

R5.B.09 – CYBERSÉCURITÉ

PARTIE III

Edward Staddon

Edward.Staddon@univ-ubs.fr

Université Bretagne Sud, IUT de Vannes, Département Informatique

PLAN DU COURS

- Introduction à la cybersécurité
- Les risques de la cyber espace
- Les cyberattaques
- Protection préventive
- Protection active et anticipative
- Architectures de sécurité et architectures sécurisés
- Introduction à l'analyse de risque

PLAN DU COURS

- Introduction à la cybersécurité
- Les risques de la cyber espace
- Les cyberattaques
- Protection préventive
- Protection active et anticipative
- Architectures de sécurité et architectures sécurisés
- Introduction à l'analyse de risque } PARTIE III

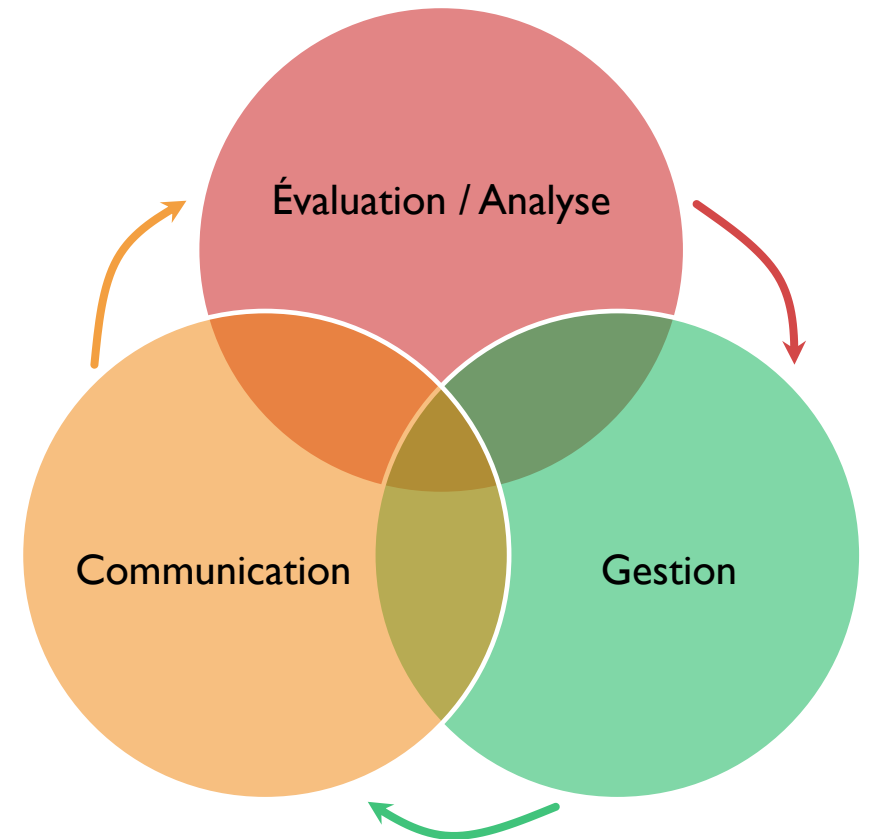


INTRODUCTION À L'ANALYSE DE RISQUES

KÉSAKO ?

Processus visant à mitiger l'impact de risques cyber

- Utilisé pour protéger contre les potentiels menaces
 - Minimise la vulnérabilité contre les évènements inattendus
- Processus multi-étape
 - **Évaluation des risques** → Identification des dangers
 - **Gestion des risques** → Politiques et gestion des décisions
 - **Communication des risques** → Echange d'informations concernant les risques



TYPES D'ANALYSE DE RISQUE

Analyse bénéfice-risque et coût-bénéfice

- Bénéfice-Risque
 - Peser les pour/contre (bénéfices/risques) d'une action
 - Classés selon leur impact et taux de réussite
- Coût-Bénéfice
 - Analyse des coûts estimés d'une action
 - Comparaison contre les potentiels bénéfices et opportunités

