ESD
Cybersecurity Academy

# Gestion des risques SI avec ISO 27005 & EBIOS

# LIVRET STAGIAIRE

Durée : 2 jours
Version : 1

# L'ESD academy

**Formations, diplômes, certifications en cybersécurité.**

- L'ESD academy est une organisation créée en 2015 dont l'objectif est d'apporter des **formations**, des **certifications** et un **mastère** en cyber-sécurité MadeInFrance
- Chaque formation aboutit sur un examen certificateur dont la liste des lauréats se trouve à cette adresse: https://certifications.esdacademy.eu
- Le Mastère est accessible à Paris, Rennes, Nantes, Lille, La Réunion
- Des professionnels agréés composent notre cercle de formateurs : https://esdacademy.eu/listeformateurs

Fondée en 2015, l'ESD academy a pour mission d'apporter des formations, des certifications et un mastère en cybersécurité pour les organisations francophones et européenne.

Notre objectif est clairement identifié, concurrencer les acteurs étrangers dans la formation et la reconnaissance en sécurité des systèmes d'information. Pour y arriver nous regroupons autour d'un label, des experts du domaine (étatiques et privés) pour de la création de contenu et l'enseignement.

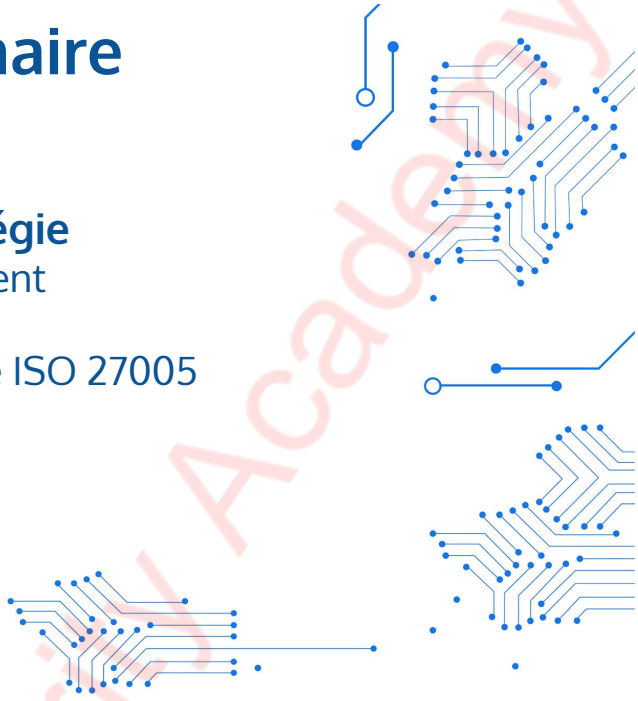
Partie d'un modèle startup, nous dépassons les 500 personnes formés en 2018 dans les domaines de l'offensif, défensif et de la gouvernance pour des clients stratégiques dans le secteur de la cybersécurité française.

La liste des formateurs agréés ESD academy se trouve ici :

