

Gestion

Comprendre la gestion des risques



Compétence demandée :
Comprendre la gestion des risques

1. Le dommage
2. Types de risques
3. Méthodologie
4. Les organisations
5. Les normes

LE DOMMAGE

Qu'est-ce qu'un dommage ?



Un **dommage** est un dégât
matériel ou immatériel, à une
chose ou une personne

A partir de quel moment un
dommage est grave ?



La **gravité** est l'ampleur des dommages potentiels

La **probabilité d'occurrence** est la probabilité de subir un dommage

La **gravité** est l'ampleur des dommages potentiels

La **probabilité d'occurrence** est la probabilité de subir un dommage



La **criticité** est une mesure du **risque** :

criticité = probabilité d'occurrence x gravité

①

②

TYPES DE RISQUES

Quels sont les types de
risques ?



Risque de **réputation** (image de l'entreprise)
Risque **financier** (perte ou manque à gagner)
Risque **systemique** (effet boule de neige)
Risque **social** (comportements)
Risque **opérationnel** (gestion de l'activité)
Risque **légal** (réglementaire)

Risque de **réputation** (image de l'entreprise)

Risque **financier** (perte ou manque à gagner)

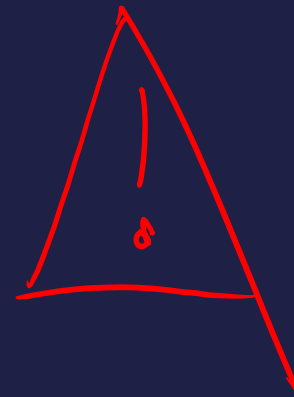
Risque systémique (effet boule de neige)

Risque **social** (comportements)

Risque **opérationnel** (gestion de l'activité)

Risque **légal** (réglementaire)

Il n'y a pas de risque systématiquement plus grand car la criticité dépend de l'activité



Il n'y a pas de risque systématiquement plus grand car la criticité dépend de l'activité



Risque de **réputation** (image de l'entreprise)

Risque **financier** (perte ou manque à gagner)

Risque **systemique** (effet boule de neige)

Risque **social** (comportements)

Risque **opérationnel** (gestion de l'activité)

Risque légal (réglementaire)

Règlement UE 2016/679 du Parlement européen

Le **RGPD** (Règlement Général sur la Protection des Données) dicte les mesures à adopter pour la **protection des données à caractère personnel (DCP)** sur le territoire de l'Union Européenne

Règlement UE 2016/679 du Parlement européen

Le **RGPD** (Règlement Général sur la Protection des Données) dicte les mesures à adopter pour la **protection des données à caractère personnel (DCP)** sur le territoire de l'Union Européenne



DCP (PII) ?

Article 4 du RGPD et article 2 de loi informatique et libertés

Toute information relative à une personne physique
identifiée ou qui peut être identifiée, directement ou
indirectement

Article 4 du RGPD et article 2 de loi informatique et libertés

Toute information relative à une personne physique
identifiée ou qui peut être identifiée, directement ou
indirectement



METHODOLOGIE

Comment mettre en place une gestion des risques ?



1. Planifier la gestion des risques
2. Identifier les risques
3. Estimer les risques
4. Maitriser les risques
5. Surveiller les risques

1. Planifier la gestion des risques

Comment organiser et planifier la gestion des risques dans une entreprise ?
Prenons une dizaine de minutes pour se sensibiliser !

1. Planifier la gestion des risques

Définir les tâches à accomplir et établir les **responsabilités** :

- en matière de politique d'**acceptation des risques** (les critères)
- concernant toutes les tâches nécessaires à la gestion des risques

2. Identifier les risques

Comment identifier les risques ? Quelles sont les pistes à suivre ?
Prenons une dizaine de minutes pour se sensibiliser !

2. Identifier les risques

Les personnes / l'environnement / les équipement impliqués

Les scénarios menant aux situations dangereuses

Les dommages potentiels

les risques déjà connus,

les bonnes pratiques (guides, normes, spécifications, réglementation)

les possibilités techniques et les limites qui sont associées

3. Estimer les risques

Doit-on estimer les risques ?

