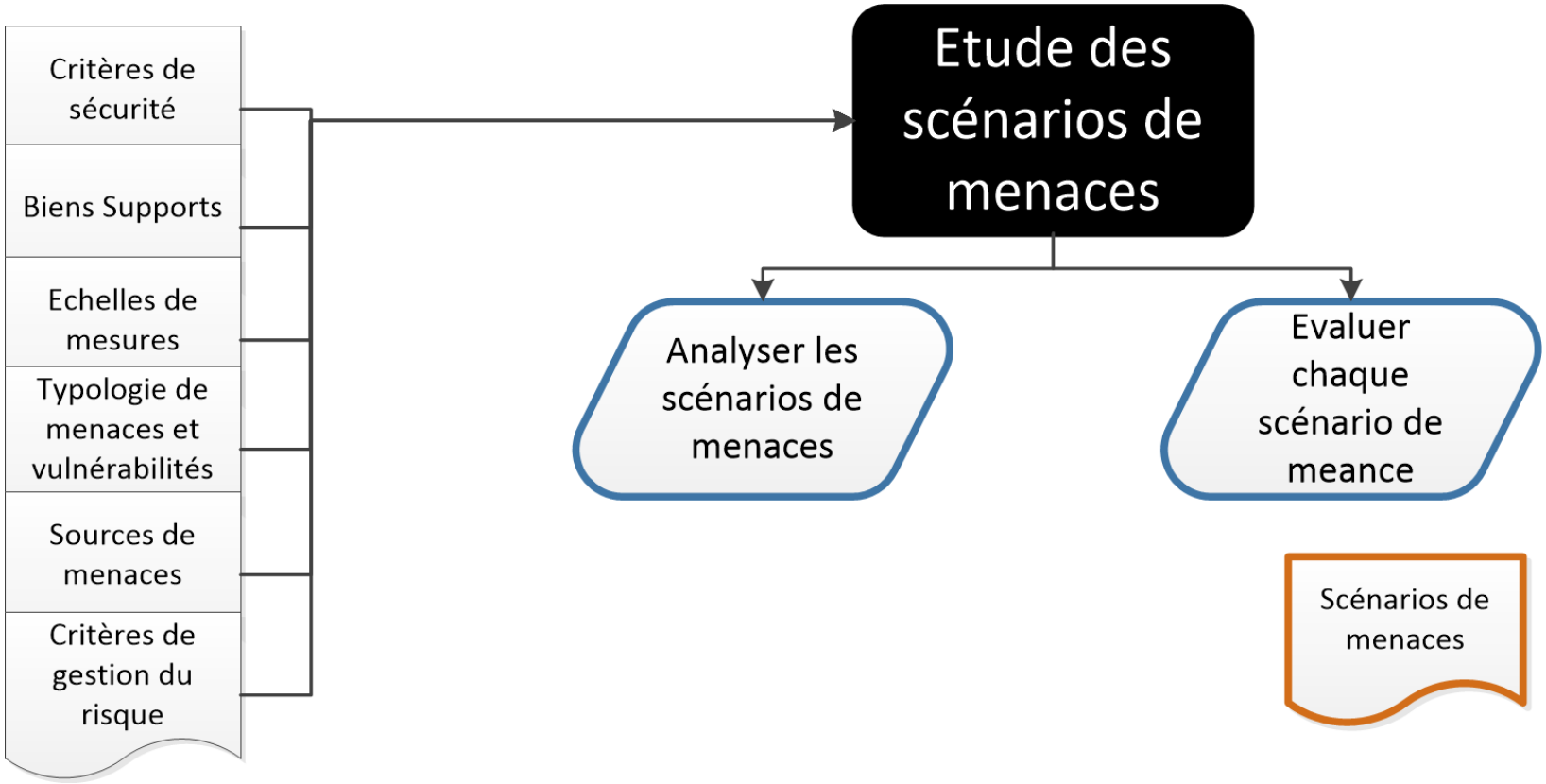
# EBIOS:




Menaces

Sources de menaces

# EBIOS: Scénarios de menaces



# EBIOS: Scénarios de menaces

## Activité 3.1 – Apprécier les scénarios de menaces

**Objectif**

Cette activité fait partie de l'appréciation des risques. Elle a pour but d'identifier les différentes possibilités d'actions sur les biens supports, afin de disposer d'une liste complète de scénarios de menaces. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.

**Avantages**

- Permet aux parties prenantes de réaliser la diversité des menaces et de comparer objectivement la faisabilité des modes opératoires
- Permet de garantir une exhaustivité de la réflexion sur les menaces et les vulnérabilités
- Permet de s'adapter aux connaissances dont on dispose sur le périmètre de l'étude
- Permet de hiérarchiser les scénarios de menaces, voire d'en écarter de la suite de l'étude

**Données d'entrée**

- Critères de sécurité
- Biens supports
- Échelles de mesures
- Typologie de menaces et des vulnérabilités
- Sources de menaces
- Critères de gestion des risques

**Actions préconisées et rôle des parties prenantes**

| Actions : \ Parties prenantes : | Responsable | RSSI | *Risk manager* | Autorité | Dépositaire | Propriétaire |
|---|---|---|---|---|---|---|
| Action 3.1.1. Analyser tous les scénarios de menaces | A | C | | | | R |
| Action 3.1.2. Évaluer chaque scénario de menace | A | C | I | | | C |

**Données produites**

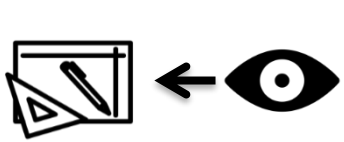
- Scénarios de menaces

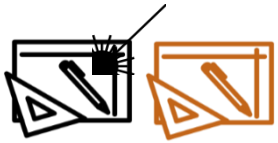
CPE LYON ÉCOLE SUPÉRIEURE DE CHIMIE PHYSIQUE ÉLECTRONIQUE DE LYON

# EBIOS: Scénarios de menaces

Analyser les scénarios de menaces

- Les menaces





- Les vulnérabilités

- Les sources de menaces






# EBIOS: Scénarios de menaces

Analyser les scénarios de menaces

## 3.1 Système d'accès (SYS_AIN)

| Bien Support | Scénario de menace | Critère | Sources de menaces | Types de menace | Menaces | Vraisemblance |
|---|---|---|---|---|---|---|
| Système d'accès (SYS_AIN) | Menace sur le réseau internet causant une indisponibilité | D | • Entreprise tierce<br>• Pirate<br>• Concurrent<br>• Employé malveillant<br>• Panne de réseau | • M15 RSX-DEP Saturation du canal informatique<br>• M16 RSX-DET Dégradation d'un canal informatique | • Blocage d'un lot d'adresses IP<br>• Occupation de la bande passante (déni de service)<br>• Rupture du canal d'accès au cloud | 4. Maximale |
| | Menace sur le réseau internet causant une | I | • Pirate<br>• Concurrent | • M13 RSX-USG Attaque du milieu sur un canal | • Attaque de type Man in the Middle | 3. Forte |

| Menace | Vulnérabilités | Pré-requis | Vraisemblance |
|---|---|---|---|
| Blocage d'un lot d'adresses IP | • Possibilité d'être impliqué dans les activités frauduleuses d'une entreprise tierce sur le cloud | • Serveurs partagés (cloud public) | 3. Forte |
| Occupation de la bande passante (déni de service) | • Réseau d'accès au cloud unique<br>• Dimensionnement insuffisant de la bande passante | • Accès à la table de routage<br>• Accès aux utilisateurs | 2. Significative |
| Rupture du canal d'accès au cloud | • Réseau d'accès au cloud unique<br>• Dimensionnement insuffisant de la bande passante | • Contrôle insuffisant du matériel<br>• Accès physique au réseau | 4. Maximale |
| Acquisition de données par écoute passive | • Réseau perméable<br>• Données transmises interprétables | • Accès à la table de routage<br>• Accès aux utilisateurs | 3. Forte |
| Attaque de type Man in the Middle | • Possibilité de falsification du service appelé<br>• Routage altérable | • Accès à la table de routage<br>• Accès aux utilisateurs | 3. Forte |