https://esdacademy.eu/listeformateurs

# Sommaire





Source : ___

___

# Entreprise : Une stratégie

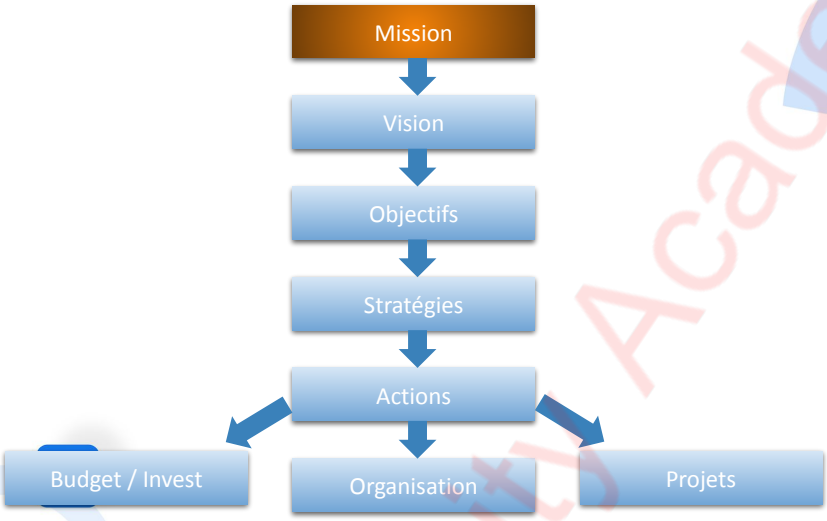
## La raison d'être de l'organisation

- Toute démarche classique d'élaboration d'une stratégie d'entreprise passe par les deux étapes fondamentales suivantes :

Définir ***la mission*** de l'entreprise : c'est à dire sa raison d'être, sa finalité.
Identifier ***la vision*** de l'entreprise : c'est à dire son ambition, sa cible à plus ou moins long terme.

- Ces deux étapes constituent les bases sur lesquelles seront élaborées les objectifs stratégiques, puis les stratégies mises en œuvre.

# Entreprise : Une stratégie



# Entreprise : Une stratégie

## La raison d'être de l'organisation

- Cela commence par la question suivante: *POURQUOI J'EXISTE ?*
- C'est la question fondamentale! Elle fixe la raison d'être de l'entreprise ou de toute entité. Elle donne un sens à son existence.
- La mission constitue la finalité de l'organisation. Elle décrit en quelques mots ce que fait l'entreprise.
- La mission tient souvent en une phrase qui permet d'expliquer aussi bien pour les acteurs internes qu'externes la raison d'être de l'organisation.

# Entreprise : Une stratégie

## Exprimer sa mission

- Ce sont les dirigeants des grandes structures et fondateurs des petites et moyennes entreprises qui en ont généralement la charge.

- Une mission bien pensée permettra de :

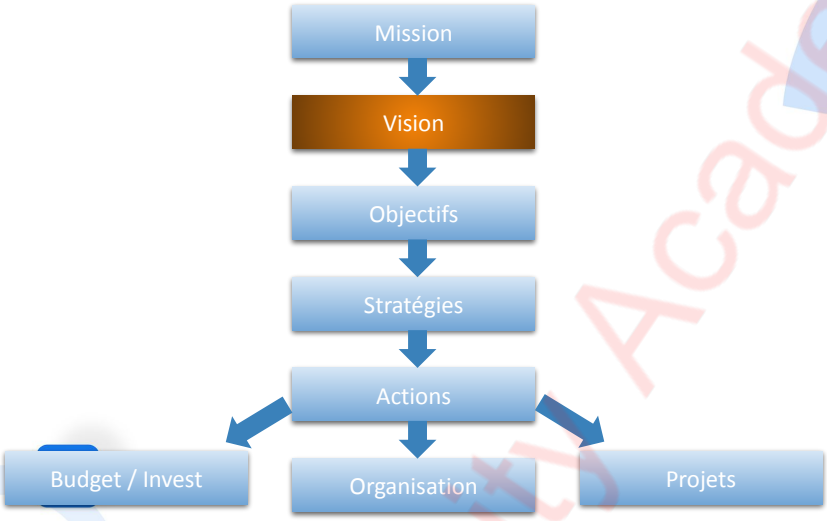
    - Représenter de manière épurée la raison d'être de l'organisation.
    - Communiquer simplement et de manière percutante avec ses clients et partenaires.
    - Motiver et mobiliser les collaborateurs sur une raison d'être et des valeurs.
    - Aligner les stratégies et les actions
    - Donner un cadre de réflexion et de travail aux cadres de l'entreprise.

