Une affaire de standards

l'ISO, Organisation internationale de normalisation, «*International organization for standardization***»**

- organisation internationale, créée en 1947 ;
- composée de représentants des organismes de normalisation nationaux d'environ 150 pays ;
- produit des normes internationales dans les domaines industriels et commerciaux.

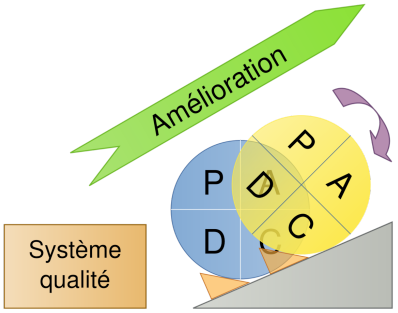
Différentes normes, IS, «*International Standard*» :

- IS 9000 : consacrée à la définition d'un «*système de management*» :
  - établir une politique et fixer des objectifs :
    - référentiel écrit ;
    - ensemble de mesures organisationnelles et techniques destinées à mettre en place un certain contexte organisationnel et à en assurer la pérennité et l'amélioration ;
  - vérifier que l'on a atteint les objectifs fixés :
    - réaliser un *audit* qui consistera à comparer le référentiel à la réalité pour relever les divergences, nommées *écarts* ou *non-conformités*.
    - sans référentiel, l'auditeur en peut réaliser sa mission ;
      mais il existe de nombreux référentiels…
- IS 9001 : consacrée aux systèmes de management de la qualité et aux exigences associées ;
- IS 14001 : consacrée aux systèmes de management de l'environnement ;
- IS 27001 : consacrée aux **systèmes de management de la sécurité de l'information** ;
- IS 19001 : directives à respecter pour la conduite de l'audit d'un système de management.

La norme ISO 27001

Système de management de la sécurité de l'information ou SMSI

- s'applique à un SMSI ;
- fournie un schéma de certification pouvant être appliqué au SMSI au moyen d'un audit ;
- s'appuie sur une approche *par processus* : exemple du PDCA, «*Plan, Do, Check, Act*» :



  - phase **Plan** :
    - définir lechamp du SMSI,
    - identifier et évaluer les risques,
    - produire le document (*Statement of applicability*, SOA) qui énumère les mesures de sécurité à appliquer ;
  - phase **Do** :
    - affecter les ressources nécessaires,
    - rédiger la documentation,
    - former le personnel,
    - appliquer les mesures décidées,
    - identifier les risques résiduels ;
  - phase **Check** : audit et revue périodiques du SMSI, qui produisent des constats et permettent d'imaginer des corrections et des améliorations ;
  - phase **Act** :
    - prendre les mesures qui permettent de réaliser les corrections et les améliorations dont l'opportunité a été mise en lumière par la phase Check,
    - préparer une nouvelle itération de la phase Plan.

La norme ISO 27001

Le SMSI a pour buts de :

- **maintenir et d'améliorer la position** de l'organisme qui le met en œuvre du point de vue :
  - de la compétitivité,
  - de la profitabilité,
  - de la conformité aux lois et aux règlements,
  - de l'image de marque.
- **protéger les actifs «**assets**»** de l'organisme, définis au sens large comme *tout ce qui compte pour lui*.

Le vocabulaire du SMSI est fournie dans l'IS 27000.

Les mesures de sécurité énumérées dans la phase Plan peuvent être prises dans le **catalogue** de «mesures» et «bonnes pratiques» proposé par l'IS 27002.

Les méthodes d'analyse des risques

IS 27001 impose une **analyse des risques**, mais **ne propose aucune méthode** pour la réaliser :

- **liberté de choisir** une méthode pour le SMSI, à condition que :
  - elle soit documentée ;
  - elle garantisse que les évaluations réalisées avec son aide produisent des résultats **comparables** et **reproductibles**.
- Un risque identifié peut être :
  - accepté,
  - transféré à un tiers (assurance, prestataire),
  - réduit à un niveau accepté.

Exemples de méthodes d'analyse des risques :

- IS 27005, méthode d'analyse fournie par l'ISO ;
- EBIOS®, «*Expression des Besoins et Identification des Objectifs de Sécurité*» : méthode d'évaluation des risques en informatique, développée par l'**Agence nationale de la sécurité des systèmes d'information** (ANSSI).
- MEHARI, «*Méthode harmonisée d'analyse des risques*» : méthode visant à la sécurisation informatique d'une entreprise ou d'un organisme. Elle a été développée et est proposée par le **Club de la Sécurité de l'Information Français**, CLUSIF.

Pour obtenir une certification IS 27001

- définir le champ du SMSI ;
- en formuler la politique de management ;
- préciser la méthode d'analyse de risques utilisée ;
- identifier, analyser et évaluer les risques ;
- déterminer les traitements qui seront appliqués aux différents risques, ainsi que les moyens d'en vérifier les effets ;
- attester l'engagement de la direction de l'organisme dans la démarche du SMSI ;
- rédiger le *Statement of Applicability* (SOA) qui sera la charte du SMSI et qui permettra de le soumettre à un audit.

Les méthodes et l'aspect législatif

Les différents IS

- IS 27001 : système de management de la sécurité des systèmes d'information (SMSI) ;
- IS27000 : vocabulaire SSI ;
- IS 27002 (ex-17799) : catalogue de mesures de sécurité ;
- IS 27003 : implémentation du SMSI ;
- IS 27004 : indicateurs de suivi du SMSI ;
- IS 27005 : évaluation et traitement du risque ;
- IS 27006 : certification du SMSI ;
- IS 27007 : audit du SMSI.