Évaluation des besoins

- Identification et évaluation des besoins et lacunes
- Donne une idée des manques et aide la réorientation des ressources pour atteindre les objectifs efficacement

Analyse de l'impact sur l'entreprise - BIA

- Anticiper les perturbations opérationnelles par des facteurs externes
 - Catastrophes naturelles
- Bases de l'investissement dans les stratégies de récupération, prévention et mitigation

Analyse des modes de défaillances, de leurs effets et de leur criticité - FMEA

- Méthode d'anticipation des défaillances et la mitigation de l'impact sur la clientèle
- Améliore la fiabilité des produits et services rendus
- Réduit le coût des défaillances

Analyse de cause racine

- Identification et élimination des causes racines pour résoudre des problèmes
- Aide dans la prévention des problèmes récurrents
- Cible les systèmes inefficaces d'origine

MÉTHODOLOGIES

Analyse Qualitative

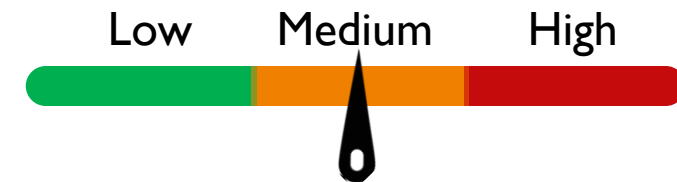
- Évaluation et classement des risques sur des critères
 - Sévérité
 - Probabilité de conséquences
- **Obtenir une liste de menaces prioritaires**
- Décrit comme la première ligne de défense du chef de projet
 - Aide à identifier les détracteurs potentiels
 - Ciblant les risques les plus dangereuses
 - Plus efficace et meilleure gestion du temps

Analyse Quantitative

- Calcule des risques basés sur un ensemble de données
- **Spécifier le cout d'impact sur l'entreprise**
- Analyse des données au préalable
 - Sur une longue période temporelle
 - Observation dans plusieurs scenarios
- Ex: 5 derniers projets
 - Machine A en panne après 7h de travail
- Assomption de 100% de risque pour 8h de travail sur la machine A

DIFFÉRENCES MAJEURES

- Bases d'évaluation différentes
 - **Qualitative** → basé sur la perception ou jugement d'une personne
 - **Quantitative** → basé sur l'analyse de données spécifiques et validés
- Différentes valeurs associées aux risques
 - **Qualitative** → classement / scores des risques
 - Ex. Score « Basse » ou 1 pour un risque mineur, pas urgent
 - **Quantitative** → pourcentage de probabilité d'occurrence du risque ou effet négative spécifique
 - Ex. Machine A



EXEMPLE QUALITATIVE

Changement de perception

- Pas de protection sur une machine de production
 - Pas d'accidents / pas de danger
 - *Classement initiale de risqué de basse importance*



- Plusieurs accidents
 - Cause trace au manque de protection
 - *Augmentation du niveau de risqué a moyenne*

Identification d'un nouveau risque

- Début d'un nouveau projet
 - Équipement en bonne état
 - *Seul risque identifiable est le manque de formation*



- Organisation des séances de formation
 - Ouvriers utilisent l'équipement plus régulièrement
 - *Équipement en mauvaise condition et peut dysfonctionner*

EXEMPLE QUANTITATIVE

Grande quantité de données de risque

- Planification d'un nouveau projet important pour l'année suivante
 - Récupération de données sur
 - les risques
 - Leur impact sur le projet
 - Leur cout de mitigation



- *Assez de données pour l'analyse l'année suivante*

Besoin de validation de l'analyse qualitative

- Pendant l'analyse qualitative
 - Tous les risques ont été classés au score maxi
 - Risques très importants
-
- Besoin d'une validation de l'impact de chaque risque
 - Justification du temps et ressources alloués