# EBIOS: Scénarios de menaces

## ❑ Types de menaces

http://www.ssi.gouv.fr/uploads/2011/10/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf

Analyser les scénarios de menaces

M1. MAT-USG – Détournement de l'usage prévu d'un matériel
M2. MAT-ESP – Espionnage d'un matériel
M3. MAT-DEP – Dépassement des limites de fonctionnement d'un matériel
M4. MAT-DET – Détérioration d'un matériel
M5. MAT-MOD – Modification d'un matériel
M6. MAT-PTE – Perte d'un matériel

M7. LOG-USG – Détournement de l'usage prévu d'un logiciel
M8. LOG-ESP – Analyse d'un logiciel
M9. LOG-DEP – Dépassement des limites d'un logiciel
M10. LOG-DET – Suppression de tout ou partie d'un logiciel
M11. LOG-MOD – Modification d'un logiciel
M12. LOG-PTE – Disparition d'un logiciel

M13. RSX-USG – Attaque du milieu sur un canal informatique ou de téléphonie
M14. RSX-ESP – Écoute passive d'un canal informatique ou de téléphonie
M15. RSX-DEP – Saturation d'un canal informatique ou de téléphonie
M16. RSX-DET – Dégradation d'un canal informatique ou de téléphonie
M17. RSX-MOD – Modification d'un canal informatique ou de téléphonie
M18. RSX-PTE – Disparition d'un canal informatique ou de téléphonie

M19. PER-USG – Dissipation de l'activité d'une personne
M20. PER-ESP – Espionnage d'une personne à distance
M21. PER-DEP – Surcharge des capacités d'une personne
M22. PER-DET – Dégradation d'une personne
M23. PER-MOD – Influence sur une personne
M24. PER-PTE – Départ d'une personne

M25. PAP-USG – Détournement de l'usage prévu d'un support papier
M26. PAP-ESP – Espionnage d'un support papier
M27. PAP-DET – Détérioration d'un support papier
M28. PAP-PTE – Perte d'un support papier

M29. CAN-USG – Manipulation via un canal interpersonnel
M30. CAN-ESP – Espionnage d'un canal interpersonnel
M31. CAN-DEP – Saturation d'un canal interpersonnel
M32. CAN-DET – Dégradation d'un canal interpersonnel
M33. CAN-MOD – Modification d'un canal interpersonnel
M34. CAN-PTE – Disparition d'un canal interpersonnel

# EBIOS: Scénarios de menaces

Evaluer chaque scénario de meance

| Vraisemblance | Scénarios de menaces |
|---|---|
| 4. Maximale | • Menace sur le réseau internet causant une indisponibilité<br>• Menace sur le système du prestataire causant une compromission |
| 3. Forte | • Menace sur le réseau internet causant une altération<br>• Menace sur le réseau internet causant une compromission<br>• Menace sur le système du prestataire causant une indisponibilité<br>• Menace sur le système du prestataire causant une altération<br>• Menace sur le réseau du prestataire causant une indisponibilité<br>• Menace sur le réseau du prestataire causant une altération<br>• Menace sur le réseau du prestataire causant une compromission<br>• Menace sur l'organisation interne causant une compromission<br>• Menace sur l'organisation du prestataire causant une compromission |
| 2. Significative | • Menace sur l'organisation interne causant une indisponibilité<br>• Menace sur l'organisation du prestataire causant une indisponibilité |
| 1. Minime | • Menace sur l'organisation interne causant une altération<br>• Menace sur l'organisation du prestataire causant une altération |