# Entreprise : Une stratégie

## Illustration de missions d'entreprise

- **Google** : organiser l'information à l'échelle mondiale et la rendre universellement accessible et utile
- **Microsoft** : donner à chaque individu et chaque organisation les moyens de réaliser ses ambitions
- **Facebook** : donner aux gens le pouvoir de partager et de rendre le monde plus ouvert et connecté

# Entreprise : Une stratégie



# Entreprise : Une stratégie

## La vision : L'ambition exprimée de l'organisation

- Une fois la mission définie, la vision de l'organisation doit être élaborée.
- Elle sert à définir l'ambition de l'entreprise, c'est à dire sa cible dans un horizon de temps déterminé (souvent 3 à 5 ans).

- Son énoncé, qui tient souvent en une phrase, doit être clair et si possible objectif. Il est difficile de savoir si on a atteint la vision sans but tangible.

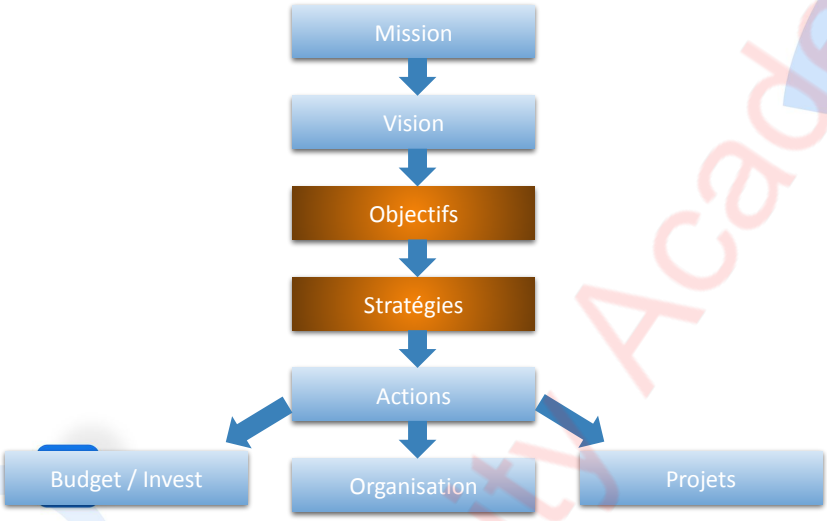
- La vision sera modifiée à chaque nouvel exercice de planification stratégique alors que la mission reste généralement plus stable, à moins d'un changement majeur de positionnement ou d'activité.

# Entreprise : Une stratégie

## Défi de la vision

- Ne pas avoir de vision, c'est aussi subir la tyrannie de l'opérationnel et du court terme.
- Une absence de vision caractérise inéluctablement une absence de projet et d'ambition.
- De fait, le court terme et les affaires courantes seront privilégiés et occuperont le temps et l'énergie des décideurs et des différents acteurs.
- Il vaut mieux se tromper de vision que de ne pas en avoir du tout.

# Entreprise : Une stratégie



# Entreprise : Une stratégie

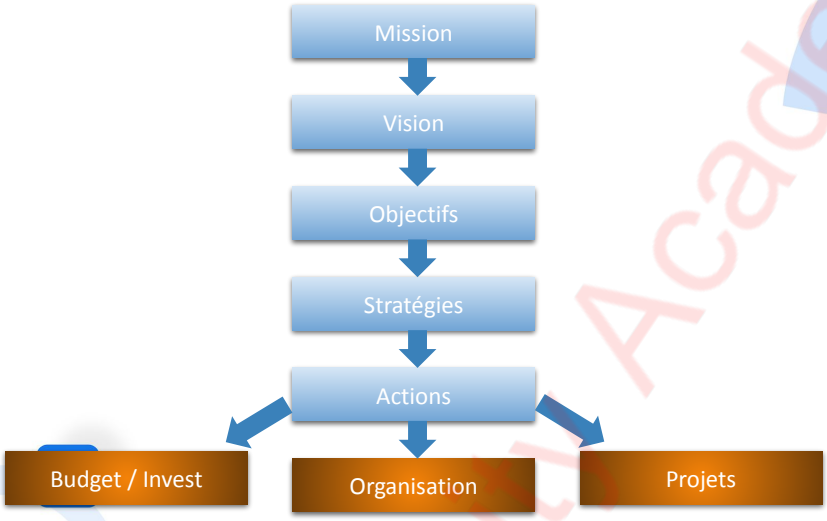
## Défi de la vision

- Une fois la vision définie, l'entreprise détermine les objectifs stratégiques. Ils sont en général au nombre de 3 à 6 et sont clairement qualifiés.

