Analyse de risques Informatiques

Méthode et approche pragmatique

Auteur : Pascal MARY

Ajouts et annexes : Gabriel BETETA

Analyse de risques Informatique
Objectif du cours

Le but de ce cours est d'apporter un éclairage suffisant dans la compréhension des enjeux d'une analyse de risques informatiques et plus particulièrement adapté aux traitement des menaces cyber pour des experts en technologies des systèmes d'informations.

Il fournira une compréhension :

- des notions de base d'une analyse de risque informatique.
- sur une approche pragmatique et simplifiée du traitement des risques informatiques.
- d'outils simplifiés pour une première mise en œuvre.

L'objectif est avant tout de fournir des éléments de compréhension sur la raison d'être et l'interprétation de résultats d'une analyse.

L'objectif n'est pas :

- de comprendre les détails et cheminement imposés par certaines normes.
- d'aborder les aspects financiers en détails.
- de traiter les sujets PRA/PCA (Plan de Reprise d'Activité / Plan de Continuité d'Activité)

Analyse de risques Informatique

Contexte d’application général

Probabilité que survienne un événement nuisible et éventualité qu'existe une menace plus ou moins prévisible pouvant influer sur la réalisation des objectifs d'une organisation

Risque provient du mot italien (Moyen Âge) risico signifiant rocher escarpé, écueil, utilisé pour désigner le péril couru en mer par les premières compagnies d’assurance

Analyse de risques Informatique

Définition scientifique

Risque : Espérance mathématique d'une fonction de probabilité d'événements

- Dès qu'un événement a moins de 100% des chances de se réaliser, il y a risque
- Une gestion du risque efficace permet de réduire l'incertitude et prévoir le futur (et non prédire!)
- Pour prévoir le futur, il nous faut des données fiables telles que :
  - Evénements du passé
  - Simulations issues de modèle probabiliste

Analyse de risques Informatique

Raison d'être

- **L'analyse de risques, outil indispensable** à une bonne hygiène informatique
  - quel que soit le secteur d'activités, le type d'établissement (public ou privé) ou sa taille.

- Une bonne vision des risques pesant sur un système d'information est une priorité pour protéger savoirs faire et **actifs numériques**.

- La **réglementation** peut contraindre à réaliser ces analyses de risques. Citons par exemple :
  - Le Règlement général sur la protection des données (RGPD) dans le cadre d'analyse d'impact ;
  - Le Référentiel Général de Sécurité pour l'homologation des systèmes d'information ou des applicatifs gérés par des établissement publics ;
  - Le Règlement européen Eidas ayant pour but d'augmenter la confiance dans les transactions électroniques au sein de l'UE, etc.
  - De la même façon, certaines certifications (nécessitent une analyse de risques pour pouvoir obtenir les agréments demandés.
  - Voir aussi : Eidas , RGPD , ISO 27001 , PSI-DSS, ….

Analyse de risques Informatique
Notions générales

Une analyse de risques permet d'identifier les menaces qui pèsent sur les systèmes d'information, comme les risques liés à :

- **La cybercriminalité (ransomware, phishing, etc.) ;**
- **La concurrence déloyale ;**
- **La corruption interne ;**
- **Des évènements naturels (inondation, incendie – cas du Datacenter d'OVH).**
- **…..**

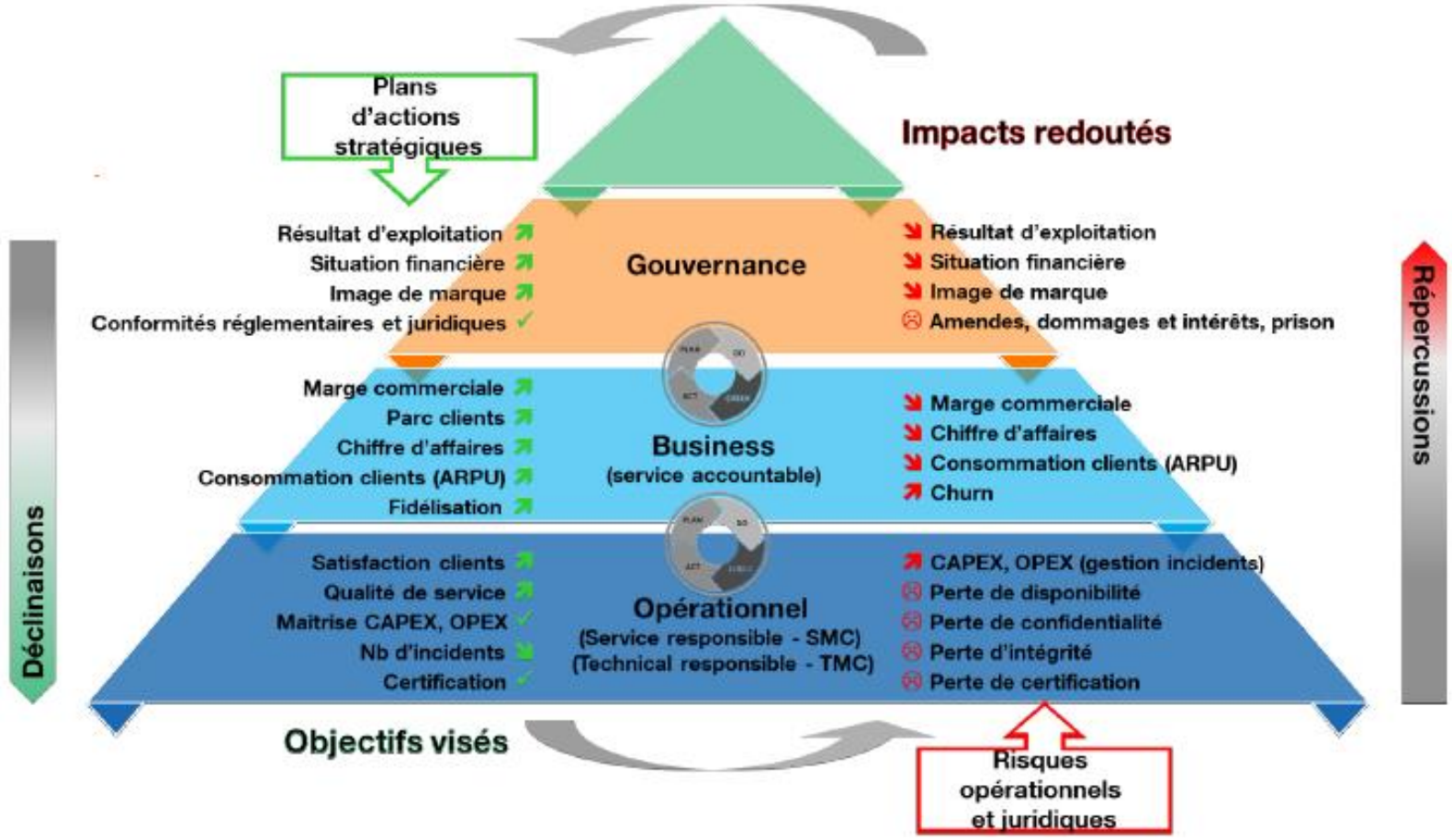
Voir exemples en annexe

L'identification des menaces pertinentes est le fruit d'un alignement avec les fonctions business de l'entreprise par un questionnement !

Quels sont les évènements redoutés ?