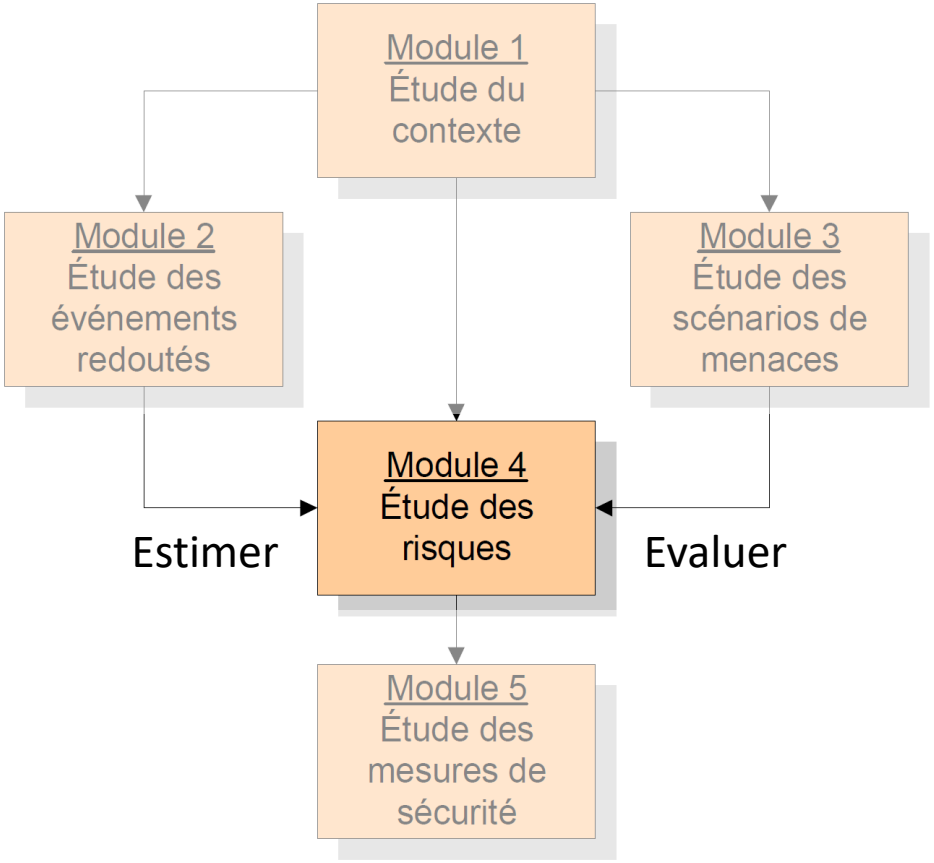
# EBIOS: Analyse de risque

Etude des scénarios de menaces

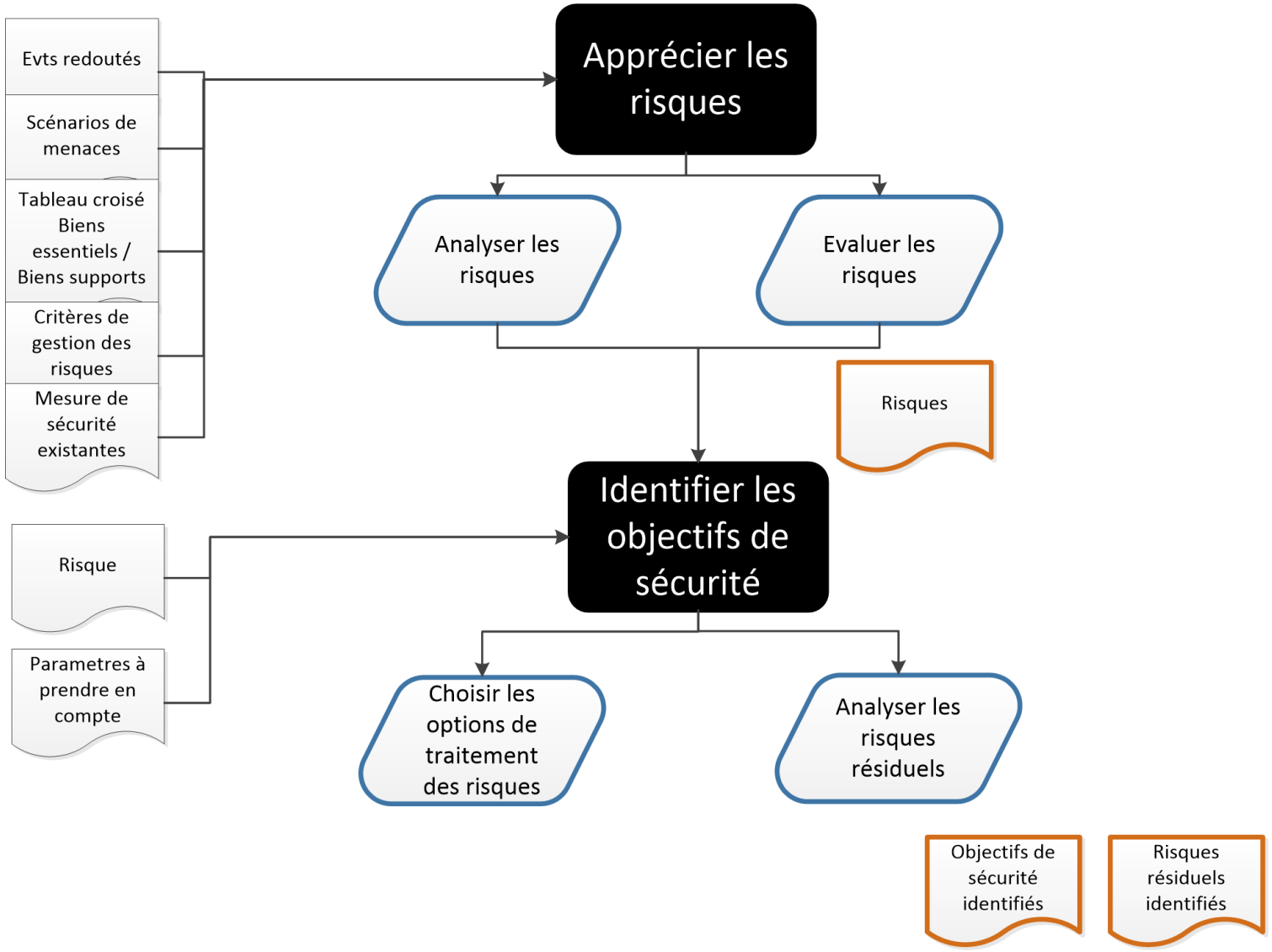
Analyser les scénarios de menaces

Evaluer chaque scénario de meance

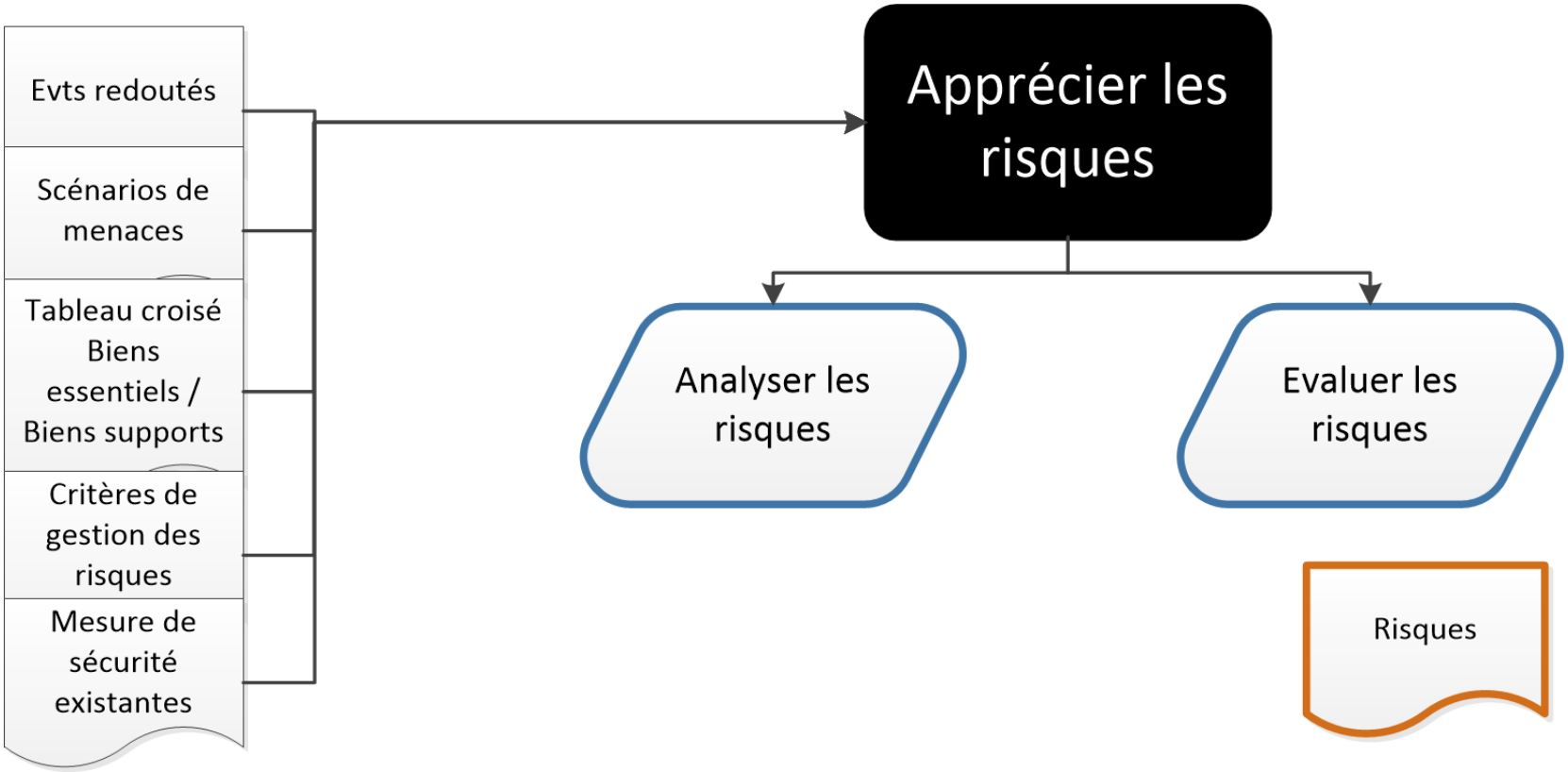
# EBIOS:



# EBIOS:


Evts redoutés
Scénarios de menaces
Tableau croisé Biens essentiels / Biens supports
Critères de gestion des risques
Mesure de sécurité existantes
Apprécier les risques
Analyser les risques
Evaluer les risques
Risques
Risque
Parametres à prendre en compte
Identifier les objectifs de sécurité
Choisir les options de traitement des risques
Analyser les risques résiduels
Objectifs de sécurité identifiés
Risques résiduels identifiés

# EBIOS: Apprécier les risques



# EBIOS: Apprécier les risques

## Activité 4.1 – Apprécier les risques

**Objectif**

Cette activité fait partie de l'appréciation des risques. Elle a pour but de mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude.