- Les objectifs représentent ce qu'il faut atteindre pour que la vision se réalise. On parle en générale de « ***QUOI*** ».

- Pour chaque objectif défini, 1 à 6 stratégies sont à identifier. Chaque stratégie représente le « ***COMMENT*** », c'est à dire ce qu'il faut faire concrètement pour satisfaire l'objectif stratégique précédemment identifié.

# Entreprise : Une stratégie



# Entreprise : Une stratégie

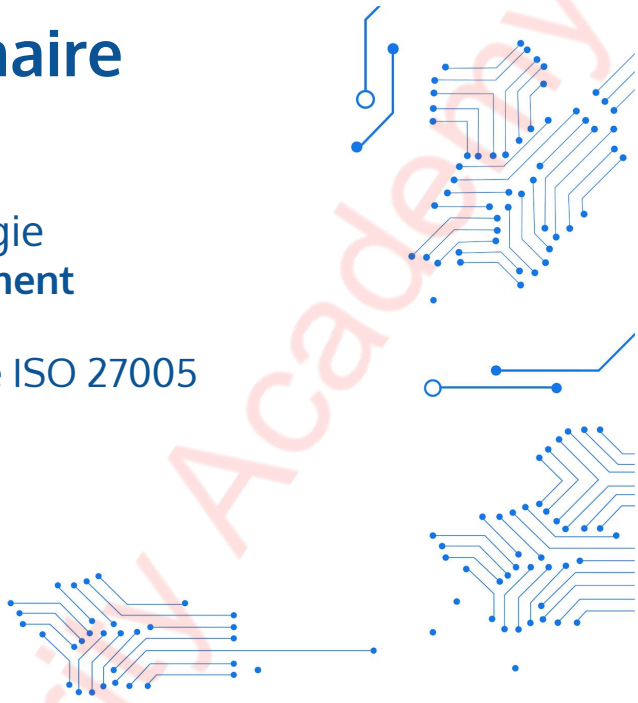
## Stratégies de développement

5 exemples :

- ***La stratégie de "Produit"***
  - Besoins du marché, caractéristiques du produit, services associés, marque, design, labels et normes, etc.
- ***La stratégie de "Distribution"***
  - Circuit court, vente en magasin, vente sur internet , etc.
- ***La stratégie de "Prix"***
  - Cohérence, acceptable par les clients, bénéfices
- ***La stratégie de "Communication"***
  - Quel est mon objectif de communication, à qui vais-je m'adresser, quel message, quel canal, etc.
- ***La stratégie "Commerciale"***
  - Fixer les objectifs dans le temps (exemple : X prospects dans les X jours)
  - Stratégie Push & Pull ( Aller vers les clients ou faire en sorte que les clients viennent à vous)