Analyse de risques Informatique
Notions générales : anticiper

La gestion de risque vise à anticiper les évènements susceptibles d'empêcher l'atteinte des objectifs



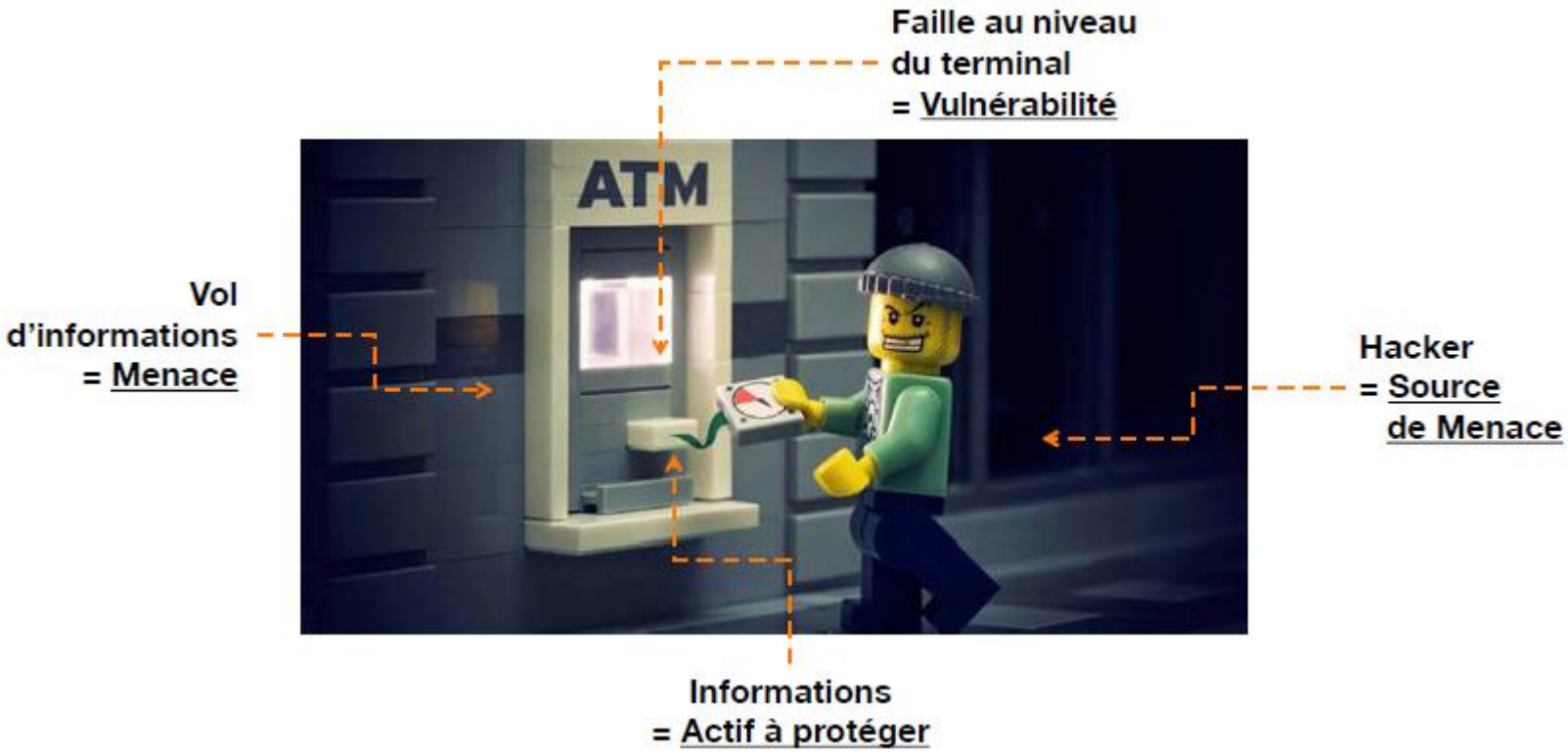
Analyse de risques Informatique
Notions générales

- **Consciemment ou non, une analyse de risques se cache derrière chaque décision de votre vie quotidienne, de la plus simple (traverser la rue) à la plus critique (accepter de recevoir un traitement de soins expérimental).**

- **Un risque peut être :**
  - **Remédié ou Mitigé**
  - **Transféré**
  - **Accepté**
  - **Evité**

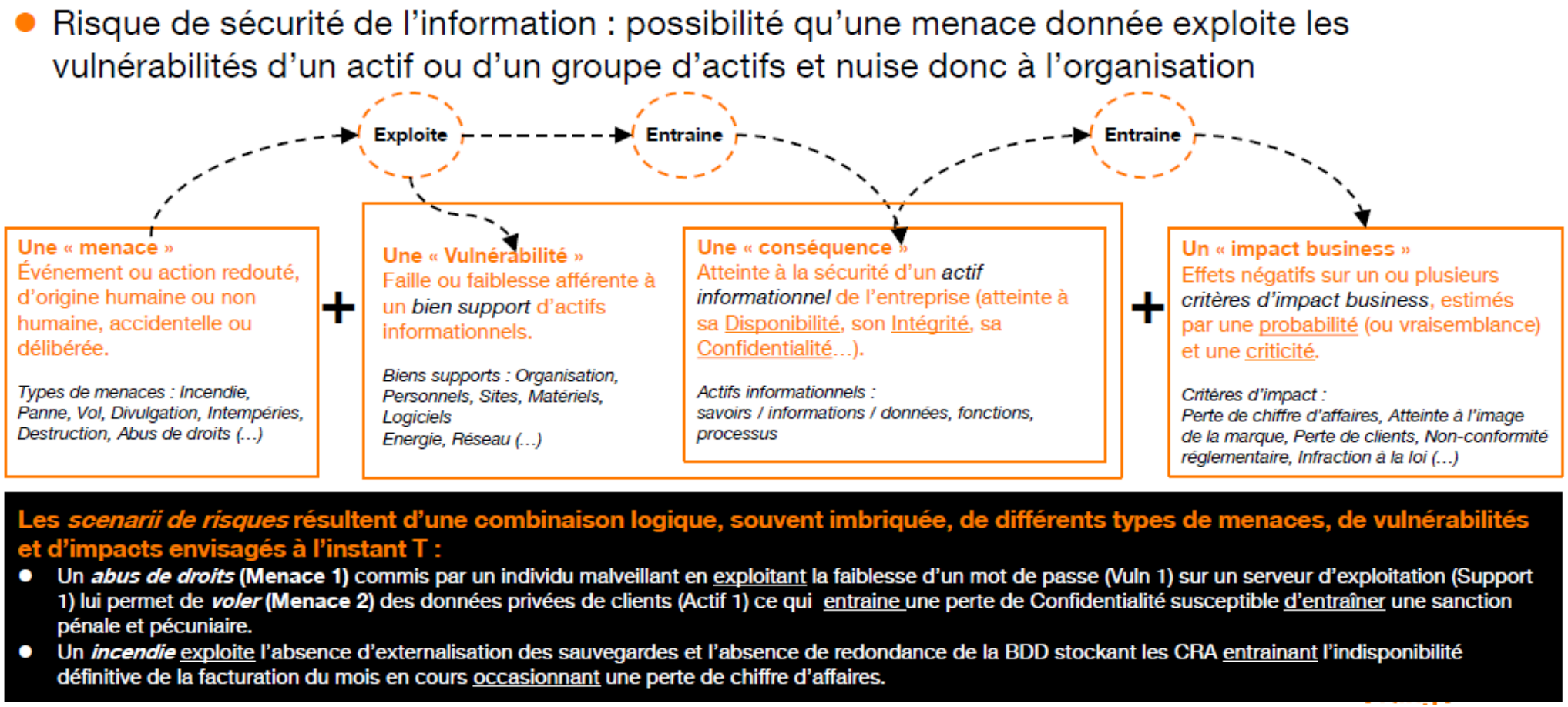
- **Un risque s'applique à un**
  - **Business (Process métier…)**
  - **Support (Serveur, PC,..)**

- **Actif**
  - Tout élément représentant de la valeur pour l'organisme
  - Primaires (Exemples: Activités, Informations)
  - Support (Exemples : Application, Machine, Équipement, Données, Site…)



Analyse de risques Informatique
Notions générales

- **Un risque est le fruit de plusieurs éléments observables et/ou +/- prédictibles :**



CRA : notion business « coût de recrutement par abonné » . Il est important de s'approprier le vocabulaire des parties prenantes.

