Intégration de Sécurité dans les Projets

Introduction

VUE GLOBALE

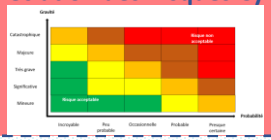
LOI REGLEMENT

NORMES

POLITIQUE RISQUES CONTROLES

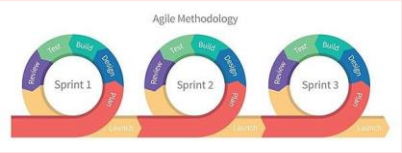
Politique & pilotage de la Cyber

Appréciation des Risques Cyber

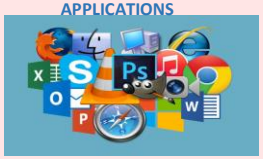


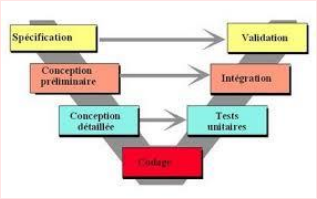
Contrôle & audit Cyber

SECURITE DANS LES PROJETS

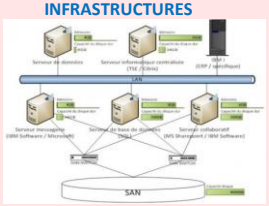


APPLICATIONS

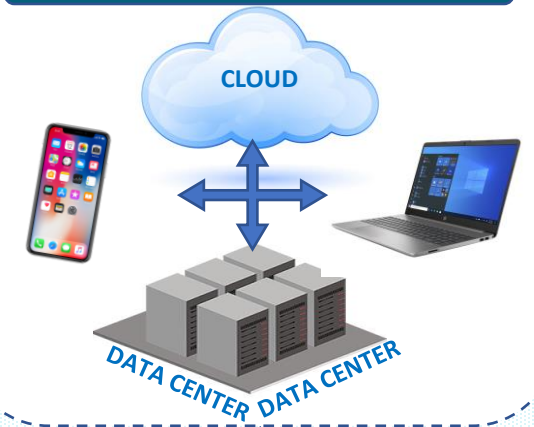




INFRASTRUCTURES



SYSTÈME D'INFORMATIONS



MESURES DE SECURITE

Gestion des identités et des accès au SI

Protection des informations

Cloisonnement et Robustesse du SI

Surveillance du SI

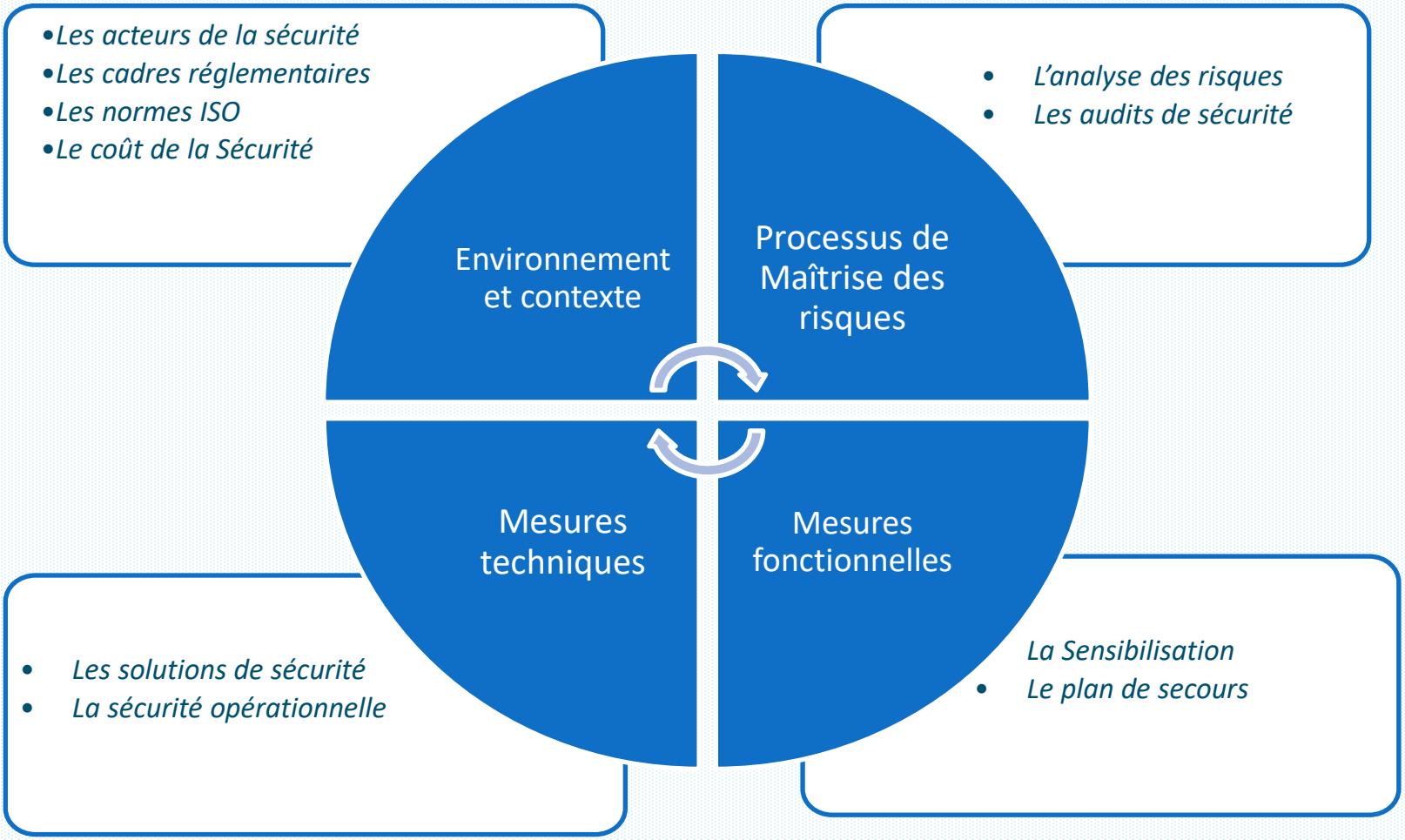
Gestion des vulnérabilités

MENACES

CONCEPT GENERAL

- La (sur)vie d'une entreprise impose :
  - De préserver son image de marque
  - De garder secret son savoir faire
  - D'assurer sa compétitivité
  - De protéger ses données sensibles (et celles de ses clients)
  - D' assurer la continuité de son activité métier
  - D'être en conformité avec les lois et réglementations
  - D'assurer la sécurité de son écosystème (fournisseurs)

LES LEVIERS DE LA CYBERSECURITE



SECURITE DU SYSTÈME D'INFORMATIONS

La sécurité du SI : de quoi parle t on ?

La sécurité du SI consiste à protéger la confidentialité, l'intégrité et la disponibilité de l'information

Source ISO 27000

Les trois grands besoins de sécurité :

Disponibilité

Propriété d'être accessible et utilisable à la demande par une entité autorisée

Intégrité

Propriété de protection de l'exactitude et de la complétude des actifs

Confidentialité

Propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés

SECURITE DU SYSTÈME D'INFORMATIONS

l'information : de quoi parle t on ?

On appel information tout élément représentant de la valeur pour l'organisation. On parle aussi d'actif (« bien » / « asset »)

Il existe plusieurs sortes d'actifs

- **les données** : nom, prénom, photos, publication sur les réseaux;
- **Les documents** : cahier des charges, dossier financier, …
- **les services** : processus métiers, produits clients, …;
- **les logiciels** : un SGBD, un OS, une appli. métier;
- **Les réseaux** : filaires et non filaires (wifi, bluetooth, 4G, …) ;
- **Les matériels** : serveur, PC, smartphone, …;
- **les locaux** : data center, salle technique, ….

SECURITE DU SYSTÈME D'INFORMATIONS

Oui mais comment ?

Une sécurité efficace **réduit les risques** en protégeant le SI de l'entreprise contre les **menaces** et les **vulnérabilités**, ce qui réduit les conséquences (impacts) sur ses **actifs**.