LES ÉTAPES D'UNE ANALYSE QUALITATIVE

4 étapes d'analyse

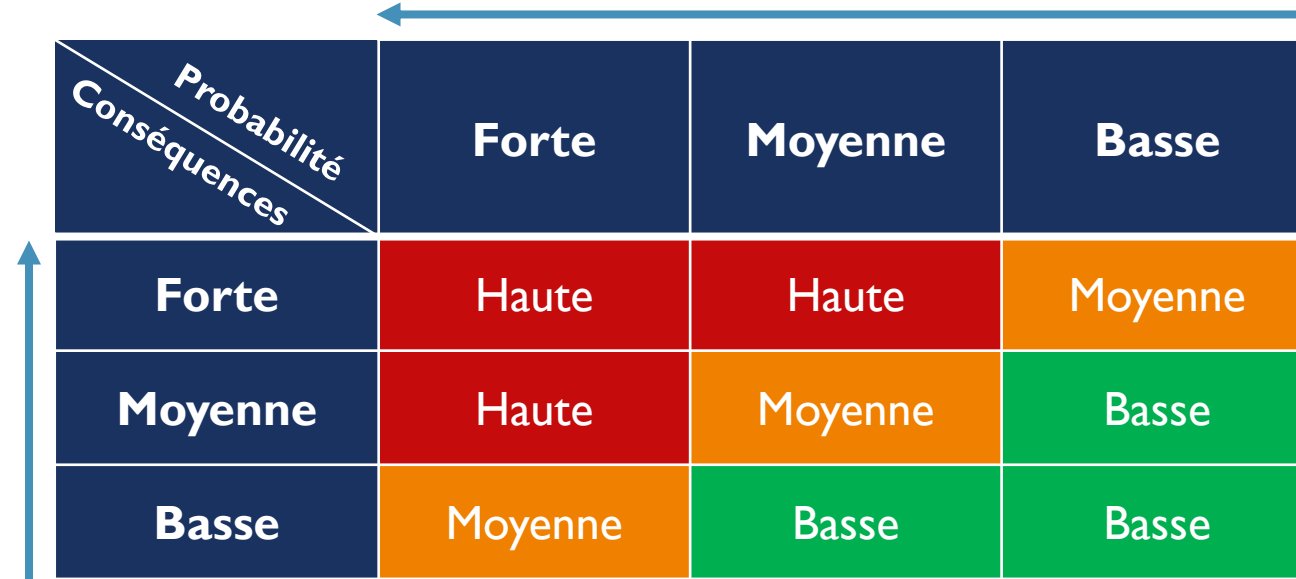
1. Identification des Risques

- Création d'une liste de risques
- Sessions de brainstorming
- Discussion avec les personnes concernées