# Sommaire





Source : ___

___

# Gouvernance et alignement

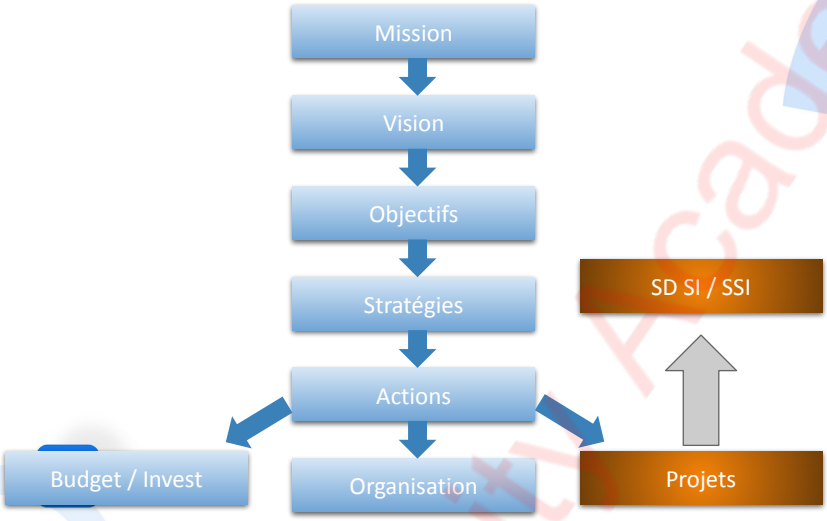
## L'alignement stratégique

- Pour qu'un alignement puisse se faire, encore faut-il que l'entreprise possède une stratégie digne de ce nom qui ne soit pas juste dans la tête de ses dirigeants ou aux abonnées absents.

- Sans stratégie l'alignement est donc impossible.

- Pour réaliser un alignement, il est donc logiquement nécessaire d'avoir et de connaître la stratégie que l'entreprise a élaborée.

# Gouvernance et alignement



# Gouvernance et alignement

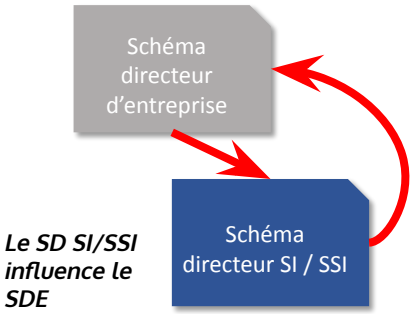
## Stratégie d'entreprise & Schéma directeur

- Le schéma directeur SI / SSI traditionnel prend justement comme point de départ les projets d'entreprise à réaliser.

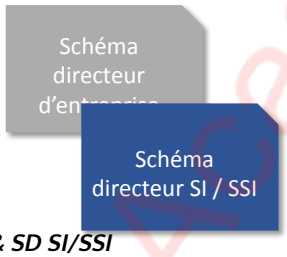
- Il convient donc d'effectuer une extraction des projets ayant une connotation SI / SSI afin de compiler les projets associés à la stratégie de l'organisation.

- Sur cette base, un portefeuille de projets SI avec une première priorisation pourra voir le jour.

# Gouvernance et alignement




***Le SD SI/SSI influence le SDE***




***SDE & SD SI/SSI sont développés conjointement***

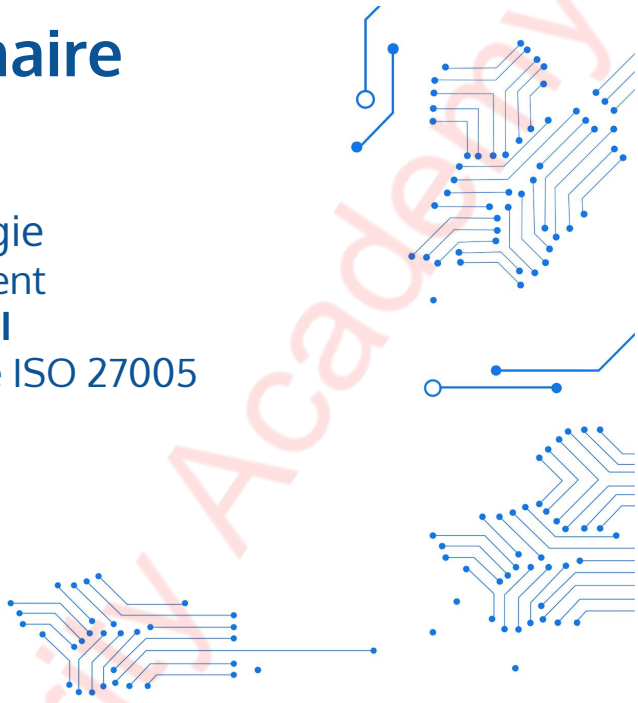
ESD Cybersecurity Academy

# Gouvernance et alignement

## Exercice 1

# Sommaire





Source : ___

___

# La gestion des risques SI

## Les avantages de la gestion des risques

- Accroître la vraisemblance d'atteindre des objectifs.
- Encourager un management proactif.
- Prendre conscience de la nécessité d'identifier et de traiter le risque à travers tout l'organisme.
- Améliorer l'identification des opportunités et des menaces.
- Se conformer aux obligations légales et réglementaires ainsi qu'aux normes internationales.
- Améliorer la gouvernance.
- Établir une base fiable pour la prise de décision.