La protection du SI est assurée par

Le respect d'une Politique Sécurité du SI : référentiel des principes et règles de sécurité de l'entreprise

la mise en œuvre de mesures de sécurité adaptées : moyens techniques ou organisationnels

LA SÉCURITÉ DANS LES PROJETS

1. **La PSSI** socle de la sécurité de l'entreprise

2. **Enjeux** de l'Intégration de la Sécurité dans les projets

3. **Les activités** de l'Intégration de la Sécurité dans les Projets

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Une Politique Générale de Sécurité du SI : C'est quoi ?

Sur la base de l'ISO généralement, **la Politique Générale de Sécurité** du SI est un document de quelques pages précisant les grands principes de sécurité. Elle est signée par la direction et est connue de tout les collaborateurs.

Elle est déclinée en différents documents :

- des politiques thématiques de sécurité: principes de sécurité
- des directives thématiques de sécurité: règles détaillées de sécurité
- des documents opérationnelles de sécurité : guides, notes, …

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Exemple de structuration du corpus documentaire SSI

Niv 1

COMEX

PGSSI

Note de gouvernance Cyber

Niv 2

Directions Métiers

Politiques Thématiques de Sécurité (PTS)

Niv 3

Direction Informatique

Directives thématiques Sécurité (DTS) et documents associés

Niv 4

Documents opérationnels (Guides / formulaires / ..)

Exemple de politique thématique Sécurité

PRINCIPES DE SECURITE

PTS Sécurité des informations

Exemple de directives thématique sécurité

REGLES DE SECURITE

DTS Conditions d'usages de la cryptographie

DTS Aliénations des matériels

DTS Recouvrement de données chiffrées

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Le document chapeau : Politique Générale de Sécurité SI

- Une définition de la sécurité de l'information, les objectifs généraux recherchés et le domaine d'application retenu, ainsi que l'importance de la sécurité en tant que mécanisme nécessaire au partage de l'information
- Une déclaration des intentions de la direction soutenant les objectifs et principes de la sécurité de l'information
- Une explication des principes, normes et exigences importantes pour l'entreprise:
  - conformité avec les exigences légales, réglementaires et contractuelles
  - exigences en terme de formation et de sensibilisation en matière de sécurité
  - gestion de la continuité de l'activité
  - conséquences des violations de la sécurité de l'information
- Une définition des responsabilités dans le domaine de la sécurité de l'information traitant en particulier les incidents de sécurité

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Principe Fondamental 1

La Politique de Sécurité du SI définit la sécurité du SI comme la combinaison de 3 critères fondamentaux :

- **DISPONIBILITE** : l'aptitude du système à être accessible et utilisable, lorsque cela est requis, par les acteurs autorisés,
- **CONFIDENTIALITE :** l'aptitude du système à réserver l'accès aux informations aux seules personnes ayant à les connaître,
- **INTEGRITE** : l'aptitude du système à demeurer intact, non corrompu, et sans altération.

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Principe fondamental 2

L'objectif de la Politique de Sécurité du SI est de protéger le SI des menaces par des dispositions assurant un bon compromis entre leur coût et leur efficacité vis-à-vis des enjeux.

- Aucune plainte, imputable au SI ne doit être instruite pour non-respect de la confidentialité ou pour discrimination dans l'accès à l'information,
- Limiter à un montant annuel inférieur à X millions d'euros les conséquences financières des dysfonctionnements du SI.

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Principe Fondamental 3

L'entreprise s'engage à respecter la réglementation française relative au domaine de l'informatique et des télécommunications :

- Protection des libertés individuelles
- Fraude informatique
- Propriété intellectuelle
- Protection des points et réseaux sensibles
- Préservation de la confidentialité des informations commerciales sensibles
- Obligations en matière de télécommunication ou de cryptologie
- Traitements de données à caractère personnel

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Principaux thèmes détaillés dans une PSSI:

1 - le contrôle des identités et des accès au SI

2 - la classification et la protection de l'information

3 - Les moyens particuliers de cryptographiques

4 - La sécurité des développements

5 - La sécurité des communications et des infrastructures

6 - La sécurité opérationnelle

- protection contre les logiciels malveillants
- La gestion des vulnérabilités techniques

7 - la surveillance du SI

8 - La sauvegarde & restauration

9 - La sécurité avec les fournisseurs

10 - Les devoirs de l'utilisateur

- 1 - utilisation correcte des actifs
- 2 - bureau propre et écran vide
- 3 - politiques et procédures de transfert de l'information
- 4 - appareils mobiles et télétravail

SECURITE DU SYSTÈME D'INFORMATIONS

La politique Générale de Sécurité

Le document de Politique générale de sécurité est accompagnée d'une **note de d'organisation de la sécurité.** Ce document précise :

- les rôles et responsabilités des acteurs de la sécurité
  - Directeur Cyber, RSSI, Correspondant Sécurité
  - Expert Sécurité technique, architecte sécurité, consultant cyber
  - SOC manager, analyste Cyber, pentesteurs, .
  - ….
- Les dispositifs de pilotage de la Sécurité
  - Comités: niveau comex pour la stratégique, niveau métier pour le pilotage / niveau opérationnel pour les activités permanent/ ..
  - Indicateurs: indicateurs de maturité cyber, indicateurs de performance des moyens mis en place, indicateurs de conformité aux règles de la PSSI, indicateurs de niveau de risques….

LA SÉCURITÉ DANS LES PROJETS

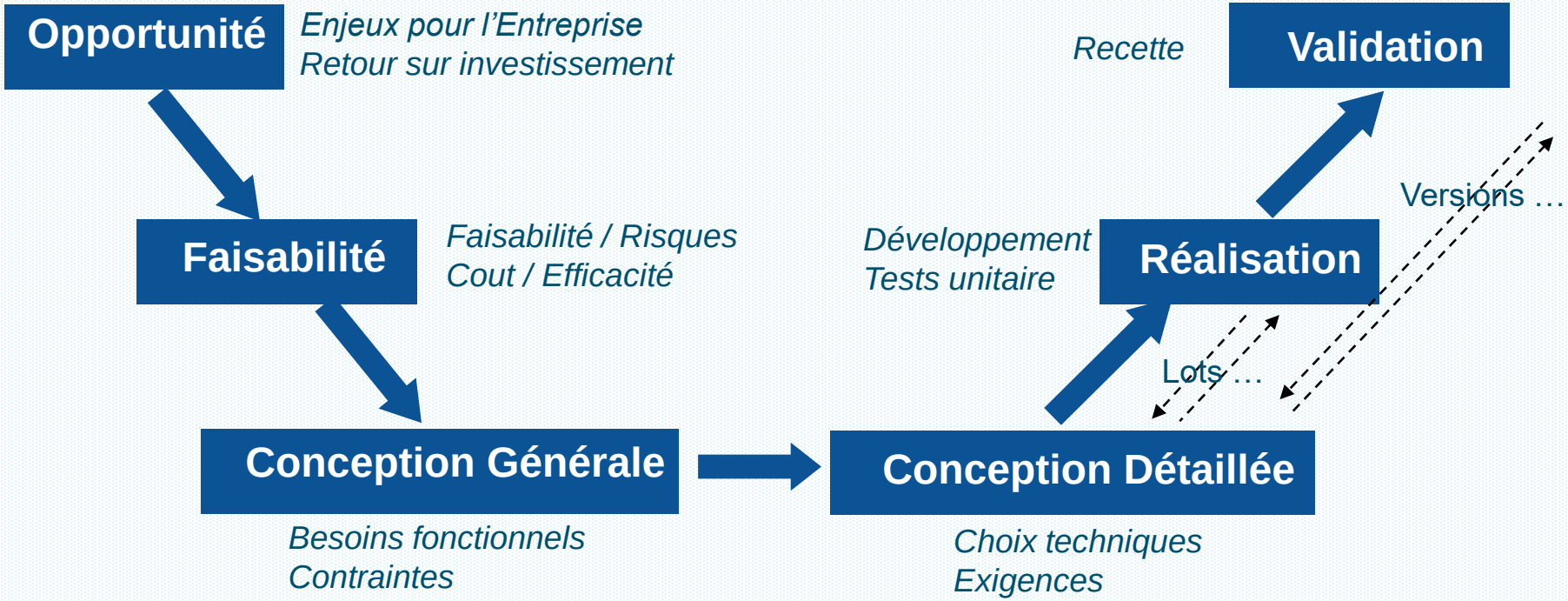
1. **La PSSI** socle de sécurité de l'entreprise