Analyse de risques Informatique

Notions générales : Lien entre l'actif , la vulnérabilité et la menace.

Actif	Vulnérabilité	Menace
1. Matériel	Entrepôt non surveillé	Vol d'équipement
	Sensibilité à l'humidité	Corrosion
2. Logiciel	Absence de piste d'audit	Abus de droits non détecté
	Interface usager compliqué	Erreur de saisie
3. Réseau	Ligne de communication non protégée	Écoute électronique
	Transfert des mots de passe en clair	Hacker
4. Personnel	Insuffisance de formation	Erreur
	Manque de supervision	Vol d'équipement, erreurs
5. Site	Site dans un endroit inondable	Inondation
	Réseau électrique instable	Perte de courant
6. Organisation	Absence de processus d'autorisation de droits d'accès	Abus de privilèges
	Absence de processus de gestion documentaire	Corruption de données

Analyse de risques Informatique

Notions générales : Lien entre la menace , la vulnérabilité et l'impact.

Menace	Vulnérabilité	Impact
Vol d'équipements	Entrepôt non surveillé	Pertes monétaires
Corrosion	Sensibilité à l'humidité	Bris d'équipement
Erreur de saisie	Interface utilisateur compliquée	Base de données corrompue
Écoute électronique	Ligne de communication non protégée	Interception de communications
Hacker	Transfert des mots de passe en clair	Vol d'information
Corruption de données	Absence de processus de gestion documentaire	Documentation SMSI pas à jour

Analyse de risques Informatique
Notions générales

La valeur du risque s'évalue :

Idem pour les valeurs de vraisemblance et d'impact.

La Cnil a donné pour cela l'échelle de valeur suivante accompagnée d'exemples concrets d'impact :

N°	Niveau de gravité	Description	Quelques exemples concrets
1	Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaitre quelques désagréments qu'elles surmonteront sans difficulté	Maux de tête passagers Réception de SPAMS Sentiment d'atteinte à la vie privée
2	Limitée	Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Refus d'un service administratif ou commercial (ex : refus de prêt bancaire) Publicité ciblée sur un aspect que la personne souhaiterait garder confidentiel (ex : traitement pharmaceutique…)
3	Importante	Les personnes concernées pourraient connaitre des conséquences significatives, qu'elles devraient pouvoir surmonter mais avec des difficultés réelles et significatives	Chantage Interdiction bancaire Blessure physique Divorce Phishing
4	Maximale	Les personnes concernées pourraient connaitre des conséquences significatives, voire irrémédiables, qu'elles ne pourraient pas surmonter	Décès Sanction pénale Perte de preuve dans le cadre d'un contentieux

Le risques 4 concerne notamment l'atteinte à des données de santé, et encore une fois l'actualité nous le rappelle tristement avec toutes les cyberattaques qui ont lieu sur les SI d'hôpitaux et de laboratoires de santé qui ont causé le décès d'une personne en Allemagne .

Analyse de risques Informatique
Notions générales

Concernant la vraisemblance, l'échelle de valeur est la suivante :

N°	Niveau de gravité	Description
1	Négligeable	Il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports
2	Limitée	Il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports
3	Importante	Il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports
4	Maximale	Il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports

Une vraisemblance 4 peut concerner par exemple une attaque informatique ayant utilisé la vulnérabilité d'une application non corrigée. Sans correctif apporté, les attaquants utiliseront de nouveau la faille.

Une autre vraisemblance 4 : un traitement de vidéosurveillance dans lequel les postes de supervision seraient accessibles ou visibles par tous les membres du personnel, voire aux visiteurs des locaux. Toutes les vidéos (données personnelles) seraient ainsi diffusées à d'autres personnes que le personnel en charge de la surveillance.

Analyse de risques Informatique
Notions générales : un exemple de synthèse

Menace	Vulnérabilité	Actif et Impact	Risque	Recommandations de contrôle
Défaillance système – Surchauffe dans la salle de serveurs **Élevée**	Le système de climatisation a dix ans **Élevée**	Serveurs. Tous les services (site Web, messagerie, etc.) seront indisponibles pendant au moins trois ans **Critique**	**Élevée** Perte potentielle de 45 000 € par occurrence	Achat d'un nouveau climatiseur 2 700 €
Attaque DDoS par des humains malveillants (interférence) **Élevée**	Le pare-feu est correctement configuré et dispose d'une bonne atténuation des attaques DDoS **Faible**	Site Web. Les ressources du site Web seront indisponibles **Critique**	**Moyen** Perte potentielle de 8 900 € par heure d'indisponibilité	Surveiller le pare-feu
Catastrophes naturelles – inondation **Moyen**	La salle de serveurs se trouve au deuxième étage **Faible**	Serveurs. Tous les services seront indisponibles **Critique**	**Faible**	Aucune action requise
Interférence humaine accidentelle – suppressions accidentelles de fichiers **Élevée**	Les autorisations sont correctement configurées, un logiciel d'audit informatique est en place, des sauvegardes sont réalisées régulièrement **Faible**	Fichiers sur un partage de fichiers. Des données critiques seront peut-être perdues, mais pourront presque certainement être restaurées depuis une sauvegarde **Moyen**	**Faible**	Continuer à surveiller les modifications apportées aux autorisations, les utilisateurs privilégiés et les sauvegardes

Analyse de risques Informatique
Identifier la source de risques

- **Lors d'une analyse de risques, il faut identifier « les sources de risques » . Elle consiste à rechercher le fait générateur d'une atteinte au SI ou à l'application concernée. On parlera des « menaces ».**
  - Cela dépend beaucoup de l'environnement dans lequel évolue le responsable de traitement ; mais des grandes tendances sont communes à tous les secteurs.
  - Les sources de risques peuvent ainsi être humaines et internes à l'entreprise : salariés en poste, administrateurs informatiques, stagiaires, dirigeants, tiers autorisés, etc.
  - Elles peuvent aussi être non humaines : codes malveillants, eau, épidémie, feu, animaux, etc.
  - Elles peuvent également être externes à l'entreprise : pirates informatiques, concurrents, journalistes, visiteurs, sous -traitants, clients, etc.

- **Cette analyse de menaces doit s'accompagner de mesures de traitement du risque.**

  -> Le but : Eliminer la menace ou pour le moins, en limiter les effets.

Analyse de risques Informatique
Méthodologie pour réaliser une analyse de risques

- **Il existe de nombreuses méthodes pour effectuer une analyse de risques, la méthode Ebios étant celle qui est recommandée par l'Anssi.** (mais celle-ci est relativement exhaustive et complexe). On peux noter également la norme ISO 31000 ou ISO 27005.

- **L'important au final est que la personne qui effectue l'analyse de risques puisse travailler de manière neutre et sans subir la pression de son propre environnement professionnel.**
  - C'est la raison pour laquelle, il est souvent préférable de confier les analyses de risques à des cabinets ou à des sociétés d'audit qui sont externes au service responsable du traitement concerné.