L'historique et l'évolution de la législation

– juillet 2002, USA : loi Sarbanes-Oxley, «*SOX*» : impose aux entreprises qui font appel au capital public (cotées en bourse) toute une série de règles comptables et administratives destinées à assurer la traçabilité de leurs opérations financières, pour garantir plus de transparence pour les actionnaires (éviter les comptes truqués comme dans le cas du scandale «Enron») ;

– 1er août 2003, France : loi du sur la sécurité financière (LSF) qui concerne principalement trois domaines :
  - modernisation des autorités de contrôle des marchés financiers ;
  - sécurité des épargnants et des assurés ;
  - contrôle légal des comptes ainsi que la transparence et le gouvernement d'entreprise. *Cette loi française ne concerne pas seulement les sociétés cotées, mais toutes les sociétés anonymes.*

– 2004, dispositif réglementaire européen «Bâle 2» qui concerne les établissements financiers.

La loi Sarbanes-Oxley concerne la sécurité du système d'information : elle impose aux entreprises des procédures de contrôle interne, de conservation des informations, et de garantie de leur exactitude :

▷ *la continuité des opérations ;*
▷ *la sauvegarde et l'archivage des données ;*
▷ *l'externalisation et son contrôle.*

Qu'est-ce qu'un système d'Information ?

Une définition du système d'information

« Tout moyen dont le fonctionnement fait appel à l'électricité et qui est destiné à élaborer, traiter, stocker, acheminer, présenter ou détruire l'information »

1. Les enjeux de la sécurité des S.I.

a. Préambule

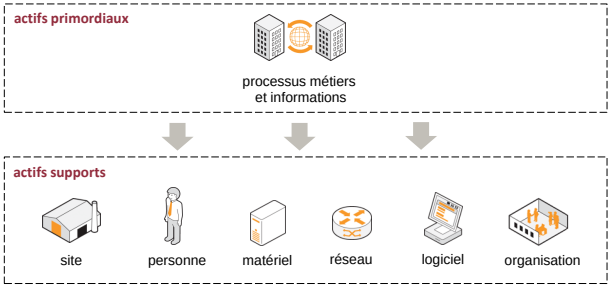
- Système d'Information (S.I.)
  - Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation
  - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de l'organisation

1. Les enjeux de la sécurité des S.I.

a. Préambule

- Le système d'information d'une organisation contient un ensemble d'actifs :



ISO/IEC 27005:2008

La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

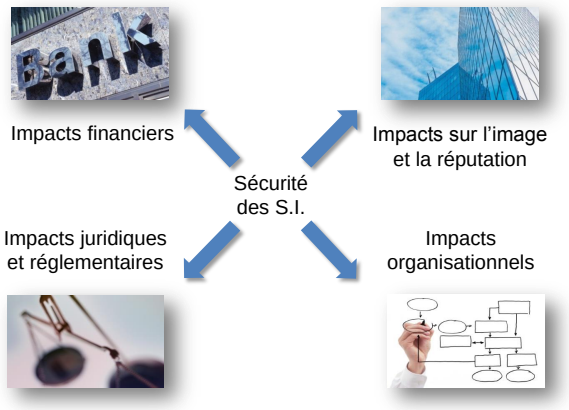
1. Les enjeux de la sécurité des S.I.

b. Les enjeux

- La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations…
- La gestion de la sécurité au sein d'un système d'information n'a pas pour objectif de faire de l'obstruction. Au contraire :
  - Elle **contribue à la qualité de service que les utilisateurs** sont en droit d'attendre
  - Elle **garantit au personnel le niveau de protection** qu'ils sont en droit d'attendre

1. Les enjeux de la sécurité des S.I.

b. Les enjeux



1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- Les motivations évoluent
  - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
  - De nos jours : majoritairement des actions organisées et réfléchies
- Cyber délinquance
  - Les individus attirés par l'appât du gain
  - Les « hacktivistes »
  - Motivation politique, religieuse, etc.
  - Les concurrents directs de l'organisation visée
  - Les fonctionnaires au service d'un état
  - Les mercenaires agissant pour le compte de commanditaires
  - …

1. Les enjeux de la sécurité des S.I.

c. Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires
- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)
- **Chantage**
  - Déni de service
  - Modifications des données
- **Espionnage**
  - Industriel / concurrentiel
  - Étatique
- …

Qu'est-ce que la sécurité informatique ?

D'après Wikipedia

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.

La sécurité informatique a pour objectif de **maintenir**, à **un niveau convenable** (défini par la direction générale), les garanties suivantes :

- **Disponibilité** : garantie que les entités autorisées ont accès à tout moment aux éléments considérés.
- **Intégrité** : garantie que les ressources sont exactes et complètes (non corrompues).
- **Confidentialité** : garantie que les ressources sont accessibles au moment voulu par les entités autorisées.
- **Traçabilité** : garantie que les accès et tentatives d'accès aux ressources sont tracés et que ces traces sont conservées et exploitables.

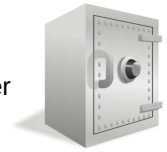
Ces quatre principes combinés, «*DICT*», permettent d'assurer un **niveau de sécurité suffisamment élevé** pour satisfaire au besoin de sécurité des données de l'entreprise concernée.

2. Les besoins de sécurité

a. Introduction aux critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger



Disponibilité
Propriété d'accessibilité au moment voulu des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité
Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

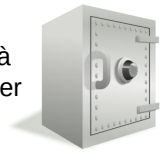
Confidentialité
Propriété des biens de n'être accessibles qu'aux personnes autorisées

2. Les besoins de sécurité

b. Besoin de sécurité : « Preuve »

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 1 critère complémentaire est souvent associé au D.I.C.

Bien à protéger



Preuve
Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe Notamment :
La traçabilité des actions menées
L'authentification des utilisateurs
L'imputabilité du responsable de l'action effectuée

2. Les besoins de sécurité

d. Exemple d'évaluation DICP

Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.

L'expression du besoin attendu peut-être d'origine :
- **Interne** : inhérente au métier de l'entreprise
- ou **externe** : issue des contraintes légales qui pèsent sur les biens de l'entreprise.

Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :

Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible

Le bien bénéficie d'un niveau de sécurité adéquat

2. Les besoins de sécurité

d. Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site institutionnel simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

Disponibilité = **Très fort**

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaitre ses services au public

Intégrité = **Très fort**

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)

Serveur web

Confidentialité = **Faible**

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = **Faible**

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

2. Les besoins de sécurité

c. Différences entre sureté et sécurité

« Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

Sûreté

Protection contre les dysfonctionnements et accidents involontaires

Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.

Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)

Parades : sauvegarde, dimensionnement, redondance des équipements…

Sécurité

Protection contre les actions malveillantes volontaires

Exemple de risque : blocage d'un service, modification d'informations, vol d'information

Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts

Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage…*

* Certaines de ces parades seront présentées dans ce cours

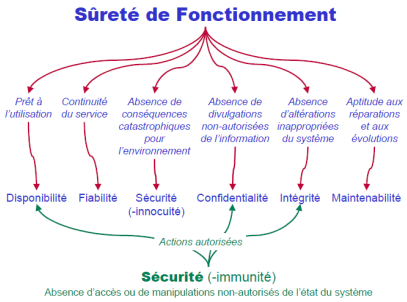
2. Les besoins de sécurité

c. Différences entre sureté et sécurité

Sûreté : ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.

Sécurité : ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Le périmètre de chacune des 2 notions n'est pas si clairement délimité dans la réalité : dans le cas de la voiture connectée on cherchera la sécurité et la sûreté.



On constate sur le schéma que la notion de sécurité diffère selon le contexte :

- sécurité ▶ innocuité
- sécurité ▶ immunité

La méthode MEHARI «*Method for Harmonized Analysis of Risk*»

▷ méthode intégrée et complète d'évaluation et de management des risques visant à sécuriser les systèmes d'information d'une entreprise ou d'une organisation ;

▷ développée, diffusée et mise à jour par le club professionnel CLUSIF depuis 1996 ;

▷ mise à jour en 2010 pour respecter les lignes directrices de la norme ISO 27005 : 2009 ;

▷ utilisable dans le cadre d'un système de gestion de la sécurité de l'information de la norme ISO 27001 : 2005.

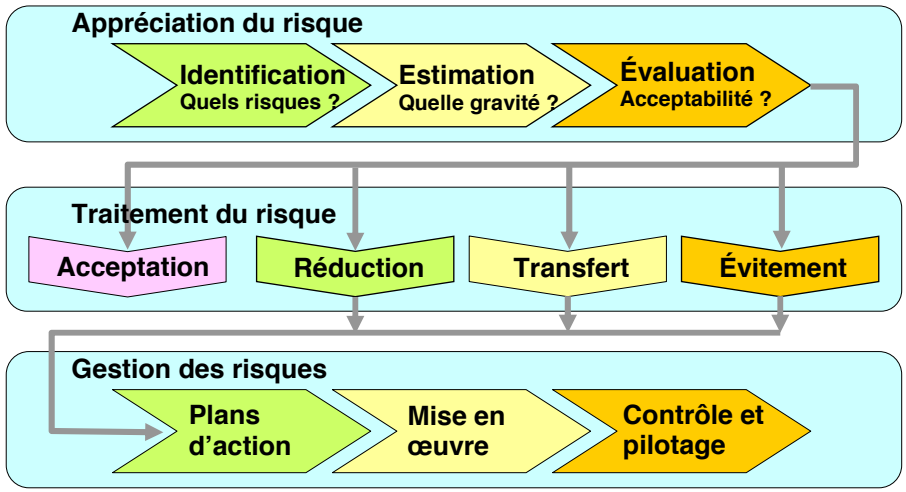
Une méthodologie en 3 étapes

I. l'**appréciation des risques** :
   a. identifier les risques du système d'information à partir d'une base de connaissance ;
   b. estimer la potentialité et l'impact de ces risques afin d'obtenir leur gravité
   c. évaluer l'acceptabilité ou non de ces risques.

II. le **traitement des risques** : prendre une décision pour chaque risque :
   ◇ accepter
   ◇ réduire
   ◇ transférer
   ◇ éviter.

III. la **gestion des risques** : établir des plans d'action de traitement des risques, des mises en œuvre de ces plans, mais aussi des contrôles et des pilotages de ces plans.

La méthode MEHARI «*Method for Harmonized Analysis of Risk*»



MÉthode Harmonisée d'Analyse des RIsques

Appréciation des risques

I. identifier tous les risques auxquels l'organisation est exposée ;
II. pour chacun des risques :
   - ◇ estimer sa **gravité** ;
   - ◇ juger de son acceptabilité.

Attention

Tout risque ignoré ne sera l'objet d'aucune analyse ni d'aucun traitement.

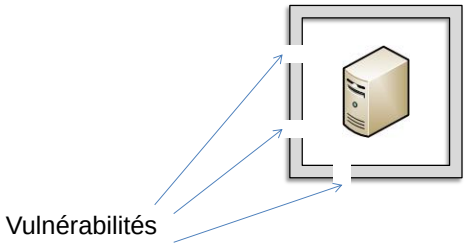
Identifier les risques

- ⋆ l'actif :
  - ◇ ce qui peut subir un **dommage** ;
  - ◇ le fait qu'un actif puisse subir un dommage crée un **risque** ;
  - ◇ la **gravité** associée à la survenance du risque **dépend de la nature** de cet actif ;
  - ◇ deux sortes d'actifs :
    - ⋆ **primaires** : les besoins de l'entreprise ;
    - ⋆ **secondaires**, ou «de support» : les différentes formes que peuvent prendre les actifs primaires.
- ⋆ la **vulnérabilité** : un actif peut posséder une ou plusieurs vulnérabilités intrinsèques qui entraîne des risques. Ces vulnérabilités dépendent du type d'*actif secondaire* (matériel, logiciel, *etc.*)
- ⋆ le **dommage subi** : exprimé suivant des **critères de conséquences** : disponibilité, intégrité et confidentialité.
- ⋆ la **menace** : cause d'exploitabilité (l'événement déclencheur) et une *probabilité d'occurence* d'un risque.