2. **Enjeux** de l'Intégration de la Sécurité dans les projets

3. **Les activités** de l'Intégration de la Sécurité dans les Projets

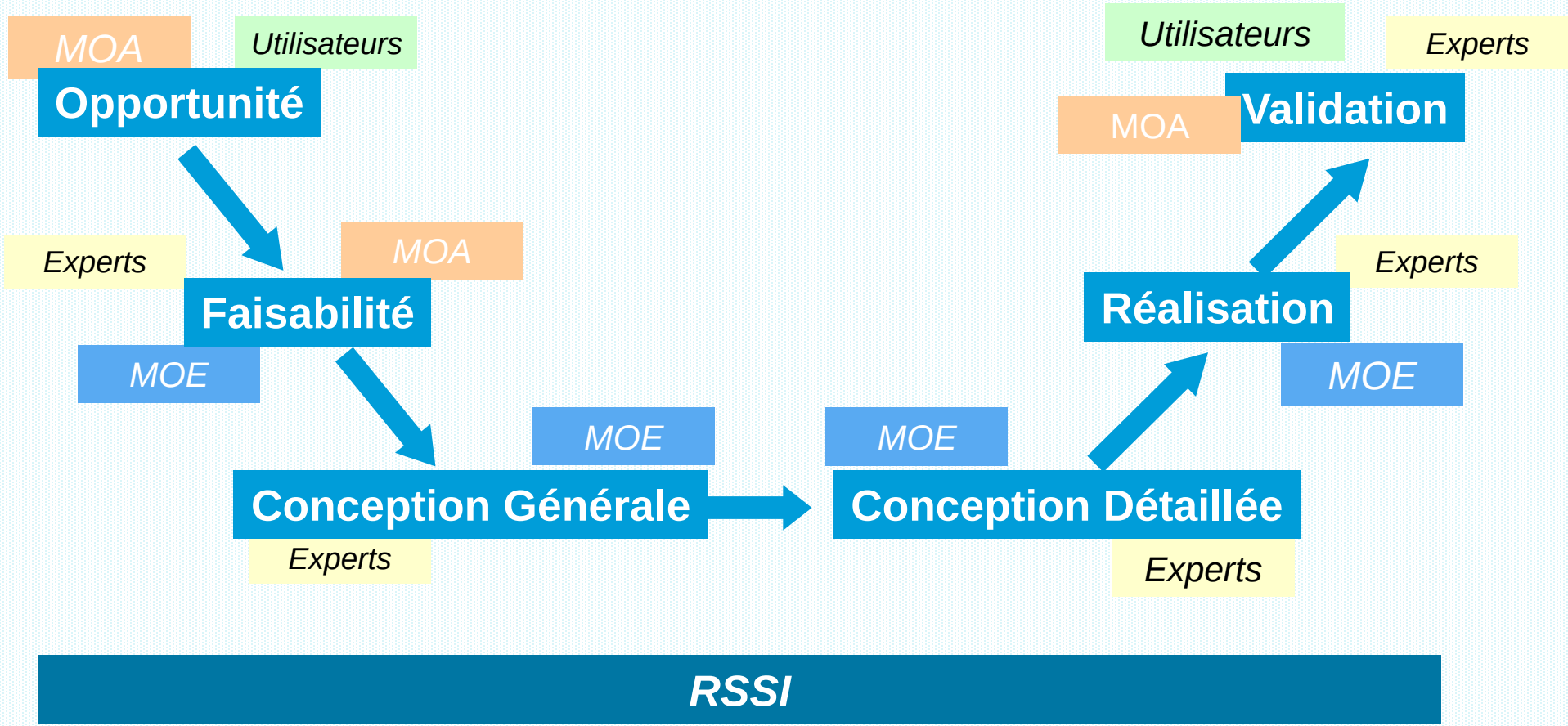
ENJEUX ISP

Les principales étapes d'un projet



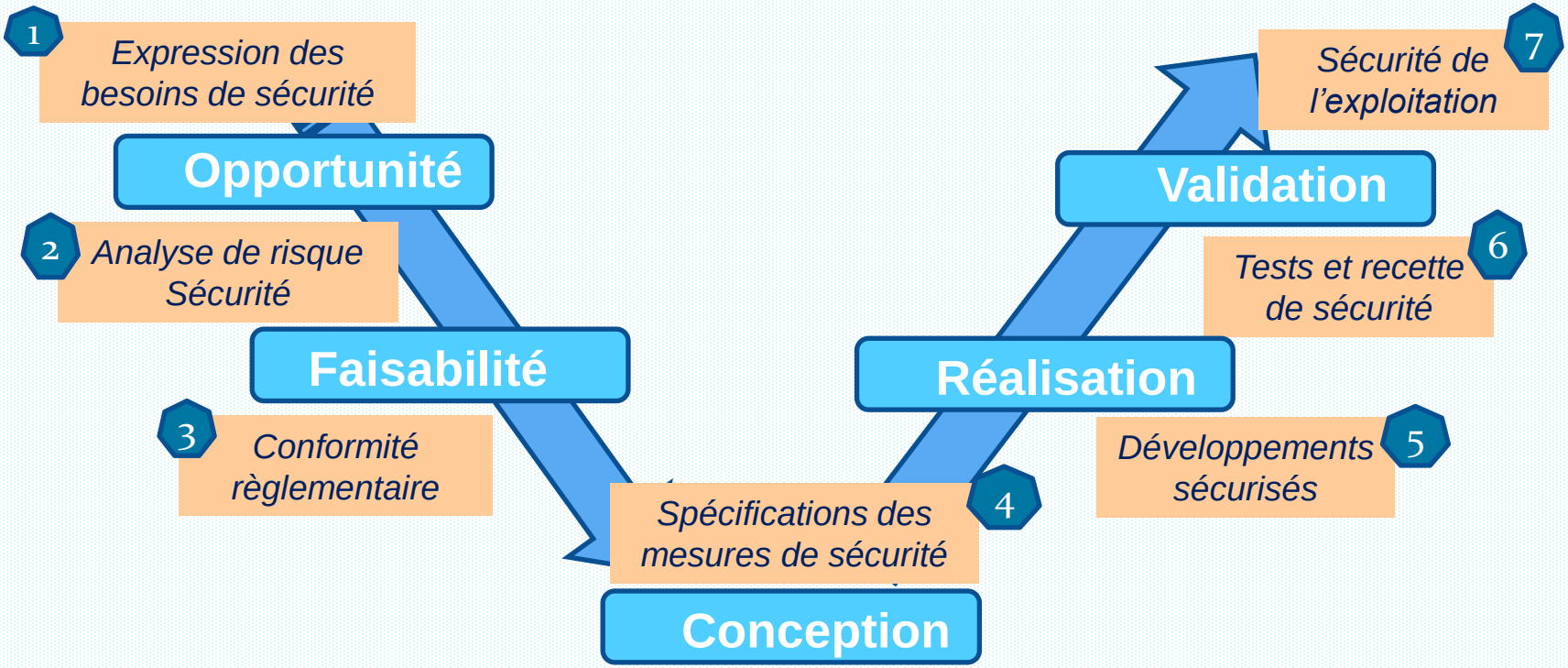
ENJEUX ISP

Les principaux acteurs d'un projet



ENJEUX ISP

Les principales activités sécurité d'un projet



ENJEUX ISP

Les principaux objectifs de l'ISP

- **Promouvoir une "culture de la sécurité »**
  - Moins d'experts, plus d'acteurs
  - Responsabiliser
  - Traiter tous les sujets au bon moment
- **Adapter les actions SSI selon les enjeux réels**
  - Faire mieux sans faire trop
  - Eviter l'effet Mille-feuille
- **Maîtriser les risques sur le cycle de vie du S.I.**
  - Etre sûr de son S.I. … et le rester

ENJEUX ISP

Quizz

- ***La phase d'analyse d'un projet de développement d'une nouvelle application devra s'assurer que :***
  - Les programmeurs fournissent les solutions aux exigences fonctionnelles.
  - Les exigences de sécurité ont été définies.
  - Le coût pour l'entretien du système est dans une marge acceptable.
  - Une solution clés en main pour couvrir les besoins du système est disponible.