**Avantages**

- Permet de construire des scénarios de manière simple et exhaustive
- Permet de justifier de l'utilité des mesures de sécurité existantes
- Permet d'éviter de traiter des scénarios qui ne constituent pas des risques
- Permet de fournir les données nécessaires à l'évaluation des risques
- Permet de forcer les parties prenantes à s'interroger objectivement sur le niveau des risques

**Données d'entrée**

- Événements redoutés
- Scénarios de menaces
- Tableau croisé biens essentiels / biens supports
- Critères de gestion des risques
- Mesures de sécurité existantes

**Actions préconisées et rôle des parties prenantes**

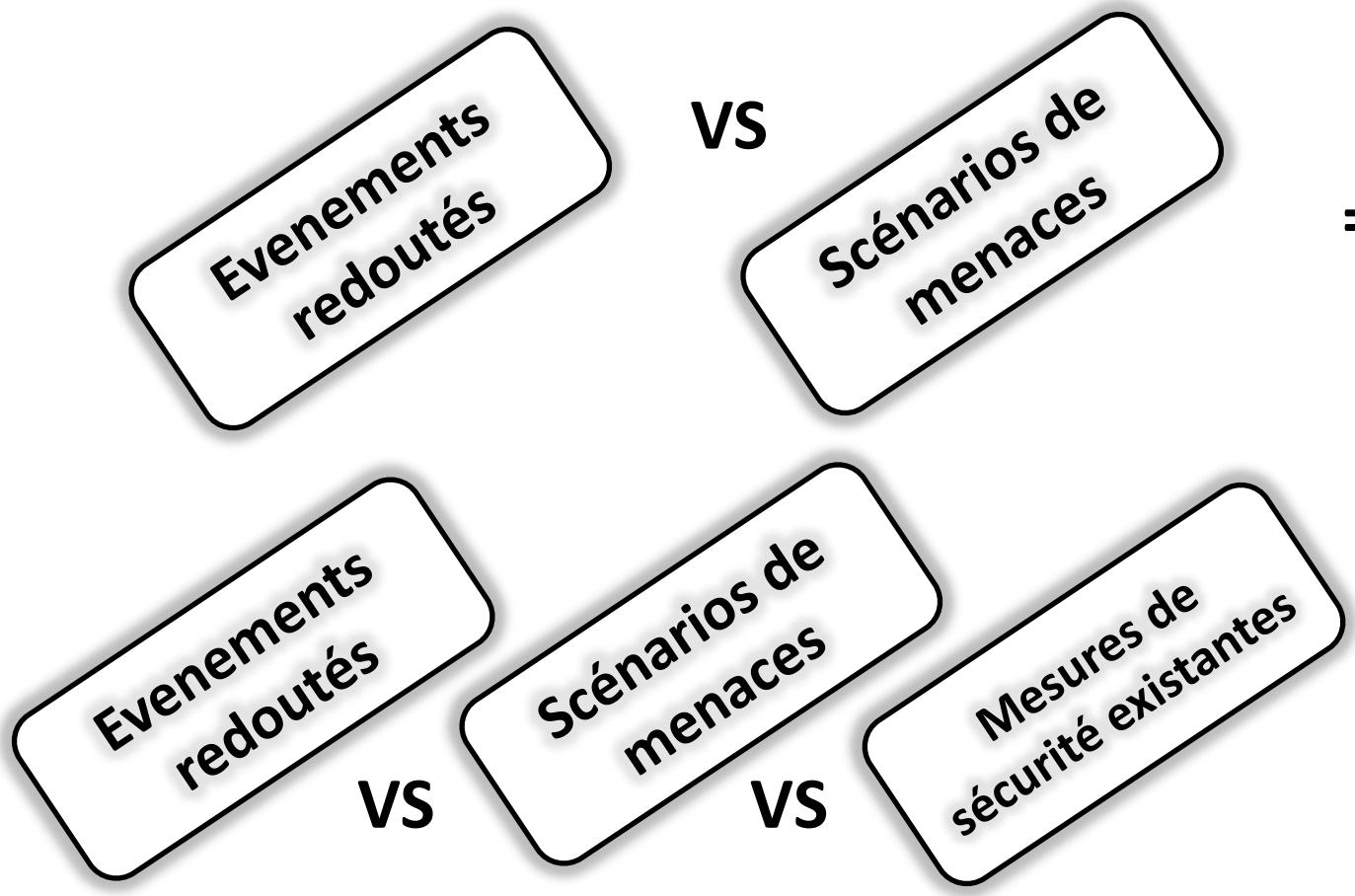
| Actions : \ Parties prenantes : | Responsable | RSSI | *Risk manager* | Autorité | Dépositaire | Propriétaire |
|---|---|---|---|---|---|---|
| Action 4.1.1. Analyser les risques | R | C | | | C | C |
| Action 4.1.2. Évaluer les risques | R | C | I | A | I | I |

**Données produites**

- Risques

# EBIOS: Apprécier les risques

Analyser les risques



# EBIOS: Apprécier les risques

## Divulgation des données de déclaration de sinistre

Analyser les risques

| N° | Evènement Redouté | Besoin | Sources de menaces | Impacts | Gravité |
|---|---|---|---|---|---|
| Données de déclaration de sinistre | | | | | |
| ER1 | Divulgation des données | Privé | • Pirate<br>• Employé du prestataire peu sérieux<br>• Employé du prestataire malveillant<br>• Bogue logiciel | • Perte de notoriété<br>• Perte de confiance vis-à-vis des clients<br>• Impossibilité de remplir des obligations légales<br>• Action en justice à l'encontre de la | 4. Critique |

| Bien support | Scénarios de menace | Critère | Sources de menaces | Types de menace | Menaces | Vraisemblance |
|---|---|---|---|---|---|---|
| Système d'accès (SYS_AIN) | Menace sur le réseau internet causant une compromission | C | • Pirate<br>• Concurrent<br>• Employé malveillant | • M14 RSX-ESP Ecoute passive d'un canal informatique | • Acquisition de données par écoute passive | 3. Forte |
| Système du prestataire (SYS_EXT) | | | | | • Collecte de données d'accès au SI externalisé<br>• Prestataire racheté par | |
| Système d'accès prestataire | prestataire | C | • Employé du prestataire | passive d'un canal | | 3. Forte |

| Menace | Vulnérabilités | Pré-requis | Vraisemblance |
|---|---|---|---|
| Acquisition de données par écoute passive | • Réseau perméable<br>• Données transmises interprétables | • Accès à la table de routage<br>• Accès aux utilisateurs | 3. Forte |
| Serveurs du prestataire saisis par la justice | • Juridiction liée à la position géographique des données | • Changement de juridiction dans le pays où sont situés les serveurs<br>Ou<br>• Une entreprise tierce mène des activités frauduleuses sur le cloud<br>Ou<br>• Juridiction relative au stockage des données personnelles | 2. Significative |
| Données rendues accessibles à d'autres utilisateurs du cloud | • Mauvaise compartimentation du logiciel | • Serveurs partagés (cloud public) ou réutilisés | 2. Significative |
| Collecte de données d'accès au SI externalisé | • SI du sous-traitant mal sécurisé<br>• Faille dans l'application | • Accès physique ou logique au SI du sous-traitant<br>• Connaissance de l'existence du logiciel<br>• Connaissance de l'existence du | 4. Maximale |