3. Notions de vulnérabilité, menace, attaque

a. Notion de « Vulnérabilité »

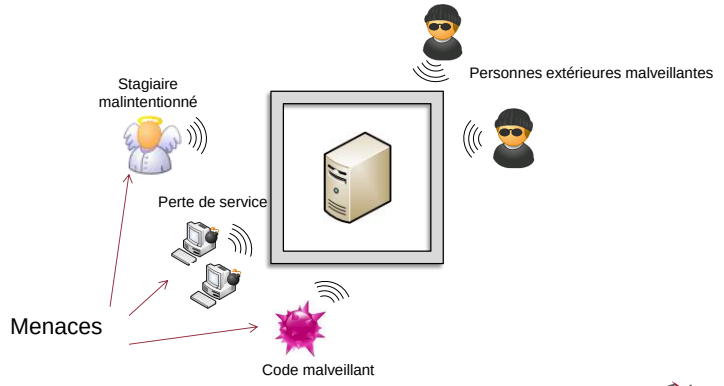
- **Vulnérabilité**
- **Faiblesse au niveau d'un bien** (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).



3. Notions de vulnérabilité, menace, attaque

b. Notion de « Menace »

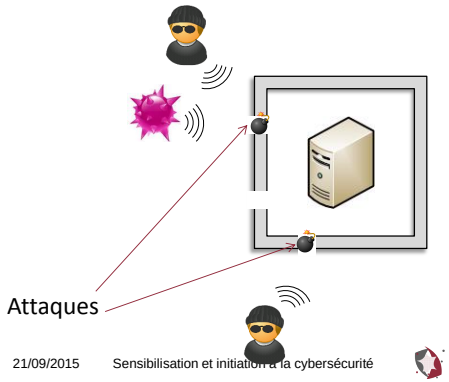
- **Menace**
- **Cause *potentielle* d'un incident**, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

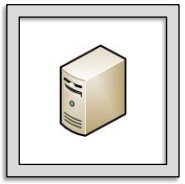
- **Attaque**
- **Action malveillante** destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**



3. Notions de vulnérabilité, menace, attaque

c. Notion d'« Attaque »

- **Attaque**
- Une attaque ne peut donc avoir lieu (et réussir) que si le bien est affecté par une vulnérabilité.

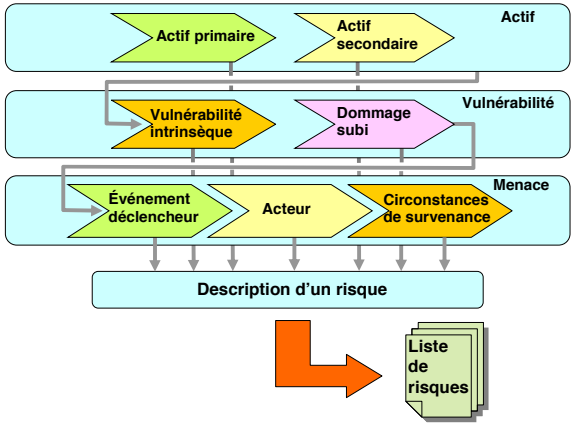


Ainsi, tout le travail des experts sécurité consiste à s'assurer que le S.I. ne possède aucune vulnérabilité.

Dans la réalité, l'objectif est en fait d'être en mesure de maitriser ces vulnérabilités plutôt que de viser un objectif 0 inatteignable.

Processus global d'élaboration des risques

- ▷ **Actifs primaires** *les besoins de l'entreprise* :
  - ◇ services : informatiques, télécommunication, généraux ;
  - ◇ données nécessaires au fonctionnement des services ;
  - ◇ processus de gestion.
- ▷ **Actifs secondaires** *les diverses formes et contingences des actifs primaires* :
  - ◇ moyens nécessaires à la réalisation des besoins fonctionnels décrits par les actifs primaires.



Un **risque** doit comprendre la description de l'actif en précisant l'actif primaire et secondaire.

Une **menace** comporte :

- ⋆ l'événement déclencheur et son caractère volontaire ou accidentel ;
- ⋆ l'acteur déclenchant cet événement ;
- ⋆ les circonstances dans lesquelles survient cet événement.

chacun de ces paramètres influe sur la probabilité d'occurrence de ce risque.

Exemples de risques, de scenarii et de préconisations : à la maison

Inventaire

Biens (maison, hi-fi, bijoux, ordinateur, etc.), personnes (famille, bébé, jeune enfant, etc.), animaux

Vulnérabilités/Services de sécurité

Porte, fenêtre, absence dans la journée ou les congés, présence de voisins, détecteurs incendie, etc.

Menaces

Cambriolage, incendie, inondation, etc.

Scénarii de risques

Incendie dans la chambre du bébé, vol avec effraction, etc.

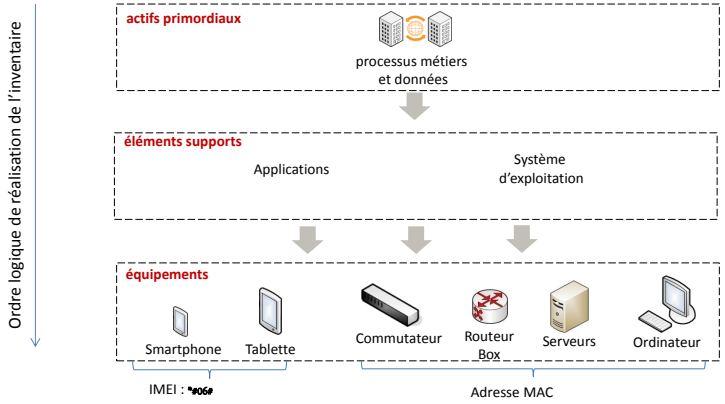
Préconisations

Mise en place de détecteurs de fumée, d'alarmes intrusion, etc.

1. Connaître le Système d'Information

a. Identifier les composants du S.I.

Différents éléments composent le SI



Comprendre son S.I. passe par l'identification de ses composants.

Actifs primaires & Secondaires

Primaires

Catégorie d'actifs : Services
Services du réseau étendu
Services du réseau local
Services applicatifs
Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)
Services systèmes communs : messagerie, archivage, impression, édition, etc.
Services d'interface et terminaux mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)
Services de publication d'informations sur un site web interne ou public
Services généraux de l'environnement de travail du personnel (bureaux, énergie, climatisation, etc.)
Services de télécommunication (voix, télécopies, visioconférence, etc.)