Analyse de risques Informatique

Notions générales : Calculer la probabilité d'un évènement redouté ?

1. L'année dernière, une organisation a enregistrée 730 incidents liés à l'oubli d'un mot de passe

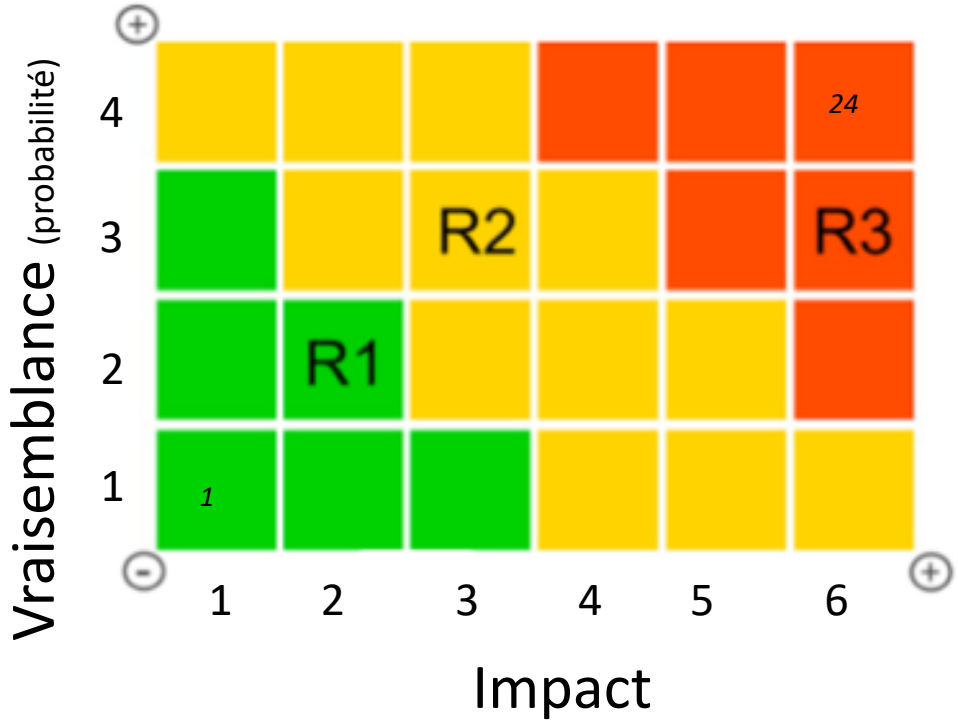
2. 730 incidents / 365 jours = 2

3. La probabilité de ce scénario d'incident pour l'organisation est d'une moyenne de 2 par jour

Analyse de risques Informatique
Le côté pragmatique de l'analyse.

L'équation du risque :

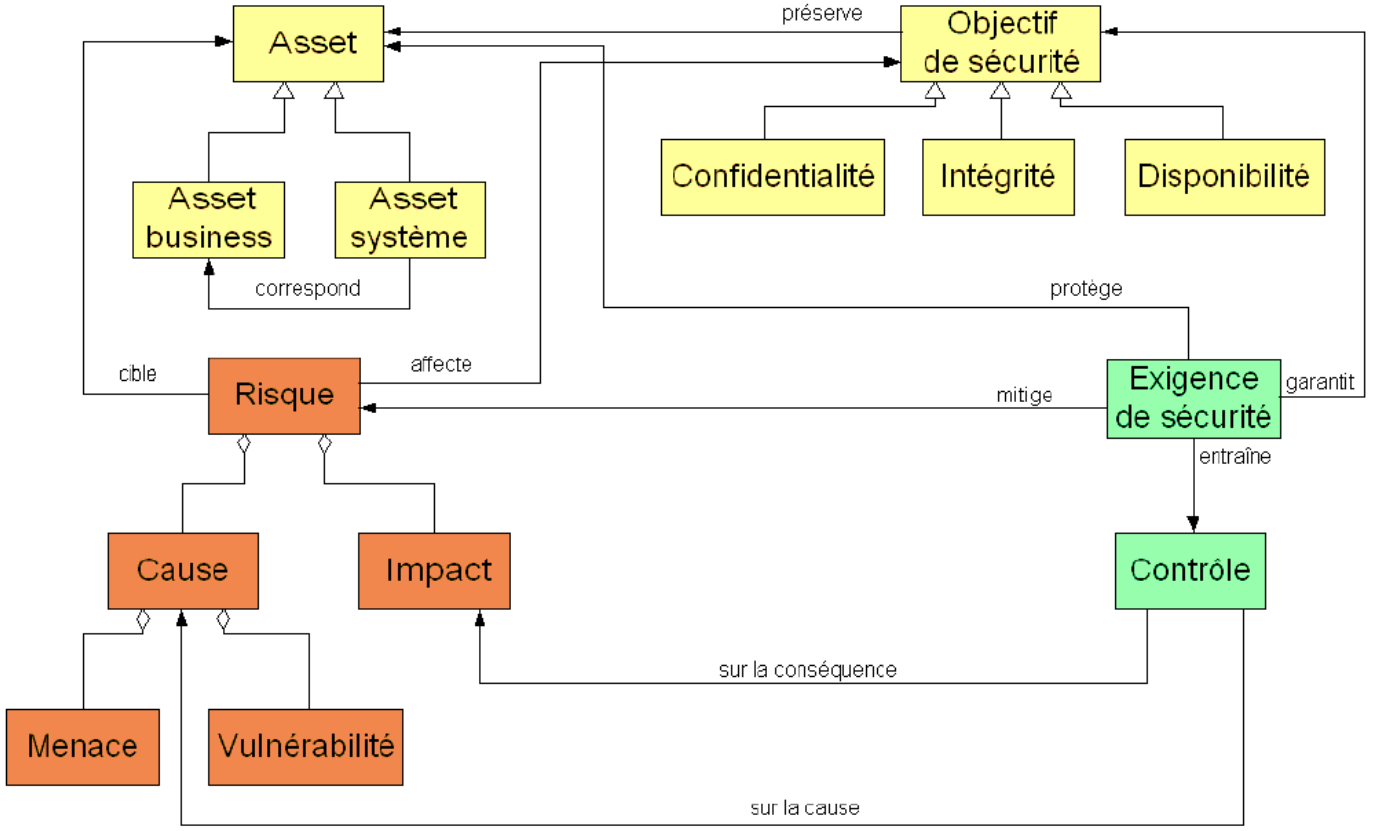
La modélisation :



Analyse de risques Informatique
Méthodologie pour réaliser une analyse de risques

La gestion des risques, se compose de trois blocs interdépendants.