# EBIOS: Apprécier les risques

Analyser les risques

**Divulgation des données de déclaration de sinistre**

## Estimation Brute

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

Mesures de sécurité existantes

| N° | Thème ISO 27002 | Mesures de sécurité existantes | Description | Prévention | Protection | Récupération | Bien support |
|---|---|---|---|---|---|---|---|
| 1 | 9.1 Zones sécurisée | Périmètre de sécurité physique | Protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité. Les serveurs doivent être inaccessibles par des personnes non autorisées et donc dans des salles hautement sécurisées. | x | x | | Système du prestataire |
| 2 | 9.1 Zones sécurisée | Contrôle physique des accès | Protéger les zones sécurisées pas des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis. Le prestataire doit donc surveiller et contrôler les accès aux datacenters et doit s'assurer que le personnel de maintenance ou de support ne peut menacer la sécurité des données, des matériels ou des logiciels. | X | x | | Système du prestataire |
| 5 | 9.2 Sécurité du matériel | Sécurité du câblage | Protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage. | | x | | Système d'accès du prestataire |
| 6 | 10.7 Manipulation des supports | Sécurité de la documentation système | La documentation décrivant l'ensemble du système doit être gardée avec un niveau de sécurité suffisant pour ne pas permettre à des personnes malveillantes d'avoir une connaissance poussée de l'architecture (mesures de « diffusion restreinte » systématiques). | | x | | Organisation interne / Organisation du prestataire |

## Estimation Nette

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

# EBIOS: Apprécier les risques

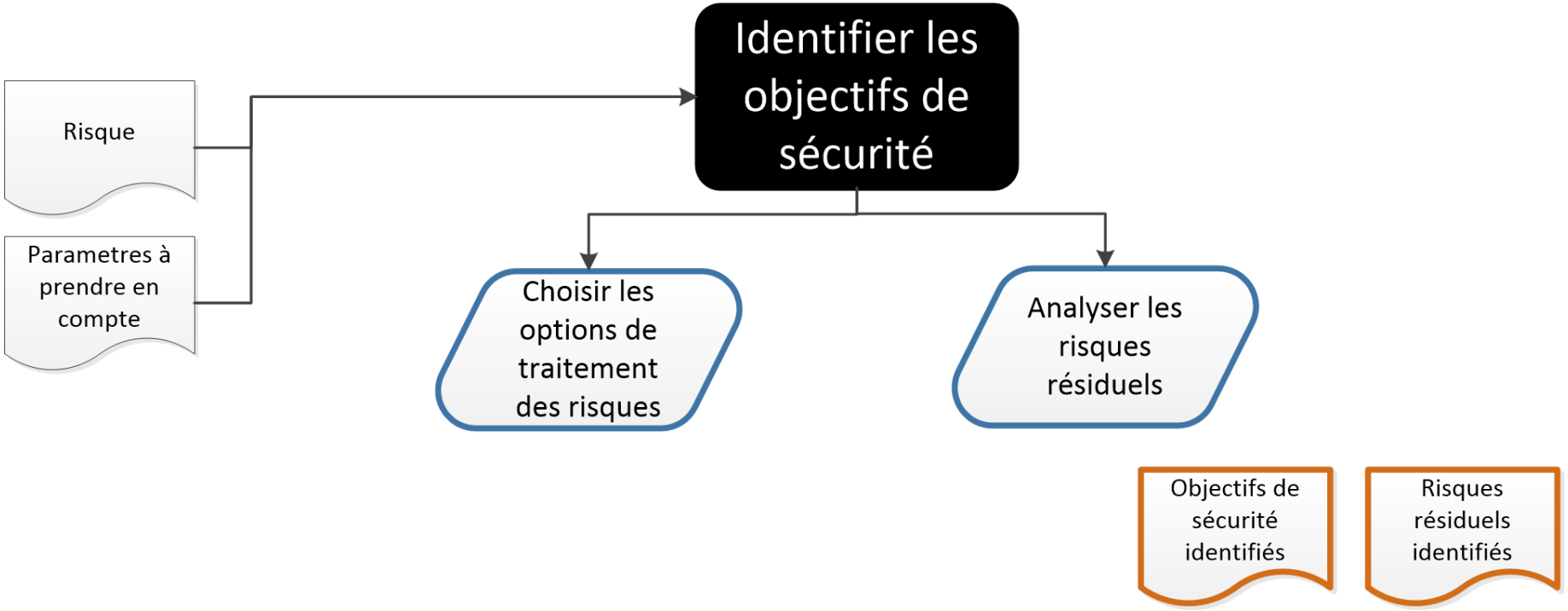
Evaluer les risques

| Gravité | 1. Minime | 2. Significative | 3. Forte | 4. Maximale |
|---|---|---|---|---|
| 4. Critiques | | Données de sécurité - Confidentialité | | |
| 3. Important | | Données de déclaration de sinistre -- Confidentialité<br>Données de déclaration de sinistre -- Intégrité<br>Données de sécurité -- Intégrité | | |
| 2. Limitée | | Données de sécurité -- Disponibilité<br>Traitement des données -- Disponibilité | Données de déclaration de sinistre -- Disponibilité | |
| 1. Négligeable | | | | |

Vraisemblance

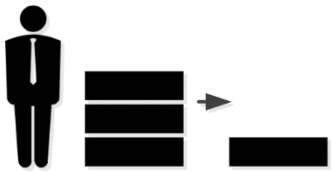
- Risque intolérable
- Risque Significatif
- Risque Négligeable

# EBIOS: Objectifs de sécurité

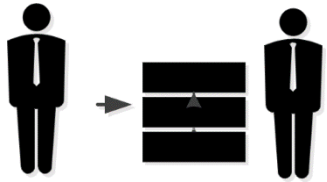


# EBIOS: Objectifs de sécurité

Choisir les options de traitement des risques

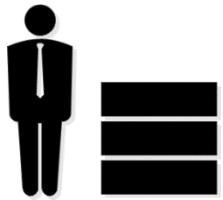


Réduire



Transférer

Eviter



Prendre

# EBIOS: Objectifs de sécurité

Choisir les options de traitement des risques

| Risque | Evitement | Réduction | Prise | Transfert |
|---|---|---|---|---|
| Divulgation des données de déclaration de sinistre | | X | | |
| Altération des données de déclaration de sinistre | | X | | |
| Indisponibilité des données de déclaration de sinistre | | X | | |
| Divulgation des données de sécurité | | X | | |
| Altération des données de sécurité | | X | | |
| Indisponibilité des données de sécurité | | X | | |
| Indisponibilité de la fonction de traitement des données de déclaration de sinistre | | X | | |