ENJEUX ISP

Quizz

- ***Pour réduire le coût de la sécurité dans un projet de développement de système, les techniques de gestion de la sécurité devraient être appliquées:***
  - Le plus prés possible de la réalisation des projets concernés.
  - Essentiellement lors du démarrage du projet pour garantir que le projet est aligné sur les normes de gouvernance de l'organisation.
  - De façon continue durant tout le projet.
  - Particulièrement à la fin du projet pour détecter les leçons apprises pour pouvoir les appliquer aux projets futurs.

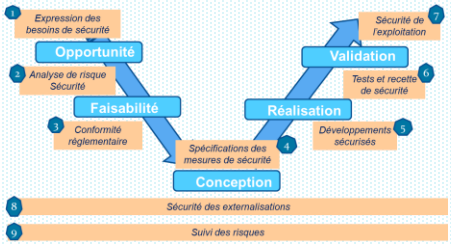
LA SÉCURITÉ DANS LES PROJETS

1. **La PSSI** socle de sécurité de l'entreprise

2. **Enjeux** de l'Intégration de la Sécurité dans les projets

3. **Les activités** de l'Intégration de la Sécurité dans les Projets

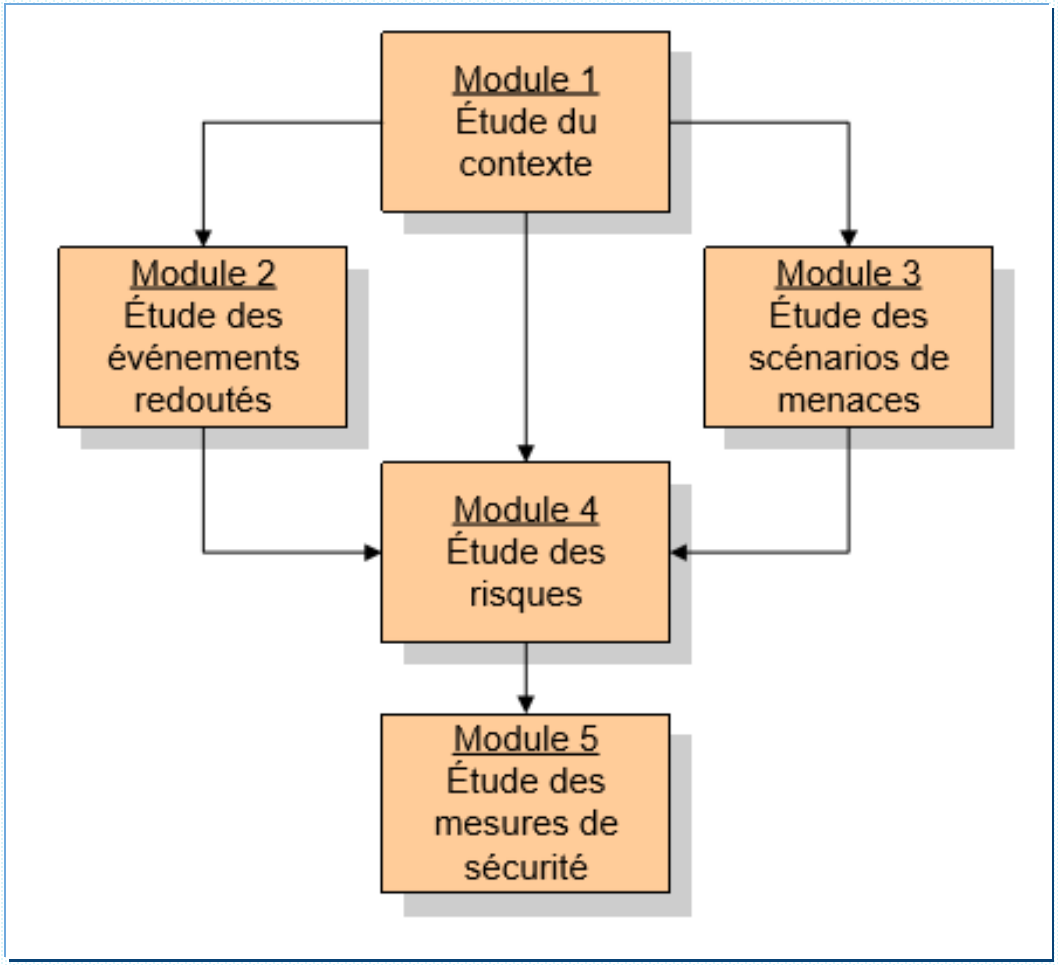
LES ACTIVITÉS ISP



1. **Les besoins de sécurité**
2. L'analyse de risque Sécurité
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. La sécurisation de la sous-traitance
8. La sécurisation de l'exploitation
9. Le suivi des risques résiduels et induits

BESOIN DE SÉCURITÉ & ANALYSE DE RISQUES

La démarche générale



BESOIN DE SÉCURITÉ

Orientation métier et IT

- L'analyse du besoin de sécurité **Métier** :
  - ✓ Identifier les données et services
  - ✓ Mettre en évidence des risques à la sensibilité des données, à la criticité de la future solution, …
  - ✓ Expression les besoins (ou exigences) de sécurité
  - ✓ Définir le niveau d'acceptation du risque

D.I.C.T.

Responsabilité : Métier

- L'analyse du besoin de sécurité **IT :**
  - ✓ Définir l'architecture/ l'application
  - ✓ Mettre en évidence des risques inhérents aux moyens techniques utilisés (Internet, langage, localisation, …)
  - ✓ Proposer des mesures de réduction des risques
  - ✓ Définir le niveau d'acceptation du risque

Mesures

Responsabilité : DSI

BESOIN DE SÉCURITÉ

Besoins de sécurité: les critères DICT

- La **Disponibilité (D)** : Propriété d'accessibilité des informations ou de traitement en toute circonstance dans des conditions prédéfinies d'horaires, de délai, de performance, et de recouvrement d'incidents
  - Ex : délai d'accès aux applications, au réseau
- **L'Intégrité (I)** : Propriété d'exactitude et de complétude des informations ou des traitements. Celles-ci ne doivent être modifiées que par des utilisateurs ou systèmes dûment autorisés
  - Ex : Logiciel de contrôle Commande
- La **Confidentialité (C)** : Propriété des informations de n'être accessibles et diffusées qu'aux personnes dûment autorisés
  - Ex : Données clients, Données de santé
- La **Traçabilité (T)** : Capacité à fournir la preuve d'un événement ou de l'existence d'une information sans contestation raisonnable
  - Ex : accès a la base de données clients

BESOIN DE SÉCURITÉ

Besoin de sécurité: échelle de sensibilité

	D	I	C	T
0	Aucun	Aucun	Public	Pas de trace
1	48 h	Intégrité non contrôlé	Interne	Pour information
2	24 h	Défaut intégrité Détectable	Restreint	Vérification de bon fonctionnement
3	4 h	Défaut intégrité corrigeable	Confidentiel	Contrôle interne
4	1 h	Intègre	Secret	Opposable juridique

BESOIN DE SÉCURITÉ

Besoin de sécurité: Niveau d'impact

Criticité	Impact	Intégrité	Confidentialité	Traçabilité
4	**Préjudice Inacceptable** pour l'Entreprise Perturbations graves et durables ; impacts majeurs et durables client ; Mise en cause pénale d'un dirigeant ; ; Défiance des parties prenantes vis-à-vis de l'Entreprise	**Pas d'altération** Aucune perte d'intégrité n'est acceptée.	**Informations Secrètes** Accédant en nombre extrêmement réduit et nommément désignés. Exemples : Projet stratégiques majeurs,	**Traçabilité opposable** Besoin de traces opposables (dans une optique de contentieux juridique)
3	**Préjudice grave** pour l'Entreprise Perturbations importantes d'une entité ou clients. Assignations ou mises en cause civiles en nombre important sur un même sujet. Dégradation de l'image du Groupe LBP auprès des parties prenantes (clients, personnel, tutelle, etc.)	**Intégrité renforcée** Une perte temporaire d'intégrité est acceptée mais la détection est systématique et la reconstruction est obligatoire.	**Informations Confidentielles** Accédant explicitement désignés par leurs noms ou leurs fonctions. Exemples : Données bancaires clients, données nominatives	**Traçabilité pour contrôle interne** Besoin de traces tangibles pour contrôle interne ou réglementaire (piste d'audit)