2. Classification des Risques

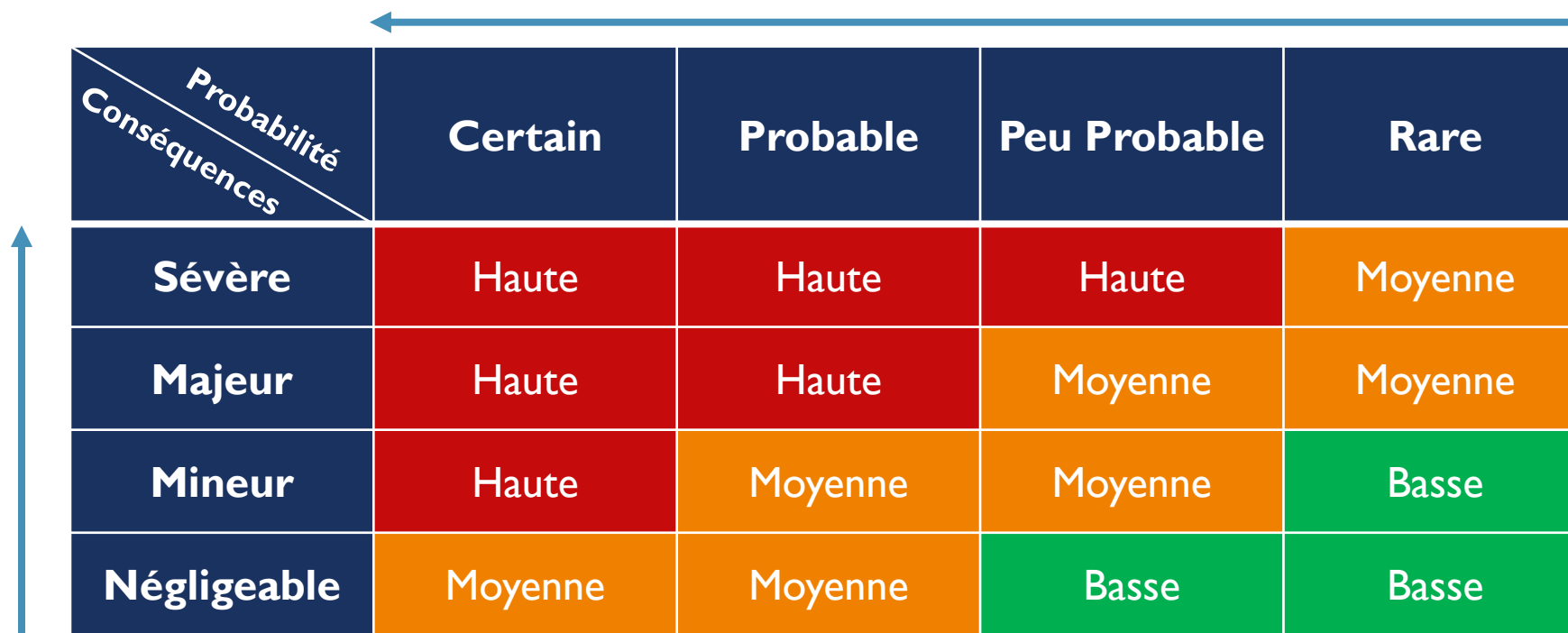
- Plusieurs techniques
 - Plus courant : utilisation d'une matrice de risque
 - Combinaison de la sévérité et probabilité de se produire
 - Plusieurs tailles → 3x3, 4x4, 5x5, ... 7x7, ...
 - Autres méthodes

MATRICE DE RISQUE – 3 X 3



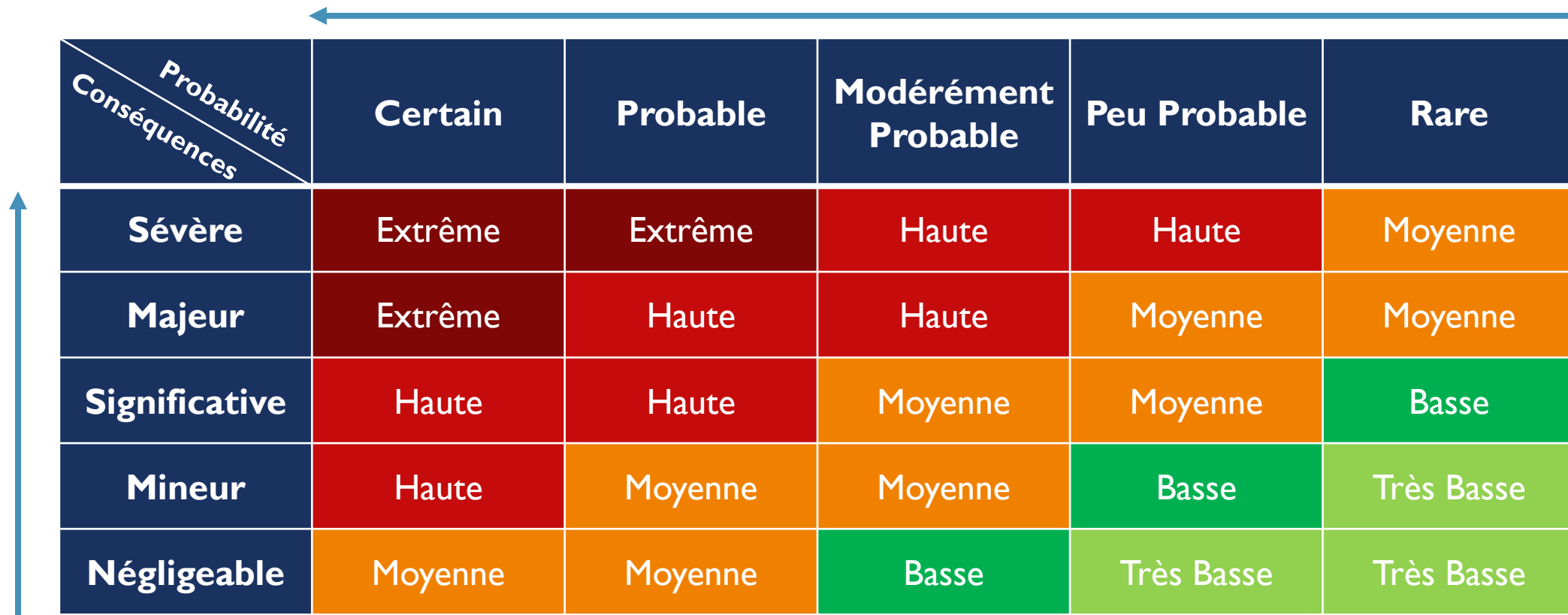
Probabilité Conséquences	Forte	Moyenne	Basse
Forte	Haute	Haute	Moyenne
Moyenne	Haute	Moyenne	Basse
Basse	Moyenne	Basse	Basse