# EBIOS: Objectifs de sécurité

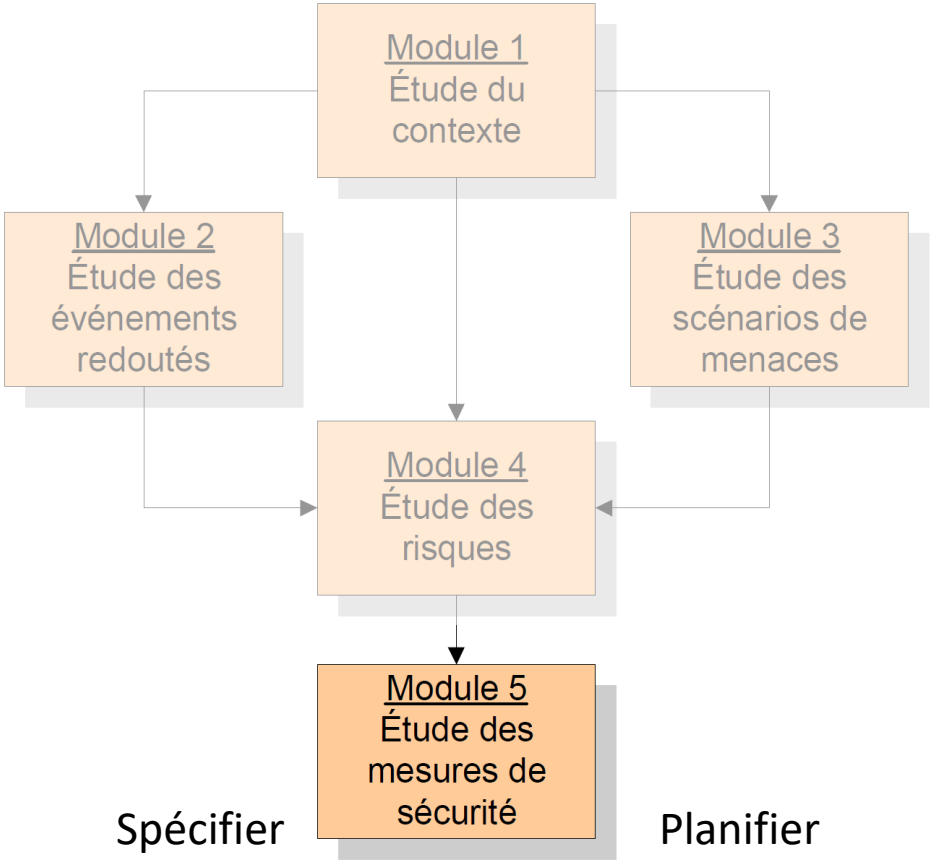
Analyser les risques résiduels

| Risques résiduels | Gravité | Vraisemblance |
|---|---|---|
| Divulgation des données de déclaration de sinistre | 2. Significatif | 2. Significatif |
| Altération des données de déclaration de sinistre | 2. Significatif | 2. Significatif |
| Indisponibilité des données de déclaration de sinistre | 3. Forte | 3. Forte |
| Divulgation des données de sécurité | 2. Significatif | 2. Significatif |
| Altération des données de sécurité | 2. Significatif | 2. Significatif |
| Indisponibilité des données de sécurité | 2. Significatif | 3. Forte |
| Indisponibilité de la fonction de traitement des données de déclaration de sinistre | 3. Forte | 3. Forte |

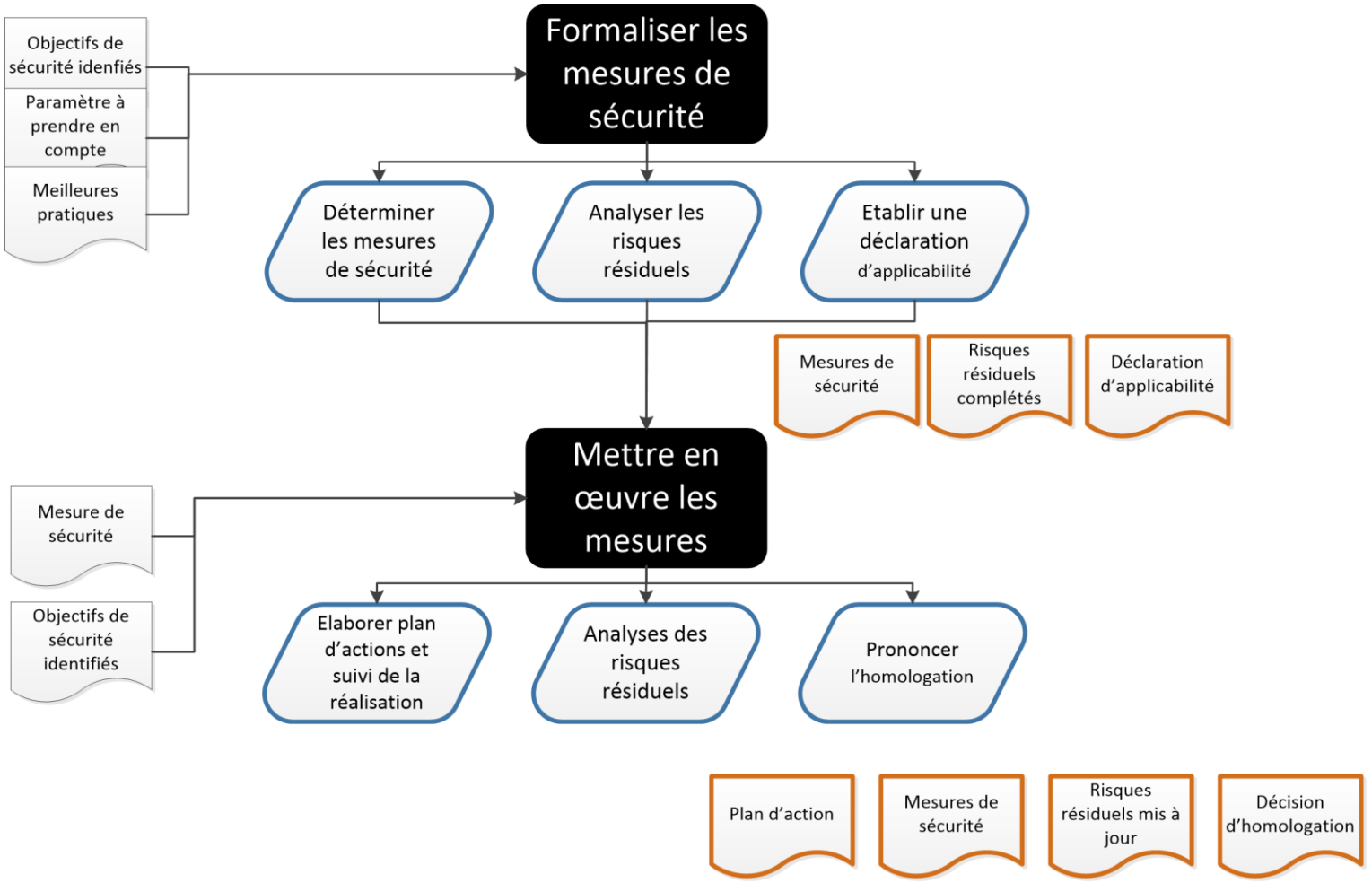
# EBIOS: Analyse de risque

- Apprécier les risques
  - Analyser les risques
  - Evaluer les risques
- Identifier les objectifs de sécurité
  - Choisir les options de traitement des risques
  - Analyser les risques résiduels