BESOIN DE SÉCURITÉ

Besoin de sécurité: Niveau d'impact

Criticité	Impact	Intégrité	Confidentialité	Traçabilité
2	**Préjudice modéré** pour l'Entreprise Perturbations limitées à un service, sans impact clients Faible altération de l'image de marque de l'Entreprise	**Intégrité moyenne** Une perte temporaire d'intégrité est acceptée mais la détection est procédurée (pas automatisée) et la reconstruction est obligatoire.	**Informations restreintes** Accédant issu de Groupes ou catégories de personnes identifiées. Exemples : règlement intérieur, procédure de traitement des opérations.	**Traçabilité pour vérification** Besoin de traces pour vérification du bon déroulement d'un traitement (processus, fonction, technique, ….)
1	**Préjudice faible** pour l'Entreprise Perturbations ponctuelles, par exemple limitées à quelques personnes. Mise en cause sans perte de confiance, issue par exemple d'une réclamation client isolée.	**Intégrité simple** Une perte temporaire d'intégrité est acceptée mais la reconstruction doit être possible si elle est demandée.	**Informations Internes** Exemple : Descriptifs des produits commercialisés, communication institutionnelle.	**Traçabilité pour information** Besoin de trace pour information (statistique, tableau de bord, ….)
0	**Aucun préjudice**	**Altération acceptée**	**C0 : Public**	**Pas de besoin de traçabilité**

BESOIN DE SÉCURITÉ

QUIZZ

Vous développez un site web **www.asso-etudiants-touristes.org** pour une association qui regroupe les étudiants souhaitant effectuer des voyages ensemble à l'étranger.

Sur ce site on retrouve les informations concernant les voyages proposés telles que :

- le pays, les villes à visiter.
- le prix du transport, les conditions d'hébergement.
- les dates potentielles du voyage.

Ces informations ont un besoin en confidentialité :

- ❑ Faible
- ❑ Fort

BESOIN DE SÉCURITÉ

QUIZZ

Choisir ci-dessous 2 exemples de données numériques sensibles pour un étudiant :

- ❑ Adresse postale
- ❑ Nom et numéro de sécurité sociale
- ❑ Numéro de carte bancaire
- ❑ Nom de famille

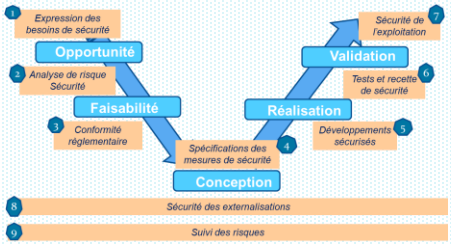
BESOIN DE SÉCURITÉ

QUIZZ

Choisir ci-dessous 2 exemples de données numériques sensibles pour une université/école :

- ❑ Le nom et l'origine de l'université
- ❑ Les noms des professeurs
- ❑ Les brevets déposés
- ❑ Les épreuves d'examens à venir (non encore passés)

LES MESURES SSI



1. Les besoins de sécurité
2. **L'analyse de risque Sécurité**
3. Les exigences réglementaires
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. La sécurisation de la sous-traitance
8. La sécurisation de l'exploitation
9. Le suivi des risques résiduels et induits

L'APPRECIATION DES RISQUES CYBER

La « culture » du risque

- Risque … mais de quoi parle-t-on ?
  - Les risques environnementaux
  - Les risques professionnels
  - Les risques projet
  - Les risques de sûreté de fonctionnement
  - Les risques juridiques
  - Les risques financiers

    Et
  - **Les risques des systèmes d'informations**

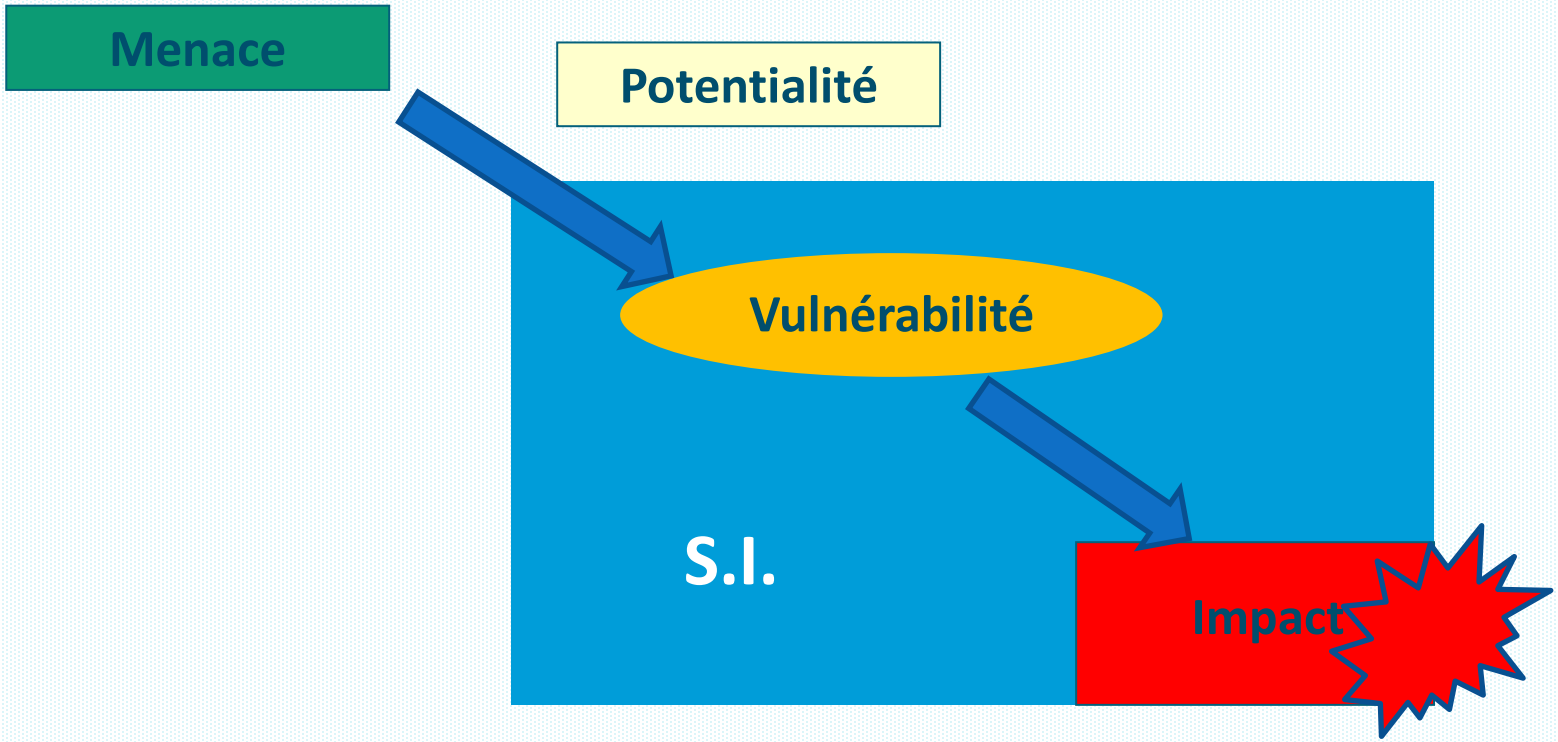
Les risques de sécurité font partie de cette famille

Source club EBIOS

L'APPRECIATION DES RISQUES CYBER

Risque : notions Générales

Risque = Fonction (Menace; Potentialité; Vulnérabilité; Impact)