Secondaires

TYPES D'ACTIFS SECONDAIRES
Catégorie d'actifs : Services
Équipements matériels supports du service
Configurations logicielles
Media support de logiciel
Comptes et moyens nécessaires à l'accès au service
Services de sécurité associés au service
Moyens de servitude nécessaires au service
Locaux
Personnels et prestataires nécessaires pour le service (internes et externes)

Actifs primaires & Secondaires

Primaires

Catégorie d'actifs : Données
Fichiers de données ou bases de données applicatives
Fichiers bureautiques partagés
Fichiers bureautiques personnels (gérés dans un environnement personnel)
Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles
Listings ou états imprimés des applications informatiques
Données échangées, écrans applicatifs, données individuellement sensibles
Courrier électronique
Courrier postal et télécopies
Archives patrimoniales ou documentaires
Archives informatiques
Données et informations publiées sur un site web ou interne

Secondaires

Catégorie d'actifs : Données
Entités logiques : Fichiers ou bases de données
Entités logiques : Messages ou paquets de données en transit
Entités physiques : media et supports
Moyens d'accès aux données : clés et moyens divers, physiques ou logiques, nécessaires pour accéder aux données

Actifs primaires & Secondaires

Primaires

Catégorie d'actifs : Processus de management
Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels
Conformité à la loi ou aux réglementations relatives à la communication financière
Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée
Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle
Conformité à la loi relative à la protection des systèmes informatisés
Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement

Secondaires

Catégorie d'actifs : Processus de management
Procédures et directives internes (dispositifs organisationnels)
Moyens matériels nécessaires aux processus de management
Personnel et prestataires nécessaires aux processus de management

Estimation des risques

Pour estimer la gravité de chaque risque identifié, il faut tenir compte de :
- la gravité de risque intrinsèque (sans tenir compte des mesures de sécurité) ;
- la gravité de risque résiduelle (en tenant compte des mesures de sécurité).

Pour mesurer le risque, on utilise 2 paramètres :
- la probabilité ou la vraisemblance, appelée *potentialité*.
- la gravité des conséquences, appelé *impact*.

MEHARI fournit une échelle de potentialité et une échelle d'impact, standards à 4 niveaux.

La potentialité intrinsèque d'un risque

C'est la *probabilité maximale* de survenance du risque en l'absence de toute mesure de sécurité.
Elle dépend :
- ⋆ de la localisation et de l'environnement de ce risque ;
- ⋆ de l'enjeu d'un acte volontaire pour son auteur ;
- ⋆ de la probabilité qu'une action volontaire vise précisément l'organisation.

Exemple : une entreprise de haute technologie est plus explosée au risque d'espionnage alors qu'une entreprise traitant des flux financiers est plus exposée aux tentatives de fraudes.

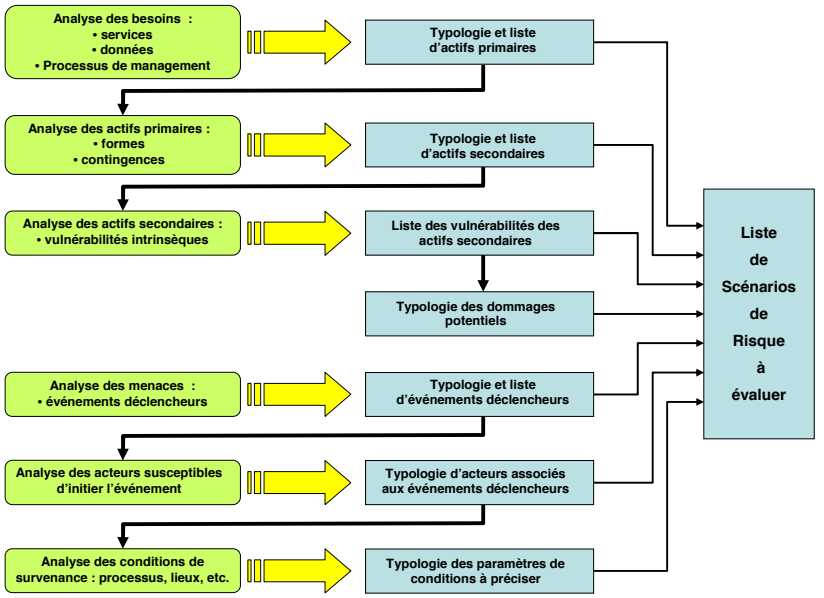
L'impact intrinsèque

C'est le *niveau maximum* des conséquences possibles pour l'organisation en l'absence de toute mesure de sécurité.

Les mesures de sécurité

Ce sont des facteurs de *réduction des risques* :
- □ **Facteurs de réduction de potentialité** :
  - ◇ cumulables : empêcher totalement un événement de se produire, interdire une action humaine, *etc.*
  - ◇ deux types :
    - ⋆ **Dissuasion** : rendre moins probable que l'acteur passe à l'action.
      Elle repose sur 3 principes :
      - ▷ l'imputabilité de l'action à son auteur ;
      - ▷ l'existence de sanctions ;
      - ▷ la connaissance par l'auteur des possibilités d'imputation et des sanctions.
    - ⋆ **Prévention** : rendre moins probable que l'action aboutisse à la réalisation du risque : mesures techniques et de mécanismes de contrôle.
- □ **Facteurs de réduction d'impact** :
  - ◇ cumulables : limiter les conséquences directes possibles, prévoir la réparation d'un équipement suite à un sinistre, *etc.*
  - ◇ deux types :
    - ⋆ **Confinement** : limiter l'ampleur des conséquences directes : fixation de limites telle que des limites physiques, fixation de points de contrôle intermédiaires, *etc.*
    - ⋆ **Effet palliatif** : minimiser les conséquences indirectes du risque par une anticipation de la gestion du risque : plans de maintenance matérielle et logicielle, plans de sauvegarde et de restauration de données, *etc.*

Estimation des risques



Évaluation des risques dans MEHARI

MEHARI propose trois types de gravité de risque :
- ⋆ les risques insupportables : ils doivent faire l'objet de mesure d'urgence.
- ⋆ les risques inadmissibles : ils doivent être éliminés ou réduits à une échéance fixée.
- ⋆ les risques tolérés.