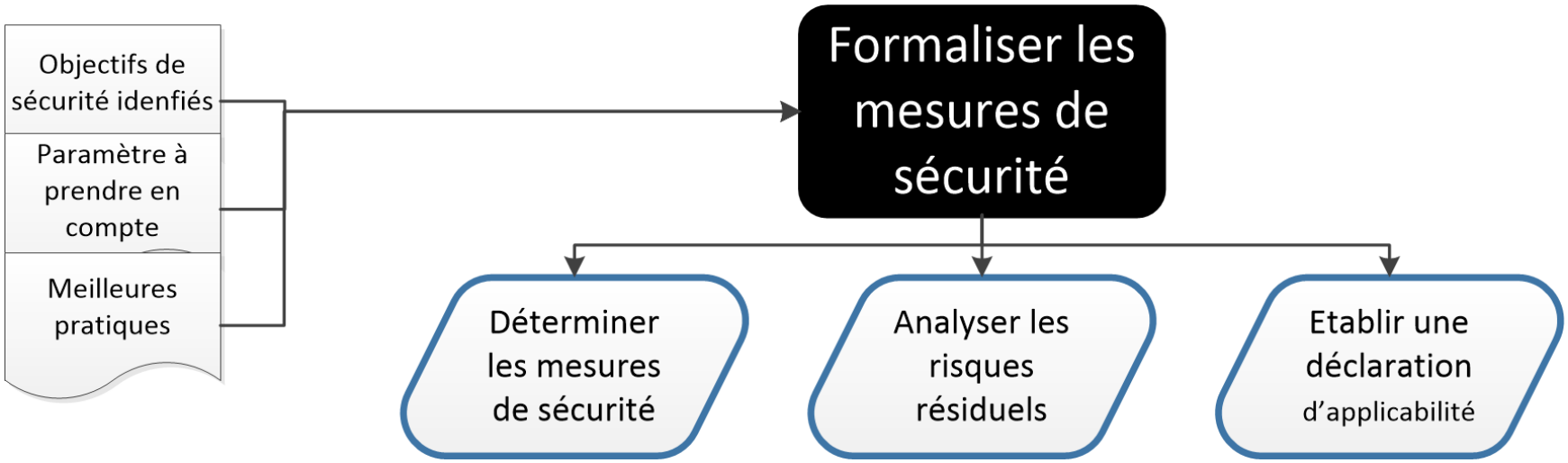
# EBIOS:



# EBIOS: Mesures de sécurité



# EBIOS: Mesures de sécurité

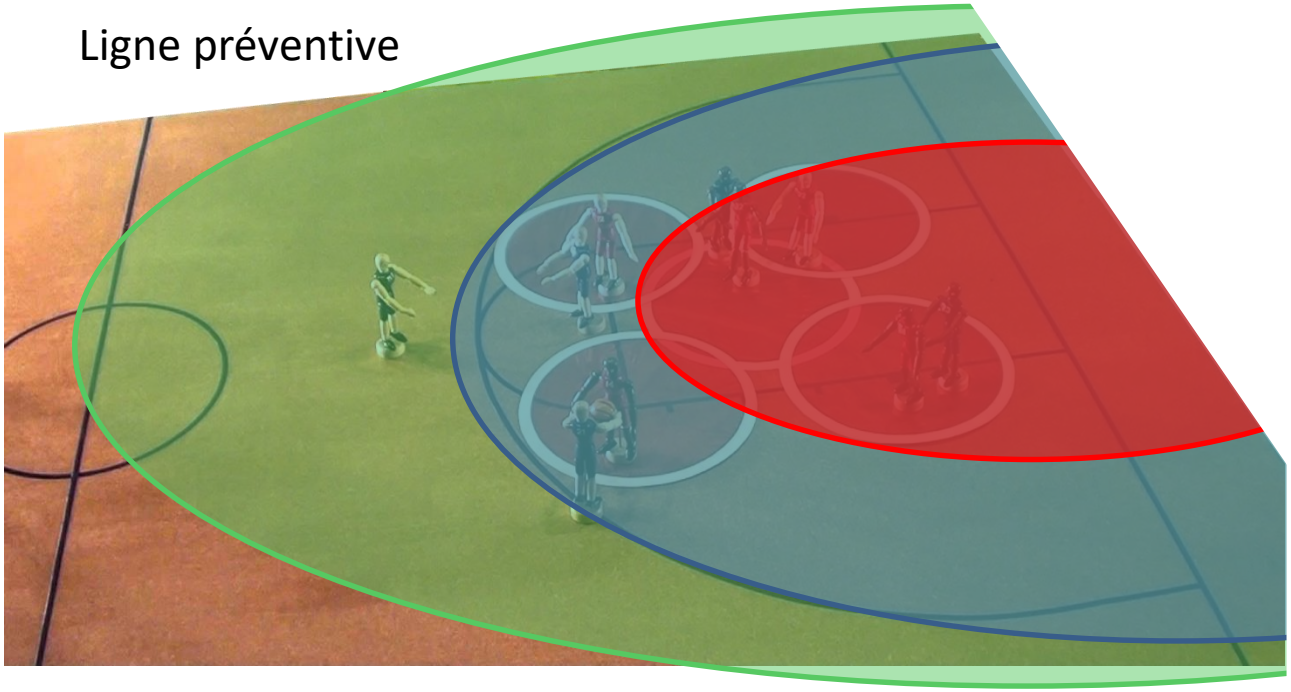


# EBIOS: Mesures de sécurité

Analyser les risques résiduels

Ligne Récupératrice

Ligne préventive



Ligne Défensive

# EBIOS: Mesures de sécurité

Déterminer les mesures de sécurité

| N° | Thème ISO 27002 | Mesure de sécurité | Description | Prévention | Protection | Récupération | Bien support |
|---|---|---|---|---|---|---|---|
| 1 | 6.1 Organisation interne | Attribution des responsabilités en matière de sécurité de l'information | Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information. La répartition des responsabilités entre le personnel interne et le personnel du prestataire doit être formalisée et respectée. | x | | | Organisation interne / Organisation externe |
| 2 | 8.2 Pendant la durée du contrat | Sensibilisation, qualification et formations en matière de sécurité de l'information | Le personnel interne doit être formé aux bonnes pratiques de sécurité. Il doit avoir un niveau de sensibilisation pertinent pour ses fonctions. Cela passe par des sessions de formation et des missives d'information concernant la sécurité. | x | x | | Organisation interne |
| 3 | 8.2 Pendant la durée du contrat | Procédures disciplinaires | Mettre en place un processus disciplinaire clair pour toute ayant enfreint les règles de sécurité pour réduire les risques d'influence et de corruption. Par exemple, les sanctions peuvent être précisées dans une charte définissant les engagements de responsabilités. | x | x | | Organisation interne |
| 4 | 8.3 Fin ou modification de contrat | Retrait des droits d'accès | Les droits d'accès de tout utilisateur ou administrateur aux données et aux logiciels doivent être supprimés en fin de contrat ou doivent être modifiés en cas de changement de contrat ou de responsabilités. | x | | | Organisation interne |
| 5 | 9.2 Sécurité du matériel | Mise au rebut ou recyclage sécurisé du matériel | Vérifier tout le matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut. Le prestataire devra préciser les mesures mises en œuvre pour assurer la mise au rebut de ses matériels. | x | x | | Système du prestataire |
| 6 | 10.2 Gestion de la prestation de service par un tiers | Prestation de service et contrat | S'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. Notamment, le contrat de prestation de service doit inclure les éléments liés à la journalisation d'évènements, au suivi du service hébergé (mise à jour, maintenances, sauvegardes…), aux modalités de prévention | | | | Système du prestataire |