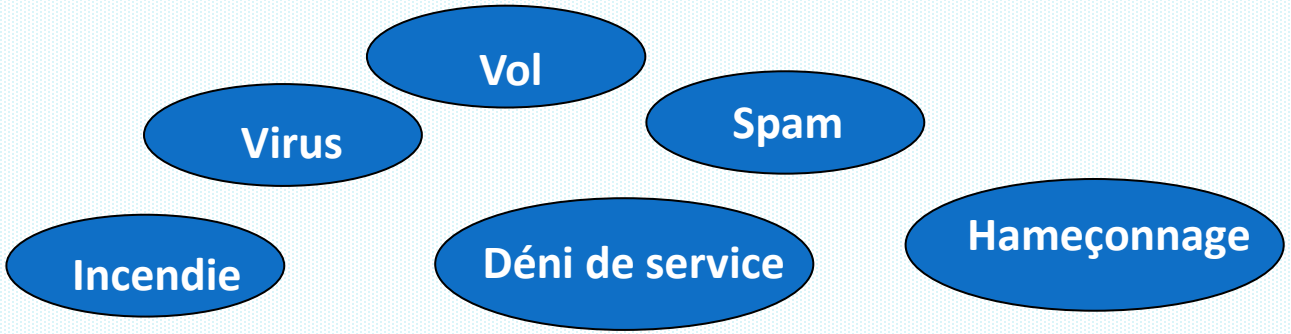
L'APPRECIATION DES RISQUES CYBER

Risque : notions Générales

« Une menace est un évènement susceptible d'endommager les actifs tels que des informations, des processus et des systèmes et, par conséquent, des organismes ».

Les menaces peuvent :

- Être d'origine naturelle ou humaine
- Être accidentelles ou délibérées
- Survenir de l'intérieur ou de l'extérieur de l'organisme



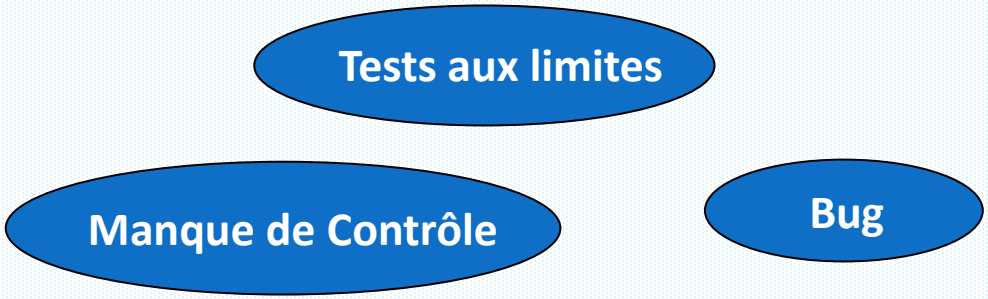
L'APPRECIATION DES RISQUES CYBER

Risque : notions Générales

« Une vulnérabilité ou faille est une faiblesse dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité et l'intégrité des données qu'il contient »

Les vulnérabilités peuvent :

- Être issues d'une mauvaise conception
- Être issues de négligence dans la réalisation.
- Être issues d'un manque de contrôle



L'APPRECIATION DES RISQUES CYBER

Risque : notions Générales

« L'impact est une évaluation globale de l'ensemble des conséquences d'un scénario de risques précis. Les conséquences, directes ou indirectes, peuvent être d'ordre financier, juridique, d'image ou humain »

La métrique de l'impact est une cotation sur une échelle à 4 niveaux (de 1 à 4) :

- Niveau 1 Impact insignifiant au niveau de l'organisation
- Niveau 2 Impact significatif, causant du tort à l'organisation
- Niveau 3 Impact très grave, sans menacer la vie de l'organisation
- Niveau 4 Impact extrêmement grave, menaçant l'organisation ou l'une de ses activités vitales

L'APPRECIATION DES RISQUES CYBER

Risque : notions Générales

« La potentialité est une estimation de la possibilité qu'un scénario précis survienne »

La métrique standard de la potentialité est une cotation sur une échelle à 5 niveaux (de 0 à 4) décrite ci-dessous :

- Niveau 0 Non envisageable ou non envisagé
- Niveau 1 Très improbable, ne surviendra sûrement jamais
- Niveau 2 Improbable, bien que possible
- Niveau 3 Probable, devrait arriver un jour
- Niveau 4 Très probable/ quasi certain, surviendra sûrement à court terme

L'APPRECIATION DES RISQUES CYBER

Analyse des Risques : Les 4 étapes clés à retenir

- Établissement du contexte
  - Périmètre de l'étude
  - Objectifs
  - Organisation
- Appréciation des risques
  - Identification : Quels sont les risques ?
  - Evaluation : Quel est le niveau des risques ?
  - Classement : quels sont les plus important ?

Le plus difficile !

- Traitement des risques
  - Choix pour traiter les risques : réduction, transfert / partage, évitement / refus ou acceptation
  - Mise en place de mesures pour traiter les risques
- Acceptation des risques
  - Validation formelle des risques résiduels (en intégrant les mesures de protection

Source ISO 31000

L'APPRECIATION DES RISQUES CYBER

Identification des risques

Type	Menaces
Dommage physique	Incendie
	Dégât des eaux
	Pollution
	Accident majeur
	Destruction de matériel ou de support
	Poussière, corrosion, congélation
Catastrophes naturelles	Phénomène climatique
	Phénomène sismique
	Phénomène volcanique
	Phénomène météorologique
	Inondation
Perte de services essentiels	Panne du système de climatisation ou d'alimentation en eau
	Perte de la source d'alimentation en électricité
	Panne du matériel de télécommunications
Perturbation due à des rayonnements	Rayonnements électromagnétiques
	Rayonnements thermiques
	Impulsions électromagnétiques
Compromission d'informations	Interception de signaux d'interférence compromettants
	Espionnage à distance
	Ecoute
	Vol de supports ou de documents
	Vol de matériel
	Récupération de supports recyclés ou mis au rebut
	Divulgation
	Données provenant de sources douteuses
	Piégeage de matériel
	Piégeage de logiciel
	Géolocalisation
Défaillances techniques	Panne de matériel
	Dysfonctionnement du matériel
	Saturation du système d'information
	Dysfonctionnement du logiciel
	Violation de la maintenabilité du système d'information
Actions non autorisées	Utilisation non autorisée du matériel
	Reproduction frauduleuse de logiciel
	Utilisation de logiciels copiés ou de contrefaçon
	Corruption de données
	Traitement illégal de données
	Erreur d'utilisation
	Abus des droits

Source ISO 27005

L'APPRECIATION DES RISQUES CYBER

Evaluation et classement des risques

- **Évaluation**
  - Aller vers le « qualitatif » entre 3 et 5 niveaux
  - exemple : « faible, moyen, élevé » - « rare, peu probable, probable, fréquent »

- **Classement**
  - La formule de calcul / matrice **doit être la même** pour tous les risques
  - Le plus important : le classement des risques entre eux

L'APPRECIATION DES RISQUES CYBER

Echelle pour le calcul des risques

Exemple

	Vraisemblance d'un scénario d'incident	Très faible (Très peu probable)	Faible (Peu probable)	Moyenne (Possible)	Élevée (Probable)	Très élevée (Fréquente)
Impact sur l'activité	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Élevé	3	4	5	6	7
	Très élevé	4	5	6	7	8

Source ISO 27005

L'APPRECIATION DES RISQUES CYBER

La réponse française … par EBIOS RM

- Evolution majeure de la version 2010.
- Approche modulaire et customisable.
- Permet la prise en compte des risques cyber ciblés.
- Introduction de nouvelles données
  - Objectifs de conformité
  - Connaissance de son écosystème
  - Appréciation des risques des parties prenantes
  - Défense en profondeur

L'APPRECIATION DES RISQUES CYBER

EBIOS RM : démarche basée sur 5 ateliers

1 – **CADRAGE ET SOCLE DE SÉCURITÉ**

- Définir le cadre de l'étude, son périmètre métier et technique, les événements redoutés associés et le socle de sécurité.