Pour savoir dans quel type se range un risque, on :
- ▷ détermine sa gravité globale ;
- ▷ consulte la *Grille d'acceptabilité des risques*.

La **G**ravité globale d'un risque dépend de sa **P**robabilité et de son **I**mpact :

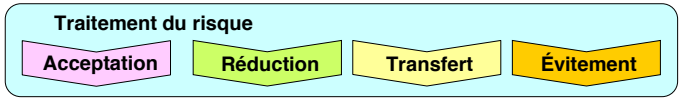
4	risque insupportable
3	risque inadmissible
1& 2	risque toléré.

	P = 1	P = 2	P = 3	P = 4
I = 4	G = 2	G = 3	**G = 4**	**G = 4**
I = 3	G = 2	G = 3	G = 3	**G = 4**
I = 2	G = 1	G = 2	G = 2	G = 3
I = 1	G = 1	G = 1	G = 1	G = 2

L'utilisation d'une grille prédéterminée permet de :
- déterminer quelle décision prendre en terme « *d'acceptabilité du risque* » ;
- assurer la cohérence des décisions prises.

Traitement des risques

Les options principales conformes à la norme IS 27005



- ▷ **accepter** : l'entreprise accepte de rien faire vis-à-vis de cette situation :
  - ◇ le risque a été évalué comme acceptable dans la « grille d'acceptabilité des risques » ;
  - ◇ pour des raisons économiques, il a été jugé impossible d'y remédier ;
  - ◇ le risque est connu et sera surveillé dans le futur.
- ▷ **réduire** : sélectionner des services de sécurité dans une « **base de connaissance** » où chaque service est décrit avec
  - ◇ sa finalité/objectif ;
  - ◇ les mécanismes techniques/organisationnels pour sa mise en œuvre ;
  - ◇ un niveau de qualité suivant une échelle de niveau permettant de :
    - ⋆ donner une valeur globale lors de la combinaison de plusieurs services ;
    - ⋆ vérifier que le risque est ramené à un **niveau de gravité acceptable**.
- ▷ **transférer** : généralement en ayant recours à une assurance mais aussi en transférant la charge sur un tiers responsable par une action en justice.
- ▷ **éviter** : réduction par des mesures structurelles :
  - ◇ déménager en cas de risque d'inondation ;
  - ◇ limiter les encours disponibles en cas de risque de vol.

2. Les besoins de sécurité

e. Mécanismes de sécurité pour atteindre les besoins DICP

Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie :

		D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dument habilitées		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

Gestion des risques

- ◦ intervient après les décisions de traitement de risques ;
- ◦ comprend l'ensemble des processus qui vont permettre de :
  - ◇ mettre en œuvre ces décisions ;
  - ◇ en contrôler les effets ;
  - ◇ les améliorer si nécessaire ;

Élaboration des plans d'action

- – mise en place de services de sécurité, avec, pour chacun, un objectif de niveau de qualité ;
- – mesures structurelles visant à réduire l'exposition à certains risques ;
- – mesures organisationnelles visant à éviter certains risques.

En raison de contraintes de budget, de personnels, toutes ces actions ne peuvent être entreprises immédiatement :

- ▷ choix des objectif prioritaires en terme de services de sécurité et optimisation de ce choix ;
- ▷ transformation de ces choix de services de sécurité en **plans d'action concrets** ;
- ▷ choix des mesures structurelles et des mesures d'évitement des risques ;
- ▷ **validation** des décisions précédentes.

Gestion des risques

Choix des objectifs prioritaires et optimisation

Pour définir les priorités, il faut tenir compte de :

- – les niveaux de gravité des risques que les mesures prioritaires permettront de réduire : les risques de niveau le plus élevé doivent être traités en premier ;
- – le nombre de risques traités et le nombre de risques dont le traitement sera remis à plus tard ;
- – la rapidité avec laquelle les premiers résultats pourront être observés ;
- – l'incidence de ces choix sur la sensibilisation du personnel ;
- – *etc.*

Des outils informatiques d'optimisation peuvent aider à déterminer ces choix.

Choix des solutions : mécanismes techniques et organisationnels

Le choix revient au équipes et personnels spécialisés : DSI, «Direction des Systèmes d'Information», responsables réseaux, responsables de la sécurité physique, RSSI *etc.*

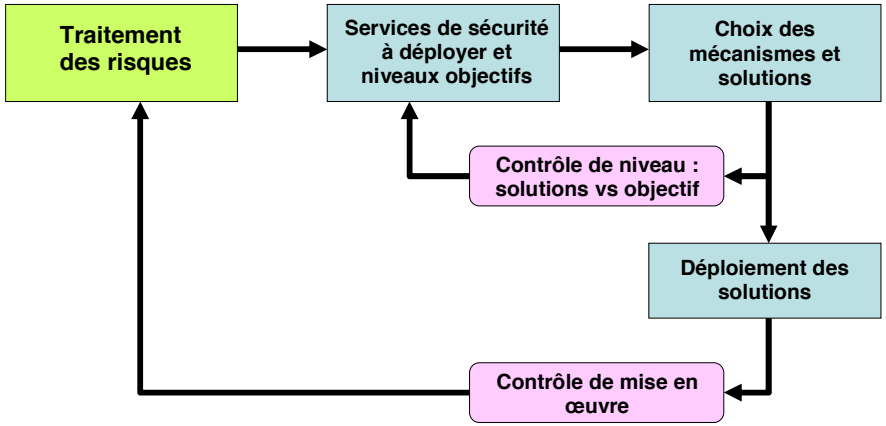
Regroupés dans un «*manuel de références des services de sécurité*», chaque service de sécurité :

- □ l'**objectif** du service ;
- □ les **résultats attendus** de la mise en œuvre du service ;
- □ la description des **mécanismes** associés à chaque service techniques et organisationnels ;
- □ les éléments permettant d'évaluer la **qualité** de chaque service :
  - ◇ efficacité ; ◇ robustesse ; ◇ mise sous contrôle ;

L'utilisation de ce manuel garantit la concordance entre les fonctionnalités attendues par les gestionnaires de risques et les estimations des facteurs de réduction de risques utilisées pour les sélectionner.