# EBIOS: Mesures de sécurité

Analyser les risques résiduels

*Divulgation des données de déclaration de sinistre*

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

*Indisponibilité des données de déclaration de sinistre*

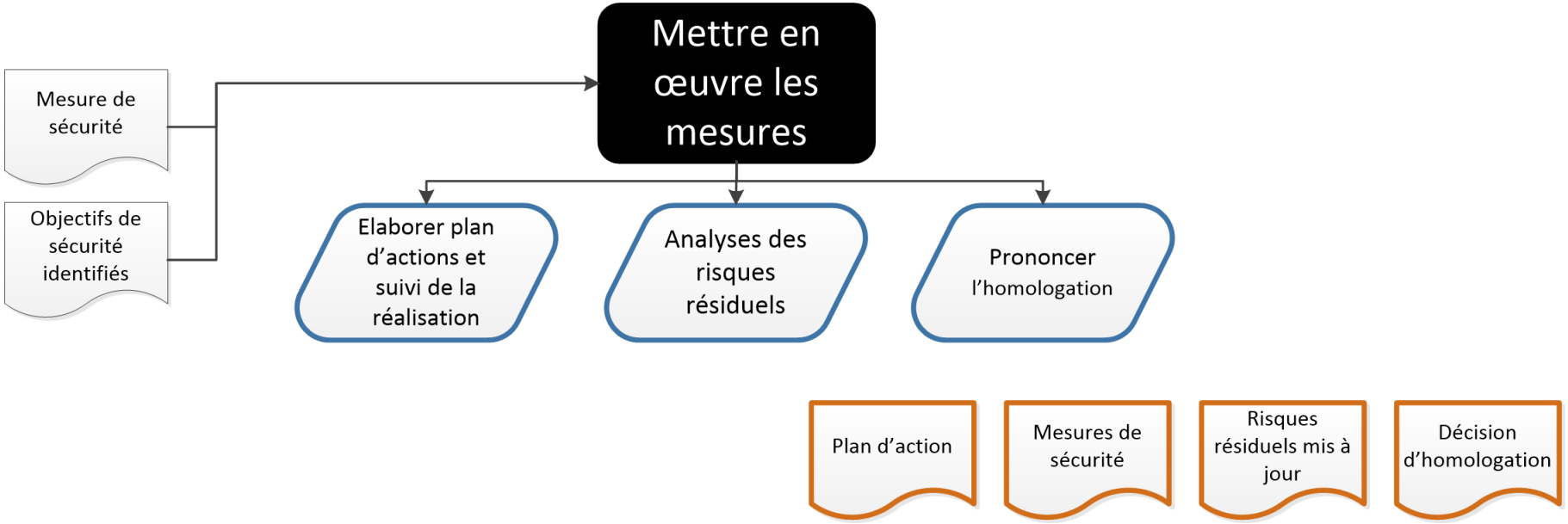
| **Niveau de risque** | 1. Négligeable | **2. Limité** | ~~3. Significatif~~ | 4. Intolérable |
|---|---|---|---|---|
| **Gravité** | 1. Négligeable | **2. Limitée** | 3. Importante | 4. Critique |
| **Vraisemblance** | 1. Minime | **2. Significative** | ~~3. Forte~~ | 4. Maximale |

# EBIOS: Mesures de sécurité

Etablir une déclaration d'applicabilité

| Type | Paramètre | Justification | Etat |
|---|---|---|---|
| Hypothèses | Le datacenter du prestataire comporte toutes les mesures de sécurités nécessaires (accès physique controllé, matériel non soumis aux menaces environnementales, réseau électrique de secours, réseau de communication protégé...) | | Satisfait |
| Hypothèses | Les postes de travail du prestataire sont sécurisés et ne présentent pas de vulnérabilité. Ils ne sont pas retenus comme bien support. | | Satisfait |
| Hypothèses | Les postes de travail internes sont sécurisés et ne présentent pas de vulnérabilité. Ils ne sont pas retenus comme bien support. | | Satisfait |
| Références communautaires, légales et réglementaires à appliquer | Respect des règles fixées par la CNIL relative à la protection des données à caractère personnel. | | Prévu |

# EBIOS: Mesures de sécurité



# EBIOS: Mesures de sécurité

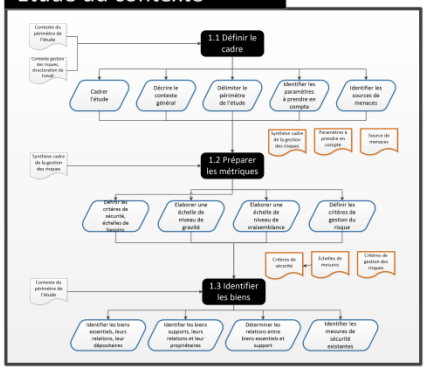
Elaborer plan d'actions et suivi de la réalisation

| Mesure de sécurité | Responsable | Bien Support | Risque | Ind<br>Stade d'applicat |
|---|---|---|---|---|
| Adopter une démarche globale | | | | |
| Adapter la SSI selon les enjeux | | | | |
| Gérer les risques SSI | | | | |
| Élaborer une politique SSI | | | | |
| Utiliser les produits et prestataires labellisés SSI | | | | |
| Viser une amélioration continue | | | | |
| Des efforts proportionnés aux enjeux SSI | | | | |
| Un engagement systématique: l'homologation de sécurité | | | | |
| Des outils ciblés pour les projets de système d'information | | | | |
| Utilisation de mécanismes cryptographiques | | | | |
| Utilisation des identifiants / mots de passe statiques | | | | |
| Authentification d'une personne par certificat électronique | | | | |
| Authentification d'un serveur par certificat électronique | | | | |
| Utilisation de mécanismes cryptographiques | | | | |
| Signature d'une personne par certificat électronique | | | | |
| Cachet d'un serveur par certificat électronique | | | | |
| Utilisation de mécanismes cryptographiques | | | | |
| Confidentialité par certificat électronique | | | | |
| Habilitations | | | | |
| Utilisation des mécanismes cryptographiques | | | | |
| Horodatage par contremarques de temps | | | | |
| Règles de sécurité | | | | |
| Qualification élémentaire | | | | |
| Qualification standard | | | | |

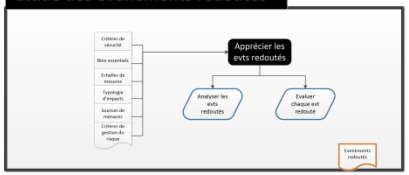
CPE LYON
ÉCOLE SUPÉRIEURE DE CHIMIE PHYSIQUE ÉLECTRONIQUE DE LYON

# EBIOS: Sum UP

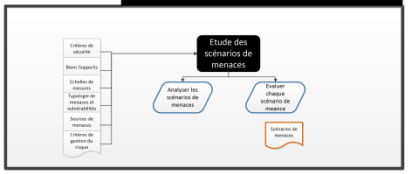
Etude du contexte



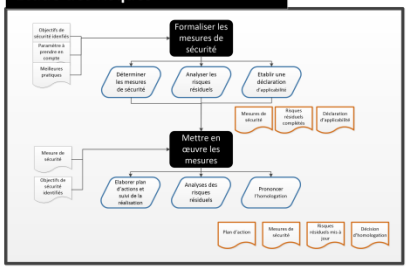

Etude des évènements redoutés



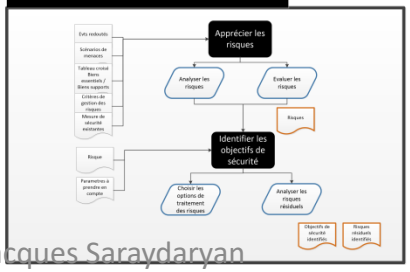

Etude des scénarios de menaces




Etude des risques




Etude des mesures de sécurité



# References


- http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/
- http://eduscol.education.fr/ecogest/si/SSI/risk_conf
- Point Sur les méthodes de sécurité, CLUSIR, 2004
- Gérer les risques [EBIOS] [ARS 2011 –risques en environnement santé], Assistance Publique Hopitaux de Marseille, 2011
- The Global Risks Report 2016, World Economic Forum, 2016
- Allianz Risk Barometer Top Business Risks 2016
- CISSP, Exam Guide, Shon Harris, 2009
- http://www.ssi.gouv.fr/administration/bonnes-pratiques/

ÉCOLE SUPÉRIEURE
DE CHIMIE PHYSIQUE ÉLECTRONIQUE
DE LYON

# Jacques Saraydaryan

Jacques.saraydaryan@cpe.fr