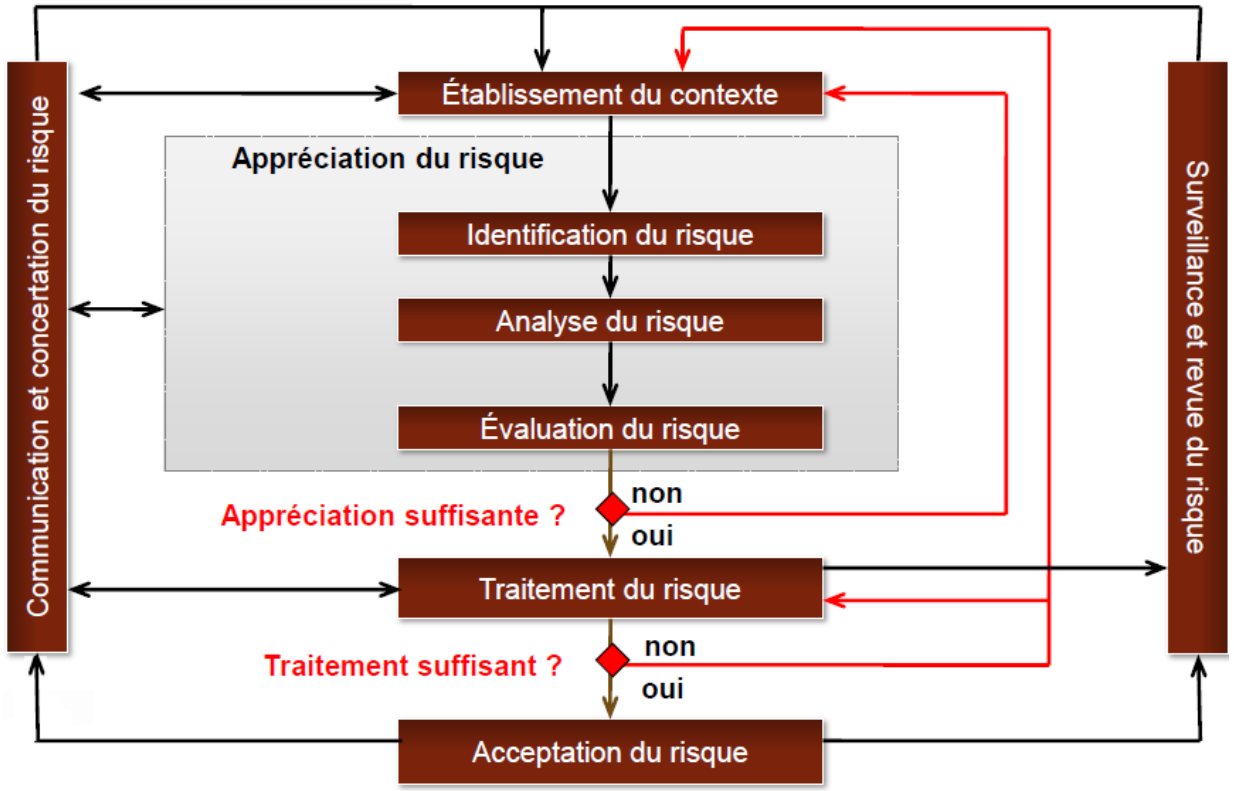
1. L'**organisation** cible de l'étude, définie par ses assets et ses besoins de sécurité,
2. Les **risques** pesant sur ces assets,
3. Les **mesures** prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité.



Les assets sont définis comme étant l'ensemble des biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement

Analyse de risques Informatique
Le côté pragmatique de l'analyse.

Comment faire ?



Quelles sont les étapes ?

1. Effectuer les interviews
2. Rassembler la documentation
3. Dresser un état des lieux des mesures de protection.
4. Evaluer les risques
5. Effectuer des recommandations
6. Réévaluer les risques

Définissez des critères …

Quantitatif	Qualitatif
Inférieur à 50 k€	Faible
Compris en 50 et 500 k€	Moyen
Supérieur à 500 k€	Élevé

… mais : Il n'existe aucune méthodologie purement quantitative ou qualitative

Analyse de risques Informatique
Comment procéder ?

Étape 1 : effectuer les interviews des personnes concernées

- Les personnes concernées peuvent être les dirigeants, le délégué à la protection des données, les équipes métiers, les équipes informatiques, les équipes d'info gérance, etc.
- Le ton employé aura alors ici une importance primordiale. Il est ainsi nécessaire d'installer un climat de confiance avec la personne interviewée. L'entretien ne devra pas prendre une forme accusatoire si vous souhaitez obtenir des informations correctes.
- Il s'agira de bien comprendre les usages au sein de l'entreprise.

Objectif : identification des évènements redoutés et permet très souvent de découvrir les « **Shadow IT** ». Il est important de collecter un maximum d'informations car il est impossible de protéger ce qui est inconnu.

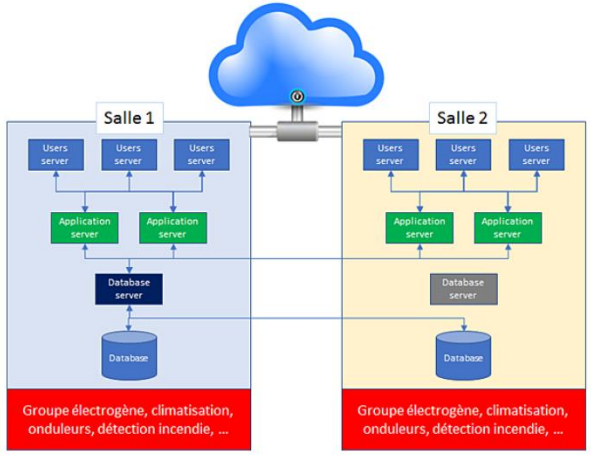
Analyse de risques Informatique
Comment procéder ?

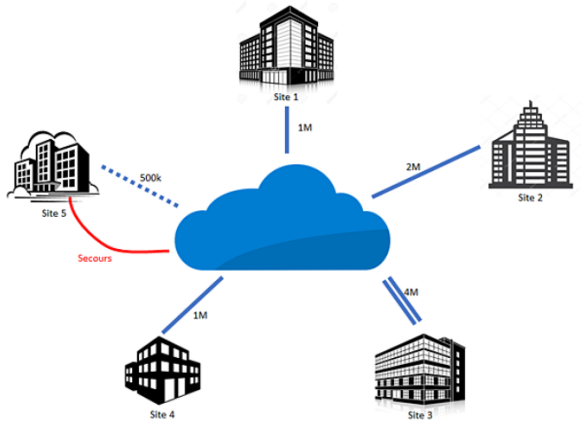
Étape 2 : rassembler la documentation

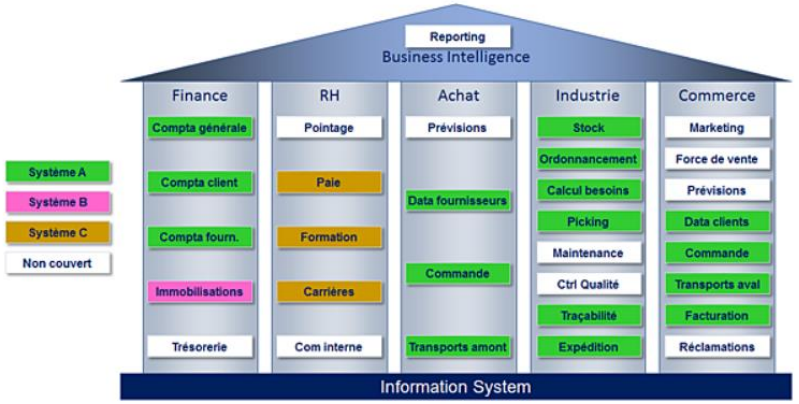
- Il s'agit ici d'étudier toute la documentation de sécurité utilisée par le responsable de traitement ou son sous-traitant.

- Obtenir la cartographie précise des applications hébergées sur le SI, des flux de données qui naviguent entre elles et des « datacenter » utilisés par le responsable de traitement.
  - Ce document est important car il permet de détecter les zones vulnérables d'un SI et notamment celles ouvertes sur internet.
  - Si ce document n'existe pas, l'étude devra être complétée par des schémas visuels à minima techniques et/ou fonctionnels.