MATRICE DE RISQUE – 4 X 4



Probabilité Conséquences	Certain	Probable	Peu Probable	Rare
Sévère	Haute	Haute	Haute	Moyenne
Majeur	Haute	Haute	Moyenne	Moyenne
Mineur	Haute	Moyenne	Moyenne	Basse
Négligeable	Moyenne	Moyenne	Basse	Basse

MATRICE DE RISQUE – 5 X 5



<div> <div>Conséquences</div> <div>Probabilité</div> </div>	Certain	Probable	Modérément Probable	Peu Probable	Rare
Sévère	Extrême	Extrême	Haute	Haute	Moyenne
Majeur	Extrême	Haute	Haute	Moyenne	Moyenne
Significative	Haute	Haute	Moyenne	Moyenne	Basse
Mineur	Haute	Moyenne	Moyenne	Basse	Très Basse
Négligeable	Moyenne	Moyenne	Basse	Très Basse	Très Basse

MATRICE DE RISQUE – 5 X 5

1 – 4	Acceptable	Pas d'actions nécessaires
5 – 9	Adéquante	Analyse approfondie possible
10 – 16	Tolérable	Revue rapide et réponse nécessaire
17 – 25	Inacceptable	Besoin d'action immédiate et cessation d'activité

<div> <div>Probabilité</div> <div>Conséquences</div> </div>	5 Certain	4 Probable	3 Modérément Probable	2 Peu Probable	1 Rare
5 Sévère	25 Extrême	20 Extrême	15 Haute	10 Haute	5 Moyenne
4 Majeur	20 Extrême	16 Haute	12 Haute	8 Moyenne	4 Moyenne
3 Significative	15 Haute	12 Haute	9 Moyenne	6 Moyenne	3 Basse
2 Mineur	10 Haute	8 Moyenne	6 Moyenne	4 Basse	2 Très Basse
1 Négligeable	5 Moyenne	4 Moyenne	3 Basse	2 Très Basse	1 Très Basse

LES ÉTAPES D'UNE ANALYSE QUALITATIVE

4 étapes d'analyse

1. Identification des Risques

- Création d'une liste de risques
- Sessions de brainstorming
- Discussion avec les personnes concernées

2. Classification des Risques

- Plusieurs techniques
 - Plus courant : utilisation d'une matrice de risque
 - Combinaison de la sévérité et probabilité de se produire
 - Plusieurs tailles → 3x3, 4x4, 5x5, ... 7x7, ...
 - Autres méthodes

3. Control des Risques

- Deux catégories
 - Cibler les causes racines → dangers, gestion inefficace
 - Réduction de l'impact négative → actions de corrections