MEHARI propose un manuel de référence de services de sécurité.

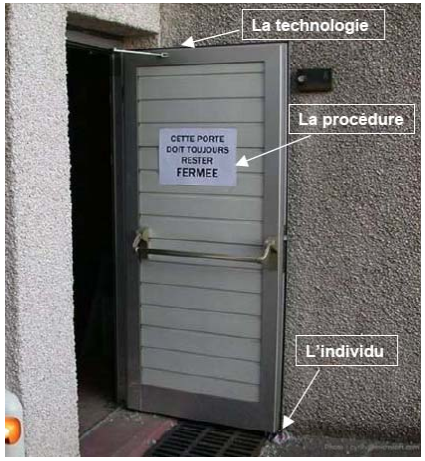
Contrôle et pilotage de la gestion directe des risques



Contrôle à effectuer :

- **premier niveau** : contrôler que les mécanismes et solutions de sécurité planifiés et décidés correspondent bien aux niveaux de qualité de service retenus en phase de traitement des risques ;
- **second niveau** : contrôler la mise en œuvre.

Gestion des risques : ne pas négliger le facteur humain !



La sécurité du système d'information dans l'entreprise

RSI
«Responsable du Système d'Information»

- assure la gestion et l'exploitation du SI dont il a la responsabilité ;
- connait tous les aspects aussi bien techniques, qu'organisationnels du SI dont il sert de personne de référence.

RSSI
«Responsable de la Sécurité du SI»

- sécurise le SI afin de garantir :
  - disponibilité ;
  - intégrité ;
  - confidentialité ;
- gère la sécurité au quotidien d'une manière globale, aussi bien technique qu'organisationnelle.

- PRA, *«plan de retour d'activité»* ;
- PCA, *«plan de continuité d'activité»* :
  - permet d'éviter une interruption de service qui engendrerait un PRA (reprise).
  - demande une surveillance pour fournir une continuité de service (outils de métrologie par exemple).
- SMSI, «Système de Management de la Sécurité de l'Information»
- PSSI, «Politique de Sécurité des Systèmes d'Information» : plan d'actions définies pour maintenir un certain niveau de sécurité.

PCA et PRA

PCA, «Plan de Continuité d'Activité»

But : **continuer** l'activité en cas d'incident ou de crise :
- sans perte de service ;
- avec une légère dégradation acceptable.

Exemple : *télétravail en cas de grève des transports en commun.*

PRA, «Plan de Reprise d'Activité»

But : **reconstruire** ou **basculer** sur un système de relève pour une durée déterminée en cas de crise majeure ou de sinistre :
- fournir les besions informatiques nécessaires à la survie de l'entreprise ;
- s'appui sur :
  - RPO, *«Recovery Point Objective»*, c-à-d un risque défini de perte de données ;
  - RTO, *«Recovery Time Objective»*, c-à-d une durée acceptable d'interruption.

Exemple : *basculement vers un «*DataCenter*» sur un site de secours en cas d'incendie.*

Des obligations

- Réglementation CRBF2004-02 (issue de IASB Bâle II) : obligation d'un plan de secours opérationnel pour les établissements financiers, banques et assurances.
- Code du commerce art. L.123-22 : conservation des documents comptables pendant 10 ans.
- Décret du 24 mars 2006 : conservation des fichiers de journalisation des prestataires d'hébergement (identification des personnes ayant édité du contenu mis en ligne).

Mise en œuvre d'un PCA/PRA ou «plan de secours»

Exemple d'une structure de formation

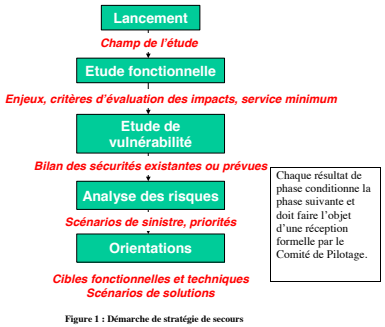


Figure 1 : Démarche de stratégie de secours

□ **Lancement** :

Objectif : déterminer et préciser les risques à couvrir :

- ⋆ objets à risque : matériels informatiques et téléphoniques, fournisseurs extérieurs, personnels, locaux...
- ⋆ nature des risques.

Périmètre et risques :

- ⋆ limiter l'analyse au système informatique : serveurs et postes clients
- ⋆ exclure la situation de perte totale de données (productions et sauvegardes)

□ **Étude fonctionnelle**

Objectif : activités qui exigent une continuité :

- ⋆ enjeux
- ⋆ activités essentielles
- ⋆ conséquences d'une interruption, dégradation : arrêt temporaire ou définitif, perte de données, dégradation de service...

Activités et exigences :

Étude du fonctionnement de la **structure de formation**

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Exemple d'une structure de formation

Quelles sont les activités qui exigent une continuité ?

Définir :

- ⋆ *les enjeux : permettre d'étalonner le niveau d'impact (caractère "non supportable") et de préciser les conditions minimales pour assurer un niveau d'activité et de disponibilité du SI acceptable.*
- ⋆ *les activités essentielles : les besoins informatiques en terme de process et de logiciels ;*
- ⋆ *les conséquences d'une interruption, dégradation (arrêt temporaire ou définitif, perte de données, dégradation de service..)*

Activités

a. un logiciel pour la **gestion des personnes inscrites** dans les différentes formations dispensées :
   - ◇ inscription ;
   - ◇ gestion des évaluations ;
   - ◇ délivrance d'une attestion de suivi ou de réussite si la formation est diplômante ou fournie un certificat.

b. un logiciel de **gestion comptable** disposant d'une passerelle vers le logiciel de gestion des inscrits.