# La gestion des risques SI

## La gestion des risques ?

- L'analyse de risques est l'ensemble des processus et procédures consistant à calculer la criticité (pertinence et gravité) et la vraisemblance de survenance de dangers pour une organisation.

- Elle vise à les quantifier et/ou les qualifier.

# La gestion des risques SI

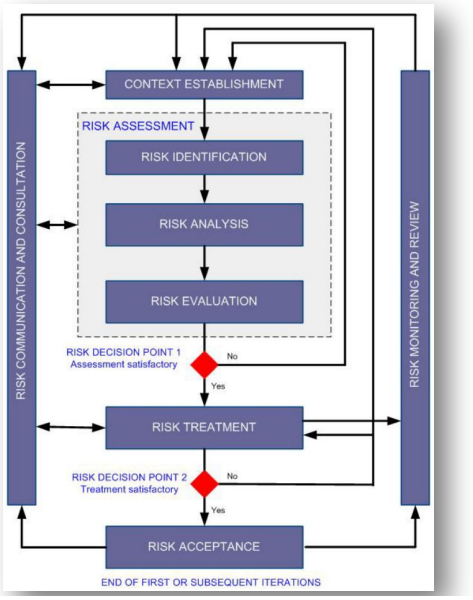
## Une question de perception

Perception du risque


Risques réels

# La gestion des risques SI

## Une norme




- La norme la plus récente en matière de gestion des risques en sécurité de l'information est l'ISO 27005.

- Plusieurs méthodes d'analyse de risques se basent sur les exigences de cette même norme (MEHARI, EBIOS etc…)

# La gestion des risques SI

## Validation et engagement de la direction

- La direction devra :
    - Définir et approuver la politique de management du risque
    - Déterminer des indicateurs de performance du management du risque
    - Aligner les objectifs du management du risque sur les objectifs et les stratégies de l'organisme
    - S'assurer de la conformité légale et réglementaire
    - Affecter les responsabilités aux niveaux appropriés de l'organisme
    - S'assurer que les ressources nécessaires sont allouées au management du risque

# La gestion des risques SI

## Définition des objectifs

- Le but de cette étape est de déterminer les objectifs de l'analyse de risques pour l'organisme.

- Exemple:
    - Soutenir un SMSI
    - S'assurer du respect des exigences légales
    - Valider le respect de contraintes contractuelles ou réglementaires
    - Préparer un PCA/PRA
    - Etc.

# La gestion des risques SI

## Les actifs / biens

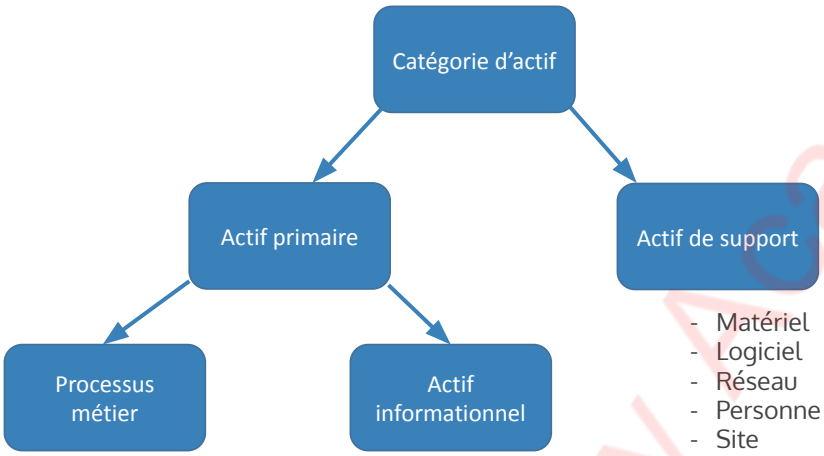
Un actif est tout ce qui a de la valeur pour l'organisme et qui a donc besoin d'une protection.