4. Surveillance des Risques

- S'appuie sur les 3 étapes précédents
- Observation des risques
 - Est-ce que le control est efficace ?
 - Est-ce que la classification était correcte ?
 - Est-ce que tous les menaces ont été identifiés

LES ÉTAPES D'UNE ANALYSE QUANTITATIVE

4 étapes d'analyse

1. Identification de l'Objectif, Portée, Méthode

- Définition de l'aperçu cherché
- Spécification du type de données concernés
- Plusieurs méthodes d'approche
 - **FMEA** → Failure Mode and Effects Analysis
 - **BIA** → Business Impact Analysis
 - **EMV** → Expected Monetary Value

2. Préparation des Données, Outils et Personnes Concernés

- Organisation et vérification de compatibilité des données
- Utilisation d'outils avec des templates → logiciel de suivi GPS
- Possibilité d'utiliser des personnes extérieurs (entreprise / équipe / département)

3. Application de la Méthode Choisi aux Données

- Application des méthodes sélectionnés
 - Utilisation des templates si disponibles (FMEA / BIA)
 - $EMV = P_{risque} \times C_{impact}$

4. Enregistrer et Stocker les Résultats

- Stockage sécurisé des données
 - Concerne données non utilisés pour l'analyse
 - Utilisable pour les analyses futures
 - Ne pas gaspiller le travail et temps consacré

GESTION ET COMMUNICATION DES RISQUES

- Gestion des risques est une notion importante
- Beaucoup de méthodes et d'approches possibles
- Besoin d'une base commune internationale
 - **Spécification de la norme ISO 31000**
 - **Management du risque – Principes et lignes directrices**
 - Publié 2009 → mise à jour 2018
- 2 autres membres de la famille ISO 31000
 - *ISO/CEI 31010:2009* → Gestion des risques – Techniques d'évaluation des risques
 - *ISO Guide 73:2009* → Management du risque - Vocabulaire
- Contient trois composants
 - **Principes** → Soutenir un système de gestion dynamique en amélioration permanente, customisable, innovateur, structuré et inclusive
 - **Framework** → Intégration proactive du management des risques sur tous les niveaux
 - **Processus** → Mise en place systématique des politiques et pratiques supportant la communication ouverte, consultation et rapport sur les risques

LES PRINCIPES DU MANAGEMENT DES RISQUES

→ 11 principes

1. Création de la valeur et la préserve
 - Contribue à l'atteinte des objectifs, amélioration des perfs, révision gestion et processus
2. Intégration aux processus d'organisation
 - Intégré dans le système de gestion existant du niveau stratégique à l'opérationnel
3. Intégration aux processus de prise de décision
 - Aide à la décision pour des choix argumentés, définir des priorités et actions plus appropriés
4. Traitement explicite de l'incertitude
 - Outils de réduction / financement des risques pour maximiser le succès et minimiser les possibilités de pertes
5. Systématique, structuré et utilisé en temps utile
 - Cohérents pour assurer l'efficacité, pertinence, cohérence et fiabilité des résultats
6. S'appuie sur la meilleure information disponible
 - Considération et compréhension de toutes les infos disponibles et pertinents, avec les limites des données et modèles
7. Adapté
 - En fonction des ressources disponibles (personnel/finance/temps) et de l'environnement (interne/externe)
8. Intégration des facteurs humains et culturels
 - Reconnaître la contribution des personnes, facteurs culturels
9. Transparent et participatif
 - Implication des parties prenantes, internes et externes pour reconnaître l'importance de la communication et la consultation lors des étapes d'identification, évaluation et traitement des risques
10. Dynamique, itératif et réactif au changement
 - Flexible, adapter au contexte interne et externe, surtout avec des risques nouvelles, modifiés, disparus
11. Faciliter l'amélioration continue de l'organisation
 - Maturité en matière de gestion, investissement long terme, démontrant une réalisation régulière des objectifs