Exemple de documents importants :
- PSSI, Plan assurance sécurité ,
- Charte informatique
- Politique de mot de passe,
- Politique de sauvegarde et d'archivage des données,
- Résultat des tests de sécurité effectués en interne ou en externe (test d'instruction, pentest, audit de code),
- PCA et PRA ,
- Politique de gestion des logs,
- Accord de confidentialité,
- Politique de sureté des locaux,
- etc.







Analyse de risques Informatique
Comment procéder ?

- **Étape 3 : dresser un état des mesures mises en œuvre par le responsable de traitement ou son sous-traitant**

-> Il s'agira par exemple de décrire les mesures de sécurité appliquées comme la politique de mot de passe, la durée de conservation des logs, la durée de conservation des sauvegardes, le type de sauvegarde effectuée, les mesures de chiffrement, la protection des locaux, la sécurité des postes de travail et également les mesures organisationnelles telles que relation avec les tiers, gestion du personnel, etc.

Analyse de risques Informatique
Comment procéder ?

- **Étape 4 : évaluer les risques**

Etablir une liste des risques identifiés et les projeter dans un tableau de synthèse.

Exemples :

- vous avez détecté qu'une seule et unique personne disposait d'un mot de passe pour accéder à une boite mail créée pour recueillir les alertes professionnelles des salariés. Il y a un **risque important** en cas d'indisponibilité de cette personne que les données soient rendues inaccessibles. La source de risques sera ici interne et le risque **concernera la disponibilité des données**.

- vous avez détecté que les collaborateurs étaient administrateurs de leur poste de travail. Il y a un risque qu'un logiciel malveillant soit installé par un collaborateur. Ce logiciel malveillant pourra avoir pour effet de chiffrer les données, soit du poste de travail, soit d'une partie du SI de l'entreprise. Il s'agit donc d'un **risque critique sur l'intégrité des données**.

- vous avez détecté que les locaux du RT étaient situés dans une zone inondable et qu'aucune mesure de protection n'est prise pour protéger les baies des serveurs de ce risque naturel. À noter que si la dernière inondation de la région date de 1904, **la vraisemblance du risque restera limitée.**

Objectif : **L'ensemble de ces éléments devront être intégrés à un tableau récapitulatif et le mieux est de cartographier les différents risques sur un schéma facilement lisible pour toutes les personnes qui souhaiteraient accéder à ces informations.**

Analyse de risques Informatique
Comment procéder ?

Étape 5 : effectuer des recommandations pour améliorer le niveau de sécurité.

- **Ces recommandations doivent être adaptées** à l'environnement du responsable de traitement, par exemple il est inutile de recommander d'utiliser un antivirus comportemental (EDR) de dernière génération si le SI n'est composé que de quelques serveurs connectés entre eux.

- Il est souvent recommandé de **formaliser les usages des outils informatiques** dans des documents écrits (quand ils ne le sont pas) . On parlera de politique de sécurité. Par exemple, si une politique de mot de passe est appliquée sans être formalisée dans la PSSI.

- L'ensemble des recommandations effectuées devront être formalisées dans **un plan d'action** et contribueront à faire baisser les risques quand elles seront appliquées.

Analyse de risques Informatique
Comment procéder ?

- **Étape 6 : réévaluer les risques après applications des recommandations**

Vous devez montrer comment les mesures que vous avez formalisé atténuent les risques.

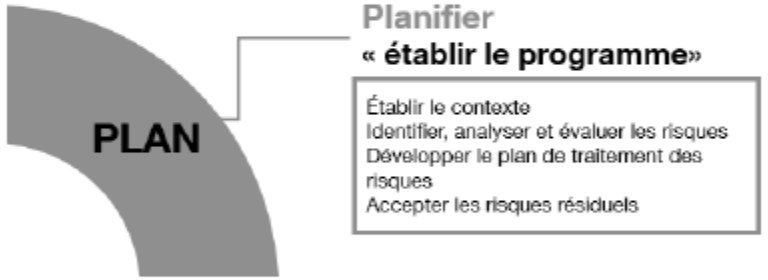
Par exemple,

- vous avez recommandé l'interdiction pour les utilisateurs d'utiliser les ports USB, cela attenue automatiquement le risques de vraisemblance d'une attaque informatique.

- vous avez recommandé de mettre en place une redondance des serveurs stockés dans une zone inondable vers un autre datacenter distant, vous avez atténué les risques d'atteinte à la disponibilité des données en cas d'inondation.

Analyse de risques Informatique
A retenir

- **Les étapes clés d'une analyse de risques sont :**
  - Établissement du contexte
    - Définition du périmètre de l'analyse
    - Identification des actifs essentiels et supports
    - Métriques et critères de traitement des risques
  - Appréciation des risques
    - Identification des risques
    - Évaluation de leurs impacts et vraisemblance
    - Cartographie des risques
  - Traitement des risques
    - Réduction, Maintien, Partage, Refus
    - Mesures de couverture
    - Risques résiduels
  - Mise à jour et communication



Analyse de risques Informatique
A retenir

- **Les pièges**
  - Mauvaise compréhension du contexte et des objectifs
  - Métriques inadaptées au contexte et/ou non validées par le commanditaire
  - Inadaptation des moyens:
    - Défauts de participation
    - Niveau des intervenants
  - L'enfermement dans la méthode
  - Le défaut de communication
  - Difficulté d'exposer en restitution

- **Ne pas maintenir la cartographie des risques**

ANNEXES

Analyse de risques Informatique
Annexe : Exemple de trame d'analyse

Description des contrôles existant	Evaluation du risque				Mesures à mettre en place	Nouvelle évaluation après mise en place de la mesure		
	Probabilité (a)	Impact (b)	Niveau de risque (a+b)	Appréciation		Nouvelle probabilité (a)	Nouveau niveau (a+b)	Δ Niveau