Exigences

Pour le logiciel a) :

élèves	temps d'arrêt max supportable
mai à juin	2 jours
septembre à octobre	2 jours
autres	3 jours

Pour le logiciel b) :

comptabilité	temps d'arrêt max supportable
janvier	1 jour
septembre à avril	2 jours
autres	4 jours

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Tableau récapitulatif du nombre de jours maximum d'interruption acceptable

mois	01	02	03	04	05	06	07	08	09	10	11	12
logiciel a) élèves	3	3	3	3	2	2	3	3	2	2	3	3
logiciel b) compta	1	2	2	2	3	3	3	3	2	2	2	2
maximum acceptable	1	2	2	2	2	2	3	3	2	2	2	2

Analyse

▷ Les logiciels d'exploitation se trouvant **sur le même serveur**, cela ramène la durée maximale d'interruption totale d'activité supportable à **deux jours sur toute l'année**.

*Si ce temps est ramené à une journée cela permet de limiter énormément le stress des **personnes concernées par l'utilisation de ce logiciel** et par conséquent, réduit le stress des **personnes qui s'occupent de la remise en activité du système**.*

▷ Ces deux jours concernent seulement la perte d'activité due au serveur.

La perte d'une journée de travail est le **maximum pour les périodes de forte activité**.
S'il y a perte totale de données, le coût devient très élevé car il faut reprendre les données en cours mais également reconstituer un historique minimum pour répondre à la législation (comptabilité, apprenants...)

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

□ **Étude de vulnérabilité** :

- ◇ Couverture assurance des risques informatiques : souscription d'une assurance couvrant les dégâts matériels et qui prévoit une indemnisation pour la reconstitution des données.
- ◇ Sécurité générale : accès protégé aux serveurs, sauvegardes sur bandes.
- ◇ Moyens de secours : pas de redondance de serveurs.
- ◇ Moyens de protections des informations stockées : la bande magnétique de sauvegarde du vendredi sort du bâtiment.
  Elle n'est probablement pas chiffrée.
- ◇ Contrats de maintenance : pour le serveur et les postes clients, imprimantes...
- ◇ Sécurité du réseau informatique : utilisation d'un parefeu/firewall.

□ **Analyse des risques**

Les principaux risques pour les structures sont les

- ◇ risques externes (force majeure) : électricité, incendie, dégâts des eaux, accès internet du FAI, vandalisme...
  Pour les risques électriques et d'incendie, les écoles accueillant du public sont contrôlées régulièrement avec des normes strictes. Les cas de forces majeures peuvent entraîner un arrêt complet si les serveurs sont tous sur le même site.
- ◇ risques internes : le matériel, la mauvaise manipulation...

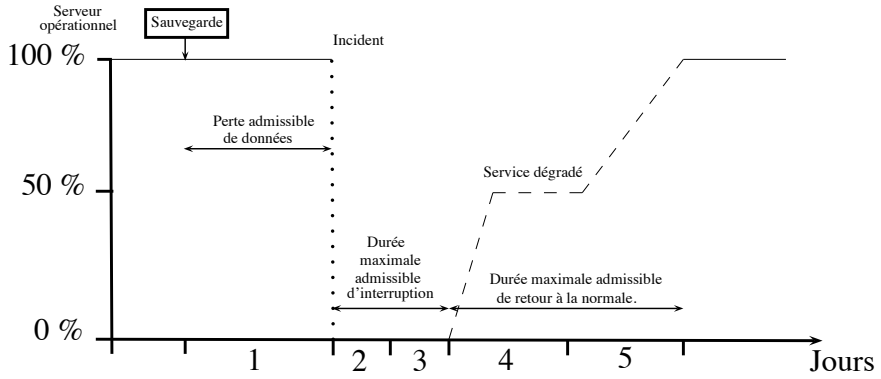
□ **Orientations**

Les solutions techniques et organisationnelles.

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Synthèse



Ressources disponibles

`https://www.clusif.asso.fr/fr/production/ouvrages/pdf/PlanContinuiteActivite.pdf`

`http://www.economie.gouv.fr/files/hfds-guide-pca-plan-continuite-activite-_sgdsn.pdf`

COMPLÉMENT

Mise en œuvre d'un PCA/PRA

Orientations : quelques solutions

- ○ Utiliser un hébergeur externe pour l'hébergement d'un site Web ;
  L'hébergeur doit disposer de son propre PCA/PRA.
- ○ Héberger ses applications métiers dans le Cloud : Amazon Elastic Compute Cloud (EC2), etc.
  Si l'application métier a été adaptée à ce mode fonctionnement.
- ○ Sauvegarder régulièrement en ligne ses données : GoogleDrive, DropBox, WEBdav...
  Disponible gratuitement pour les particuliers, à mettre en conformité avec la politique de sécurité de l'entreprise pour des données professionnelles, ou souscrire à une offre professionnelle.
- ○ Virtualiser le poste de travail : VMWare, VirtualBox...
  *Le matériel est interchangeable, seule compte la «*machine virtuelle*», qui se réduit à des fichiers représentant son disque dur. Par contre, bénéficie mal des performances des cartes graphiques.*
- ○ Stocker ses données sur un serveur dans le réseau : NAS, SAN...
  Le serveur n'héberge que des disques durs en mode RAID : survivre à la mort d'un des disques durs.
- ○ Disposer d'image complète de son poste de travail : Clonezilla, Symantec Ghost...
  Permet de restaurer la totalité du disque dur de la machine, système d'exploitation et application compris.
- ○ Utiliser des applications disponible sur le Web : Google Docs, Microsoft Office 365.
  Utiliser les solutions proposées par les éditeurs en matière de traitement de texte, de tableur et disposer de moyens de travail collaboratif.
- ○ Télétravail.
  Permet de s'affranchir des risques liés aux retards et impossibilités de déplacement professionnels. Cela s'étend à l'usage de la visio conférence en lieu et place de déplacement de travail.

COMPLÉMENT