2 – **SOURCES DE RISQUE**

- Identifier les sources de risque (SR) et leurs objectifs visés (OV), en lien avec le contexte particulier de l'étude : qui ou quoi pourrait porter atteinte aux missions et valeurs métier, et dans quels buts ?

3 – **SCÉNARIOS STRATÉGIQUES**

- Imaginer des scénarios réalistes de haut niveau, indiquant de quelle façon un attaquant pourrait procéder pour atteindre son objectif.

4 – **SCÉNARIOS OPÉRATIONNELS**

- Construire des scénarios opérationnels qui schématisent les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques.

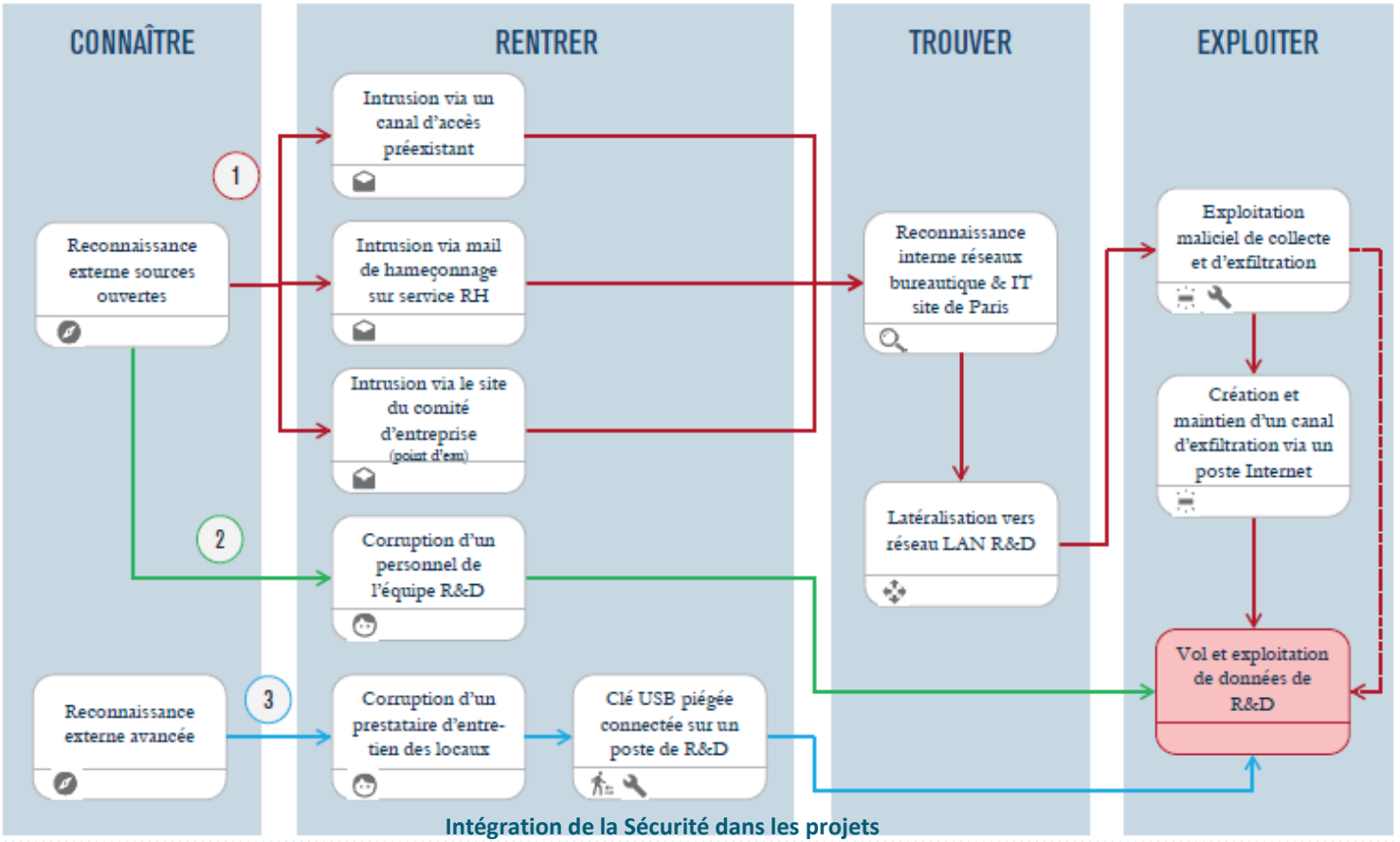
5 – **TRAITEMENT DU RISQUE**

- Réaliser une synthèse des scénarios de risque et identifier des mesures de sécurité

L'APPRECIATION DES RISQUES CYBER

Exemple de scénario d'attaque

« Un concurrent veut voler des informations en espionnant les travaux de R&D. Il veut créer un canal d'exfiltration de données portant directement sur le système d'information de la R&D (de l'entreprise) »



L'APPRECIATION DES RISQUES CYBER

QUIZZ

La Banque Locale de Martinique souhaite identifier les risques qui pèsent sur son Datacenter. Classer les menaces suivantes en fonction de leur probabilité, de la plus haute à la plus faible :

- ❑ Inondation.
- ❑ Tremblement de terre.
- ❑ Feu.
- ❑ Alimentation électrique
- ❑ Intrusion
- ❑ Climatisation

L'APPRECIATION DES RISQUES CYBER

QUIZZ

Un choix de mots de passe faibles et la transmission de données sur des réseaux de communication non protégés sont des exemples de :

- ❑ vulnérabilités.
- ❑ menaces.
- ❑ probabilités.
- ❑ impacts

L'APPRECIATION DES RISQUES CYBER

QUIZZ

Quel est le risque majeur pour une banque:

- ❑ Fraude interne et/ou externe
- ❑ Non respect de la réglementation
- ❑ Atteinte à l'image

L'APPRECIATION DES RISQUES CYBER

QUIZZ

Quel est le risque majeur pour un hôpital :

- ❑ Disponibilité des données de santé
- ❑ Atteinte à la confidentialité et l'intégrité des informations de santé de ses patients.
- ❑ Atteinte à son dispositif de facturation

L'APPRECIATION DES RISQUES CYBER

QUIZZ

Quel est le risque majeur pour un constructeur automobile

- ❑ Vol des brevets, des secrets de fabrication, …
- ❑ Vol des éléments décrivant les futurs projets
- ❑ Accès à la politique marketing

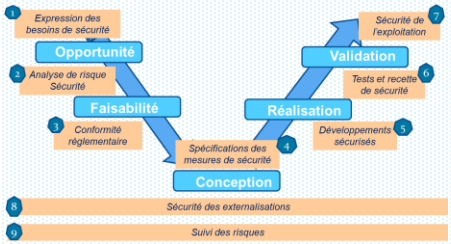
L'APPRECIATION DES RISQUES CYBER

QUIZZ

Quel est le risque majeur pour une entreprise du Bâtiment

- ❑ Accès à ses propositions commerciales
- ❑ Liste de ses collaborateurs
- ❑ Disponibilité de son S.I.

LES ACTIVITÉS ISP



1. Besoin de sécurité
2. Analyse de risque Cyber
3. **Les exigences réglementaires**
4. Les spécifications des mesures de sécurité
5. La sécurisation des développements
6. Les tests et recettes de sécurité
7. La sécurisation de l'exploitation
8. La sécurisation de la sous-traitance
9. Le suivi des risques résiduels et induits

EXIGENCES RÉGLEMENTAIRES

- Loi Informatique et Liberté
- Loi de Programmation Militaire
- Autres textes

EXIGENCES RÉGLEMENTAIRES

La Sécurité des Systèmes d'Information c'est de la technique…

… mais aussi du droit

AUTORITÉ DES MARCHÉS FINANCIERS
AMF

ACP Autorité de Contrôle Prudentiel
Banque de France

CNIL
Commission Nationale de l'Informatique et des Libertés

ANSSI | Agence nationale de la sécurité des systèmes d'information

EXIGENCES RÉGLEMENTAIRES

Réglementation Sectorielle

Règlement Européen

Loi Française

- *Données de santé*
- *Données bancaire*
- *Secret Défense*
- *…*

- *LPM*
- *I&L*
- *Droit du travail*
- *Notification*
- *Traces*
- *…*

Responsabilité : MOA & Direction Juridique

EXIGENCES RÉGLEMENTAIRES

Loi I&L

CNIL
Commission Nationale de l'Informatique et des Libertés

Loi
Informatique & Liberté

- Protection des données à caractère personnel (DCP).
- Obligation de sécurisation des DCP

- Finalité du traitement
- Information des personnes impactées
- Limitation de la durée de conservation
- Communication des mesures mises en œuvre
- Autorisation pour certains traitements (Biométrie, Données de santé, …)

- Cloisonnement,
- Gestion des droits d'accès,
- Protection des données stockées,
- Gestion des durée de rétention
- **Contrôle de l'efficience**
- …

EXIGENCES RÉGLEMENTAIRES

Loi I&L

« DCP : *Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement ».*

- **identification directe** : nom, prénom, photographie, image sur bande vidéo ;

- **identification indirecte** : numéro de téléphone, numéro de CB, numéro de compte bancaire, empreinte digitale, etc.