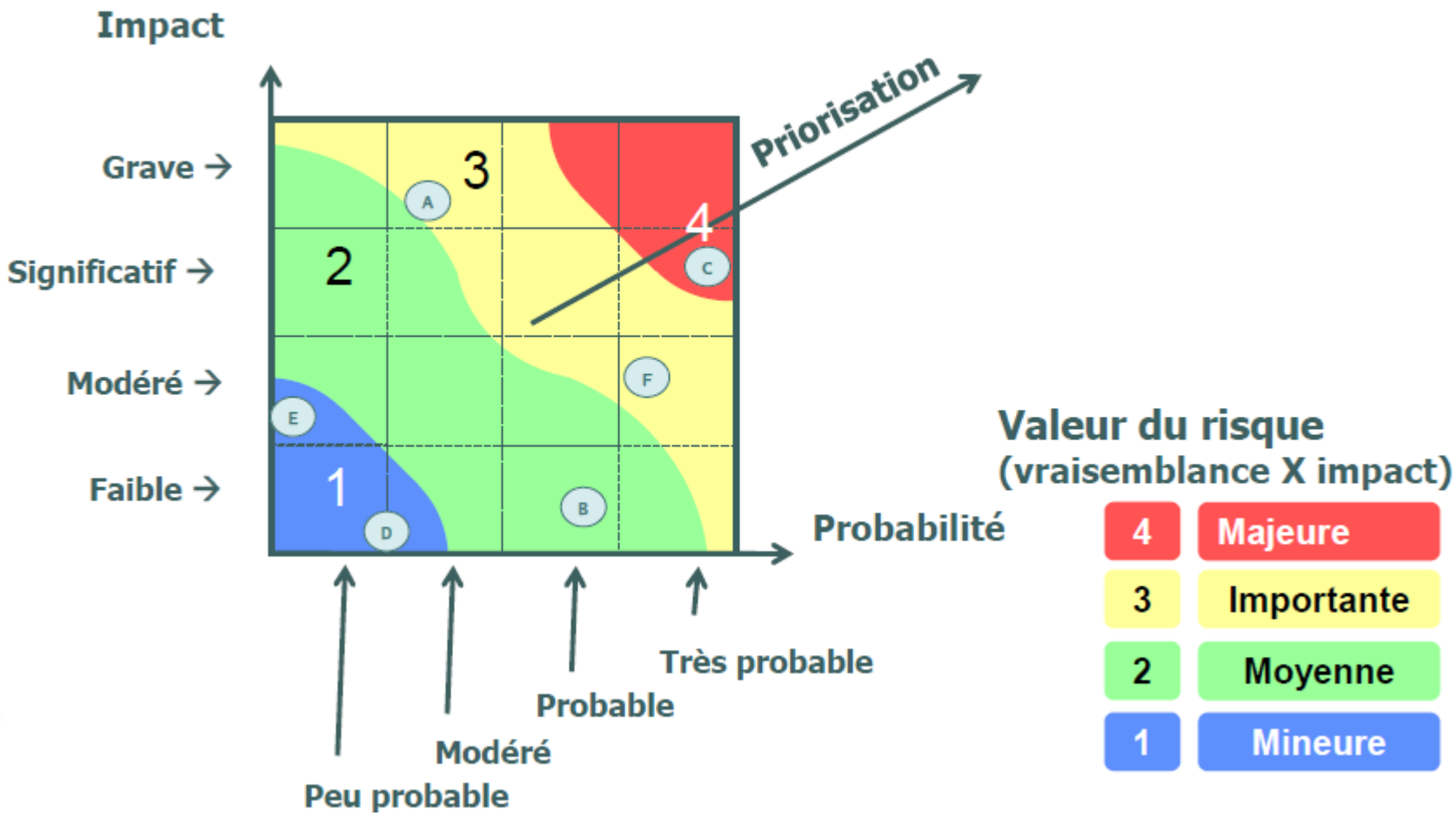
.....->

Mesures à mettre en place	Nouvelle évaluation après mise en place de la mesure			Porteur	Délai	Date de fin	Dispositif de suivi et de mise sous contrôle		Date de clôture
	Nouvelle probabilité (a)	Nouveau niveau (a+b)	Δ Niveau				Qui	Quand	

Analyse de risques Informatique
Annexe : Exemple de trame d'analyse

					Chantier 1	Chantier 2	Chantier 3	Chantier 4	Chantier 5	Chantier 6	Chantier 7	Chantier 8	Chantier 9	Chantier 10			
Réf RSK	Scénario de risque	Impact	Vraisemblance	Niveau de risque	Sécurité des ressources humaines et sensibilisation	Intégration de la sécurité dans les projets	Gestion sécurisée des fournisseurs	Gestion des vulnérabilités techniques	Gestion de la continuité	Sécurité des communications	Contrôle de la sécurité de l'information	Organisation de la sécurité	Gestion des identités et des accès	Gestion des incidents de sécurité	Gravité résiduelle	Vraissemblance résiduelle	Niveau de risque résiduel
RSK01		4	2	Critique	X	X						X			4	1	Significatif
RSK02		4	1	Significatif	X	X						X			4	1	Significatif
RSK03		2	2	Acceptable	X	X									2	1	Acceptable

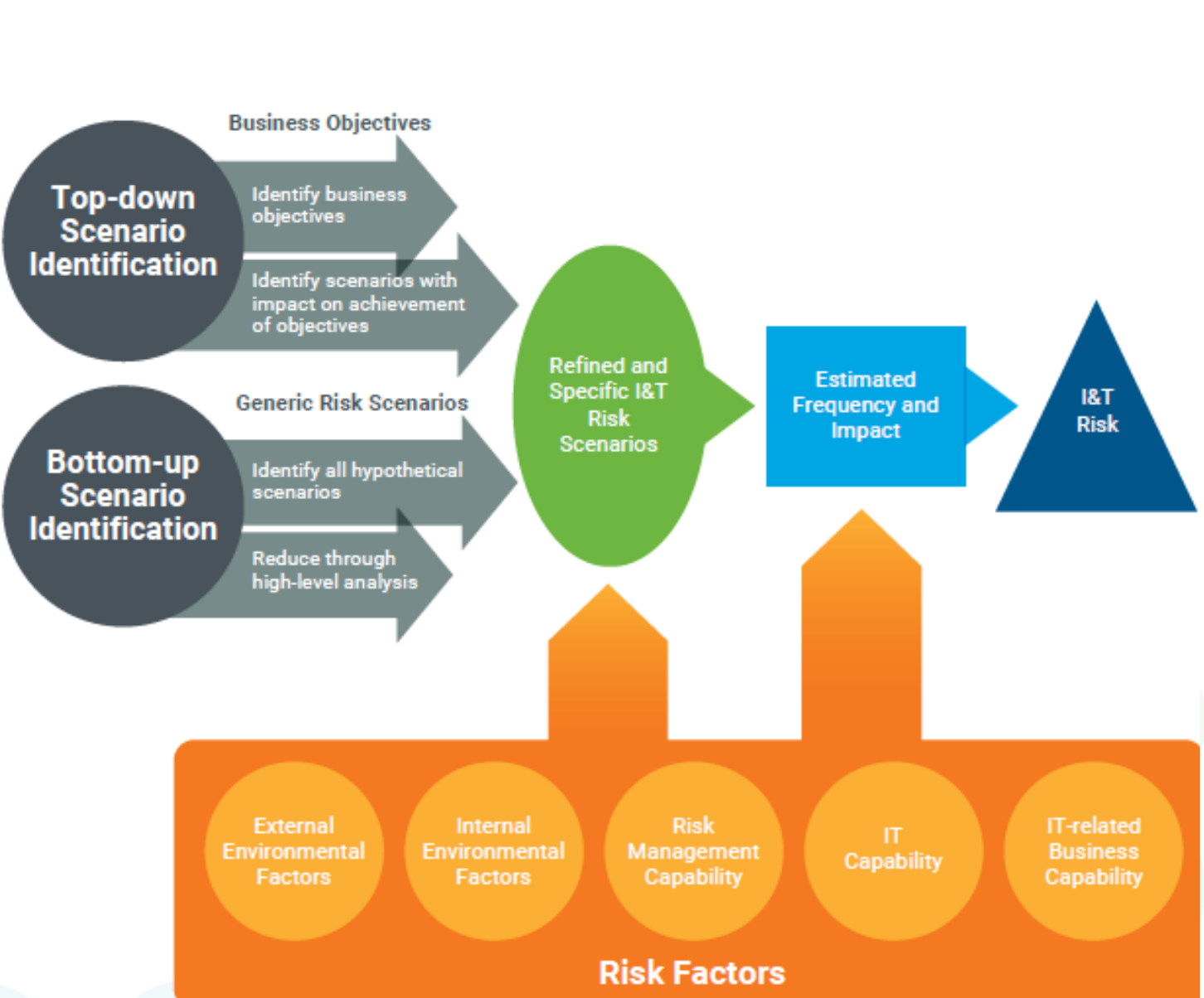
Analyse de risques Informatique
Annexe : exemple de présentation des résultats