La norme ISO 27005 utilise la terminologie : ACTIF

La méthode EBIOS 2010 utilise la terminologie : BIEN

# La gestion des risques SI

## Les actifs / biens




- Matériel
- Logiciel
- Réseau
- Personne
- Site
- Organisation

# La gestion des risques SI

## Niveau de profondeur (Zoom)

### Macro Vs Détails

- Le choix de la vision est à sélectionner en fonction du périmètre de l'analyse et donc des objectifs de celle-ci.

# La gestion des risques SI

## Méthodes

- Dans le cas où l'entreprise n'a jamais effectué d'appréciation des risques, le premier travail consiste donc à choisir une méthode.
- Un des premiers points serait donc de sélectionner 4 ou 5 actifs complètement maîtrisés sur lesquels on appliquera la démarche d'appréciation.
- Les questions courantes :
    - Comment valoriser un actif ?
    - Quelle formule pour calculer le risque ?
    - Cela correspond-il vraiment à la réalité du terrain ?

Les tâtons successifs permettront alors de stabiliser la méthode et de la roder.

# La gestion des risques SI

## Evaluation des risques

- Ce processus consiste à analyser et pondérer chaque risque identifié selon les menaces, les vulnérabilités et les impacts associés

**Risque = Gravité * Vraisemblance**

Cette équation implique que le risque est quantifié, ce qui n'est pas toujours facile pour des risques plutôt qualitatifs.

- Selon ***ISO 27005*** :
  - Un risque est l'effet de l'incertitude sur l'atteinte des objectifs

# La gestion des risques SI

## Type de menace

| Type de menace | Exemple |
|---|---|
| 1. Dommage physique | Feu / Dégât d'eau |
| 2. Désastre naturel | Tremblement de terre / Inondation |
| 3. Perte de service essentiel | Panne de climatisation / Panne électrique |
| 4. Perturbation causée par radiation | Radiation |
| 5. Information compromise | Écoute électronique / Vol de documents |
| 6. Panne technique | Bris d'équipement / Saturation de réseau |
| 7. Action non autorisée | Accès non autorisé / Logiciel pirate |

# La gestion des risques SI

## Type de menace

| | Naturelle | Délibérée | Accidentelle |
|---|---|---|---|
| Incendie | X | X | X |
| Abus de privilèges | - | X | X |
| Vol d'équipements | - | X | - |
| Tremblement de terre | X | - | - |

# La gestion des risques SI

## Vulnérabilités

- Faille d'un actif ou d'une mesure de sécurité qui pourrait être exploitée par une menace

# La gestion des risques SI

## Vulnérabilités

| Type de vulnérabilité | Exemple |
|---|---|
| 1. Matériel informatique | Manque d'entretien / Portabilité |
| 2. Logiciel | Pas de logs / Interface complexe |
| 3. Réseau | Pas de chiffrement / Point unique d'accès |
| 4. Personnel | Formation insuffisante / Manque d'encadrement |
| 5. Localisation | Système électrique instable / Zone inondable |
| 6. Structure organisationnelle | Absence de séparation de tâches / Absence de description de tâches |