Prenons une dizaine de minutes pour se sensibiliser !

3. Estimer les risques

Il faut estimer, de manière quantitative :

- les probabilités d'occurrence
- les gravités

4. Maitriser les risques

Comment maitriser les risques ?

Prenons une dizaine de minutes pour se sensibiliser !

4. Maîtriser les risques

L'idée est de définir des mesures de réduction des risques :

- Suppression totale du risque
- Mise en place d'une prévention
- Compensation du risque s'il n'est pas réduit (par exemple avec une assurance professionnelle)

5. Surveiller les risques

Quelle méthodologie pour surveiller les risques ?
Prenons une dizaine de minutes pour se sensibiliser !

5. Surveiller les risques

Choisir les **indicateurs** pour surveiller les risques connus et de détecter les risques émergents

La définition des indicateurs n'est jamais figée, elle évolue avec votre **compréhension des risques**

LES ORGANISATIONS

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé par décret en juillet 2009.

L'ANSSI apporte son expertise et son assistance technique pour la sécurité des opérateurs d'importance vitale (OIV).

<https://www.ssi.gouv.fr/>

Open Web Application Security Project (OWASP) est une communauté en ligne travaillant sur la **sécurité des applications Web**.

OWASP est aujourd'hui reconnue dans le monde de la sécurité des systèmes d'information pour ses travaux et recommandations liées aux applications Web.

<https://owasp.org/>

LE TOP 10 des menaces

<https://owasp.org/www-project-top-ten/>

1. A1_2017 : Les applications WEB ne vérifie pas assez les inputs et peuvent laisser passer du code

Chaque input est un vecteur d'injection de code

2. A2_2017 : Les fonctions applicatives liées à l'authentification et à la gestion des sessions sont souvent mal implémentées

Tester intensément les fonctions liées à l'authentification

3. A3_2017 : De nombreuses applications WEB ne protègent pas correctement les données sensibles, telles que les données financières, les soins de santé et les informations personnelles (DCP).

Vérifier les risques de fuite de données (obligations légales)

4. A4_2017 : Utilisation de technologies trop anciennes (XML processor) permettent d'exécuter du code externe et hostile.

Restez à jour dans les technologies utilisées ou bien pensez à bien les configurer

5. A5_2017 : Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont souvent pas correctement appliquées

Tester le périmètre d'application des rôles

6. A6_2017 : La mauvaise configuration de la sécurité est le problème le plus fréquemment rencontré. Ceci est généralement le résultat de configurations par défaut non sécurisées ou de configurations incomplètes.

Ne laisser pas la configuration par défaut

7. A7_2017 : Cross-Site Scripting XSS affichage d'éléments HTML non contrôlés (comme les commentaires qui peuvent contenir des éléments HTML)

Bien controler les inputs

8. A8_2017 : Certains systèmes permettent une exécution de code à distance

Limiter le périmètre d'exécution de code et ne permettre que l'exécution de code déjà présent sur le serveur seulement

9. A9_2017 : Les composants, tels que les bibliothèques, les frameworks et autres modules logiciels, peuvent présenter des failles de sécurité

Ne faites confiance qu'aux librairies, frameworks et modules qui sont populaires et bien testés

10. A10_2017 : Une surveillance insuffisante des systèmes permettent aux hackers d'attaquer davantage les systèmes informatiques

Surveiller de manière continue les comportements étranges des visiteurs (proposer par exemple des captcha)

LES NORMES

La norme **ISO/CEI 27005** est une norme internationale concernant la **Sécurité de l'information** publiée conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) **basé sur l'amélioration continue** (PDCA)

La norme **ISO 9001** est une norme internationale concernant le **Système de Management de la Qualité** (SMQ) publiée par l'Organisation internationale de normalisation (ISO).

Cette norme définit des exigences pour améliorer en permanence la **satisfaction de leurs clients** et fournir des **produits et services conformes**