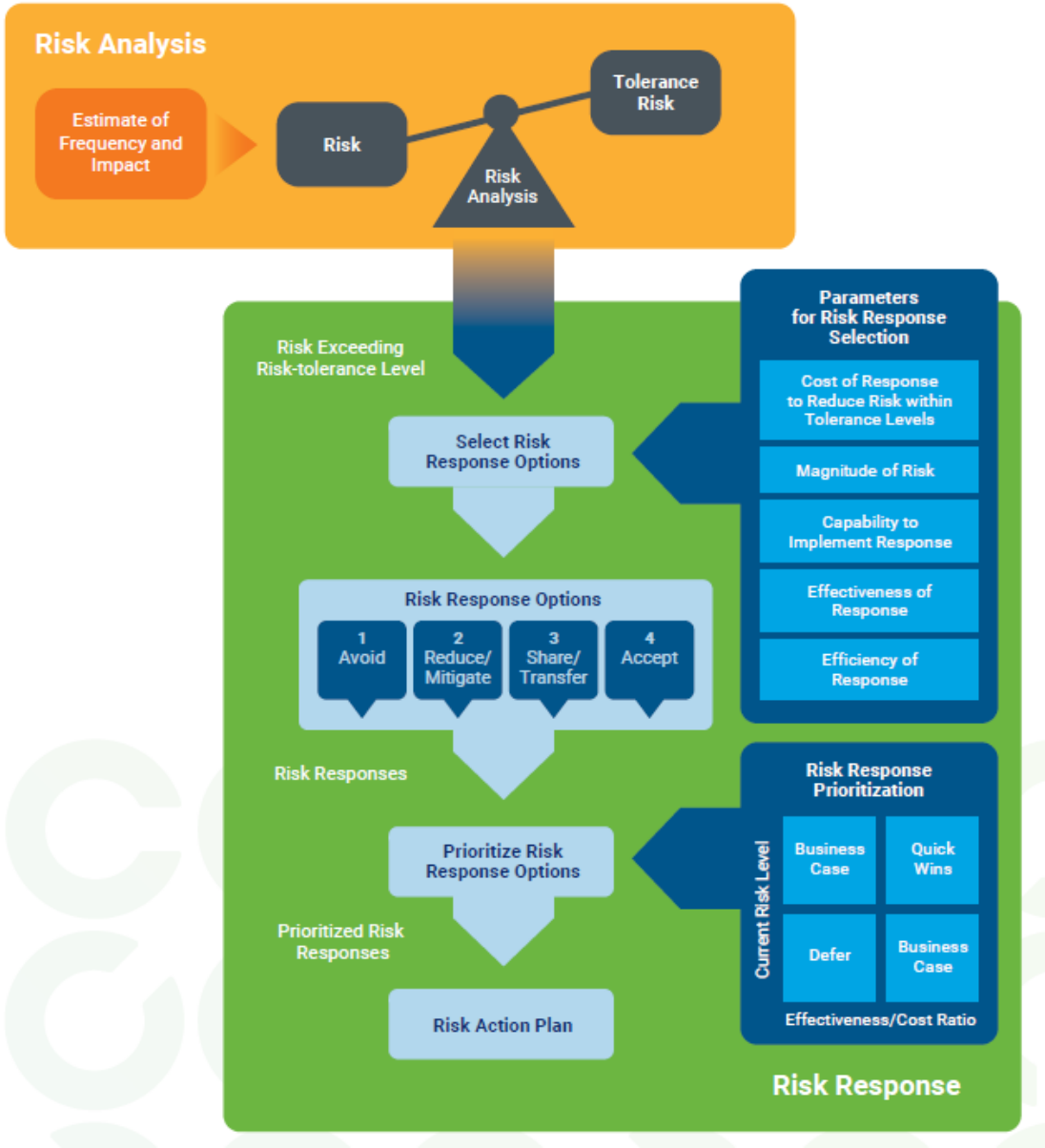


Valeur du risque
(vraisemblance X impact)

4	Majeure
3	Importante
2	Moyenne
1	Mineure

Analyse de risques Informatique
Annexe : méthodes d'analyses et de traitement.





Analyse de risques Informatique
Annexe : exemple de critères d'évaluation d'impacts - confidentialité

Impacts	1 (Faible)	2 (Modéré)	3 (Élevé)
Désavantage concurrentiel	Les initiatives stratégiques sont retardées de plusieurs jours	Les initiatives stratégiques sont retardées de plusieurs semaines	Les initiatives stratégiques sont avortées
Dommage potentiel si l'information est révélée à un concurrent ?			
Perte directe d'affaires	Plus de $50,000	Plus de $500,000	Plus de $50,000,000
Perte de revenus (clients /contrats) si l'information est révélée à un concurrent ?			
Perte de réputation	Rumeurs négatives	Apparition dans les médias économiques ou nationaux	L'image publique de l'organisme est sérieusement affectée
Dommages à la confiance des clients, des fournisseurs et / ou à l'image de l'organisme si l'information est révélée ?			
Coûts additionnels	Plus de $50,000	Plus de $500,000	Plus de $50,000,000
Travail et coûts additionnels en raison des problèmes si l'information est révélée ?			
Responsabilité légale	Accord à l'amiable	Action judiciaire et / ou légale d'une durée de moins de 12 mois	Action judiciaire et / ou légale d'une durée de plus de 24 mois
Infraction à des engagements règlementaires ou contractuels si l'information est révélée ?			
Dommage moral du personnel	La productivité du personnel est légèrement réduite	La productivité du personnel est réduite et augmentation des congés maladie	La productivité du personnel est réduite de façon dramatique et perte importante de personnel
Effet préjudiciable sur le moral ou la motivation du personnel, si l'information est révélée ?			

Analyse de risques Informatique
Annexe : exemple de critères d'évaluation d'impacts - confidentialité

Impacts	1 (Faible)	2 (Modéré)	3 (Élevé)
Désavantage concurrentiel Dommage potentiel si l'information est révélée à un concurrent ?	Les initiatives stratégiques sont retardées de plusieurs jours	Les initiatives stratégiques sont retardées de plusieurs semaines	Les initiatives stratégiques sont avortées
Perte directe d'affaires Perte de revenus (clients /contrats) si l'information est révélée à un concurrent ?	Plus de $50,000	Plus de $500,000	Plus de $50,000,000
Perte de réputation Dommages à la confiance des clients, des fournisseurs et / ou à l'image de l'organisme si l'information est révélée ?	Rumeurs négatives	Apparition dans les médias économiques ou nationaux	L'image publique de l'organisme est sérieusement affectée
Coûts additionnels Travail et coûts additionnels en raison des problèmes si l'information est révélée ?	Plus de $50,000	Plus de $500,000	Plus de $50,000,000
Responsabilité légale Infraction à des engagements règlementaires ou contractuels si l'information est révélée ?	Accord à l'amiable	Action judiciaire et / ou légale d'une durée de moins de 12 mois	Action judiciaire et / ou légale d'une durée de plus de 24 mois
Dommage moral du personnel Effet préjudiciable sur le moral ou la motivation du personnel, si l'information est révélée ?	La productivité du personnel est légèrement réduite	La productivité du personnel est réduite et augmentation des congés maladie	La productivité du personnel est réduite de façon dramatique et perte importante de personnel

Analyse de risques Informatique
Annexe : Documentations

- https://www.alain-bensoussan.com/avocats/lanalyse-de-risques-outil-indispensable-a-une-bonne-hygiene-informatique/2021/04/29/

- https://openclassrooms.com/fr/courses/1734211-analysez-et-gerez-des-risques-si/1749021-definissez-ce-qu-est-un-risque-en-securite-de-l-information

- Sites l'ANSSI et CNIL (voir annexes sur Teams)

- Etc …