# La gestion des risques SI

## Vraisemblance

- Réflexion sur la vraisemblance

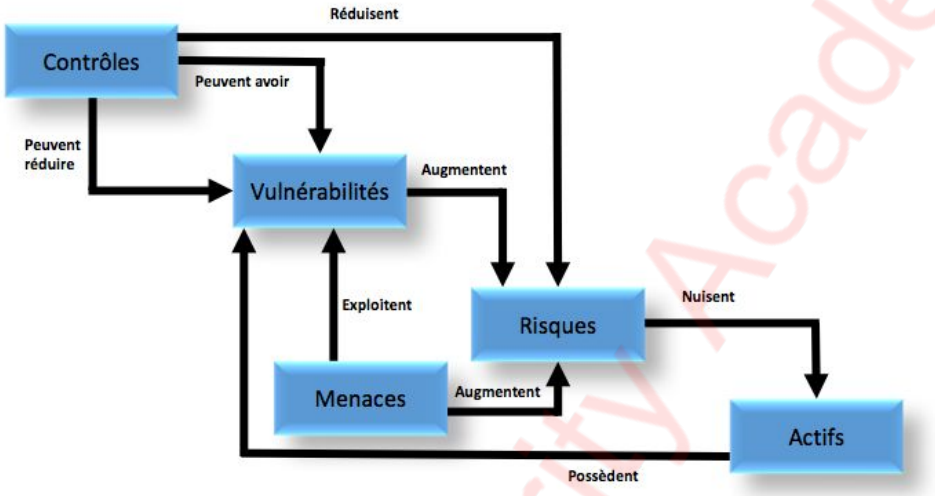
# La gestion des risques SI

## Lien actif, vulnérabilité et menace

| Actif | Vulnérabilité | Menace |
|---|---|---|
| 1. Matériel informatique | Entrepôt non surveillé / Sensibilité à l'humidité | Vol d'équipement / Corrosion |
| 2. Logiciel | Absence d'audit / Interface compliquée | Abus de droits non détecté / Erreur de saisie |
| 3. Réseau | Communication non protégée / Mot de passe en clair | Écoute électronique / Hacker |
| 4. Personnel | Formation insuffisante / Manque de supervision | Erreur / Vol d'équipement, erreurs |
| 5. Localisation | Endroit inondable / Réseau électrique instable | Inondation / Perte de courant |
| 6. Structure organisationnelle | Absence de processus d'autorisation de droits d'accès / Absence de processus de gestion documentaire | Abus de privilèges / Corruption de données |

# La gestion des risques SI

## Lien actif, vulnérabilité et menace



# La gestion des risques SI

## Traitement des risques

# La gestion des risques SI

## Evaluation des options de traitement

**Modifier le risque:**
Mesures de sécurité sélectionnées pour diminuer le risque

**Maintenir le risque:**
La direction décide d'assumer le risque

**Partager le risque:**
Décision de partager certains risques avec des parties externes : assurances ou infogérances

**Éviter le risque:**
Annulation ou modification d'une activité ou d'un ensemble d'activités liés au risque

# La gestion des risques SI

## Le plan de traitement des risques

- Une fois que les décisions de traitement des risques ont été prises, les activités pour mettre en œuvre ces décisions doivent être identifiées et planifiées :
    - Identification et planification des activités impactées par le plan de traitement des risques
    - Classement par ordre de priorité des activités sélectionnées
    - Déploiement des ressources nécessaires pour le plan de traitement

# La gestion des risques SI

## Les risques résiduels

Risque Net = Risque Brut – Efficacité des mesures existantes

Risque résiduels = Risque Net – Efficacité des mesures (traitement)

# Sommaire



Source : ___

___

# Présentation de la norme ISO 27005

La norme ISO 27005 != Méthode

# Présentation de la norme ISO 27005

## La norme

- L'ISO/CEI 27005:2018 contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.
- Elle vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001 ; elle est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.
- Les normes ISO sont ré-examinées tous les cinq ans (généralement)

# Présentation de la norme ISO 27005

## Certification ?

- La norme ISO 27005 ne décrit qu'une démarche, elle ne permet pas la certification d'un système, contrairement à la norme ISO 27001.

- Cependant, la compétence d'un Gestionnaire de Risque, pour l'application pratique de la norme ISO 27005, peut être reconnue par une certification de personne, à l'issue d'une formation "ISO 27005 Risk Manager".

# Présentation de la norme ISO 27005

## Processus (Rappel)