IMPLÉMENTATION ISO 31000

- Adaptation de la norme aux
 - Besoins spécifiques
 - Buts principaux
 - Objectifs
- Implémentation flexible et adaptable
 - Mise à jour lorsque les circonstances évoluent
- Compréhension claire sur les risques et leur impact entre
 - Dirigeants
 - Parties prenantes
 - Employés
- Utilisation de trois activités
 - **Évaluation des risques**
 - Identifier, analyser et évaluation
 - **Traitement des risques**
 - Sélectionner et implémenter des options pour répondre aux risques
 - **Surveillance et examination**
 - Assurer la qualité et efficacité du processus de gestion de risque
 - **Enregistrement et rapport**
 - Communication sur le résultat des activités
 - Être une base du processus de décisions
 - Amélioration continue du processus de gestion des risques

EBIOS - EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ

- Méthode d'évaluation des risques en informatique
 - Développé par la DCSSI 1995 → ANSSI
 - Permet l'identification des risques SSI
 - Contribue au traitement des risques
 - Spécifie les exigences de sécurité à implémenter
 - Préparation du dossier de sécurité et de communication des risques
 - Compatible avec les normes
 - **ISO 15408** – *Critères communs*
 - **ISO/CEI 27005** – *Évaluation des risques du SI*
 - **ISO 31000** – *Management des risques d'entreprise*
 - Risques non couverts → vulnérabilités
- Cinq étapes de démarche
 - **Étude du contexte**
 - Étude de l'organisme, système cible et détermination de la cible de l'étude de sécurité
 - **Étude des événements redoutés**
 - Réalisation des fiches de besoins et leur synthèse
 - **Étude des scénarios de menaces**
 - Étude des origines des menaces, des vulnérabilités et leur formalisation
 - **Étude des risques**
 - Confrontation des menaces aux besoins, formalisation des objectifs et détermination des niveaux de sécurité
 - **Étude des mesures de sécurité**
 - Mise en œuvre des démarches et démonstration de leur couverture

EBIOS - EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SÉCURITÉ

Avantages

- Méthode claire et universelle
- Étude des risques à 360 degrés
- Approche exhaustive
- Cibler rapidement sur les « biens sensibles »
- Démarche adaptative

Inconvénients

- Ne fournit pas de recommandations ni de solutions immédiates
- Pas d'audit et d'évaluation de la méthode utilisé
- N'identifie pas les scénarios d'attaque, que les types de risques
- Beaucoup de méthodes d'analyse de risques et d'audit SSI

MEHARI – MÉTHODE HARMONISÉE D'ANALYSE DES RISQUES

- Méthode de gestion de risque informatique
 - Développé par le CLUSIF en France → Continué par le CLUSIQ au Canada
- Permet l'identification des risques liés aux données, systèmes et processus d'information
 - Pas seulement l'informatique
- Aligné avec les normes
 - **ISO/CEI 27001** – *Systèmes de gestion de sécurité de l'information - Exigences*
 - **ISO/CEI 27002** – *Code de bonne pratique pour le management de la sécurité de l'information*
 - **ISO/CEI 27005** – *Techniques de sécurité*
 - **NIST SP 800-30** – *Cadre d'évaluation des risques*
- Contient plusieurs activités et outils d'analyse et de gestion
 - Analyse des menaces
 - Identification et mapping des actifs d'organisation, humain et technique
 - Identification des actifs selon les trois critères de sécurité
 - Considération de la probabilité de menaces représentatifs
 - Analyse et évaluation de la sévérité des risques
 - Évaluation des capacités des méthodes de mitigation actuels
 - Étude du niveau de sévérité de chaque scénario de risque
 - Définition des plans d'action et des projets de sécurité

REMERCIEMENTS

■ **Maxime DUMOUSSAUD**

- Consultant en gestion de crise cyber – *Sopra Steria*
- Parcours géopolitique spécialisé cyber
- Certifié des normes ISO 27001 et 27005
- Analyse de risques – Méthode EBIOS RM

■ **Emilie BOUT**

- Doctorat en Cybersécurité
- Spécialiste dans les attaques sans-fil
- Concepteur de formations et modules d'évaluation – *Tornado.io*