EXIGENCES RÉGLEMENTAIRES

Loi I&L & RGPD

Loi Informatique & Liberté → **Règlement General européen sur la Protection des Données personnelles**

Une Directive européenne insuffisamment efficace : trop de libertés données aux États membres dans la mise en œuvre de la Directive

- En Allemagne, un très important formalisme
- En Espagne, des sanctions très fortes
- Au Royaume-Uni, des traitements possibles sans information préalable (contrôle clandestin des salariés).

De nouveaux enjeux :

- Big Data, Cloud , Facebook, …
- Sanctions financières peu élevées, …

EXIGENCES RÉGLEMENTAIRES

Loi I&L & RGPD

Nouveau Règlement européen sur la protection des données personnelles

Les grands principes inchangés :

- ❑ Finalité
- ❑ Loyauté,
- ❑ Proportionnalité
- ❑ Les données sensibles
- ❑ Les pouvoirs opérationnels de la CNIL
- ❑ Sécurisation des données

EXIGENCES RÉGLEMENTAIRES

Loi I&L & RGPD

Nouveau Règlement européen sur la protection des données personnelles : RGPD

Une évolution nécessaire :

- Le renforcement des droits des personnes (effacement, portabilité, …)
- *Accountability* (Traçabilité, Preuve, audits)
- *Privacy by design / by default*
- L'analyse d'impact pour les traitements « à risque élevé »
- La notification des violations
- Co-responsabilité du sous-traitant
- Sanctions financières : 20 000 000 € ou jusqu'à **4 % du CA**…

Adhérez… Votez …

Données sensibles !

- **L'incident :** le Parti socialiste a été sanctionné en octobre 2016 pour de graves défauts de sécurité. Il était en effet possible d'accéder, à partir du site Internet du parti, aux « **nom, prénom, adresses électronique** et postale, numéros de téléphone fixe et mobile, date de naissance, adresse IP, **moyen de paiement** » de certains adhérents

- **Le bilan :**
  - Travaux de mise en conformité
  - Atteinte à l'image

Oh my god !

The Ministère Of Défense …

- **L'incident :** Les noms, les adresses, les numéros de passeports … de 100.000 soldats britanniques et de leurs proches, ainsi que de 600.000 candidats potentiels à une carrière militaire, sont dans la nature

- **Le bilan :**
  - Le sous-traitant **XXX** a perdu un disque dur
  - Le Ministère of Défense **ignore** si les données étaient **chiffrées**
  - Des informations sur les **comptes bancaires** sont peut-être concernées …

umfangreicher Handel

- **L'incident :** Les CD-Rom contenant les noms, adresses, numéro de compte et domiciliation bancaire de 21 millions de particuliers allemands sont à vendre …

- **Le bilan :**
  - Trois foyers allemands sur quatre concernés
  - La piste des « **call-centers** » privilégiée. Certains employés auraient **vendu** au plus offrant **les données** recueillies. A l'aide d'une **clé USB**, ces employés peu scrupuleux auraient donc subtilisé ces informations sur leur lieu de travail

EXIGENCES RÉGLEMENTAIRES

Quizz

Une obligation de la loi Informatique et Libertés (et du nouveau règlement européen) est :

- ❑ Chiffrer les données personnelles stockées.
- ❑ Assurer la sécurité des données à caractère personnel
- ❑ Donner les autorisations de recueil des données à caractère personnel

EXIGENCES RÉGLEMENTAIRES

Quizz

Les obligations prévues par le nouveau règlement européen s'appliquent

- ❑ Au responsable du traitement
- ❑ A l'Etat
- ❑ Au responsable du traitement et à ses sous-traitants

EXIGENCES RÉGLEMENTAIRES

Quizz

L'adresse IP de mon ordinateur ?

- ❑ Est une donnée à caractère personnel.
- ❑ Est une information technique
- ❑ N'a aucun caractère réglementaire

EXIGENCES RÉGLEMENTAIRES

LPM : Loi de Programmation Militaire

LPM: L'Etat légifère sur la sécurité des systèmes d'information des O.I.V (Opérateurs d'Importance Vital) :

- **OIV** : opérateurs publics ou privés pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation
- **SIIV** : système d'information d'importance vitale, qui contribue à la réalisation des activités dont l'atteinte à la sécurité ou au fonctionnement risquerait ...

Avant 2015 : Mesures de sécurité physiques et organisationnelles

Après 2015 : Elargissement à la protection des S.I.

EXIGENCES RÉGLEMENTAIRES

Autres textes – Droit du travail

Le cadre légal issu du Code du travail relatif à la surveillance des salariés

- ⇨ Principe de proportionnalité
- ⇨ Art. L1121-1 : Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

- ⇨ Principe de transparence
- ⇨ Art. L1222-4 : Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

- ⇨ Discussion collective
- ⇨ Art. L2323-27 : Le comité d'entreprise est informé et consulté sur les problèmes généraux intéressant les conditions de travail résultant de l'organisation du travail, de la technologie (…).

EXIGENCES RÉGLEMENTAIRES

Autres textes – Droit du travail

⇨ Exemple de projets et/ou mesures de sécurité concernés

- Dispositifs de vidéo-surveillance
- Dispositifs de contrôle d'accès physique
- Dispositifs de surveillance électronique (Trace des activités, traces de connexion)
- Dispositifs de biométrie

EXIGENCES RÉGLEMENTAIRES

Autres textes – Loi Godfrain

Loi Nº 88-19 du 5 janvier 1988 relative à la fraude informatique

- ⇨ Accès ou maintien frauduleux dans un système informatique :
  - ✓ 2 mois à 1 an de prison, et 300 à 7500 euros d'amende.
- ⇨ Accès ou maintien frauduleux dans un système informatique avec dommages involontaires : modification ou suppression de données, altération du fonctionnement du système
  - ✓ 2 mois à 2 ans de prison, et 1 500 à 15 000 euros d'amende.
- ⇨ Entrave volontaire au fonctionnement d'un système informatique :
  - ✓ 3 mois à 3 ans de prison, et 1 500 à 15 000 euros d'amende.
- ⇨ Introduction, suppression, modification intentionnelles de données :
  - ✓ 3 mois à 3 ans de prison, et 300 à 75 000 euros d'amende.
- ⇨ Suppression, modification intentionnelles du mode de traitement, des transmissions de données :
  - ✓ 3 mois à 3 ans de prison, et 300 à 75 000 euros d'amende.
- ⇨ Falsification de document informatique, usage de document falsifié :
  - ✓ 1 an à 5 ans de prison, et 3 000 à 300 000 euros d'amende.

EXIGENCES RÉGLEMENTAIRES

Autres textes : Réglementations sectorielles

- Bancaire (AMF, CRBF, PCI DSS, …)
  - Préservation de l'intégrité et de la confidentialité des informations bancaires (Secret Bancaire)
  - Contrôle des SI, appréciation et maîtrise du niveau de sécurité.
  - Continuité d'activité des Prestations Essentielles
  - Garantie du secret bancaire
- Santé (Décrets, codes de la santé, …)
  - Préservation de l'intégrité et de la confidentialité des informations de santé
  - Gestion du droit d'en connaître
- Postes et Télécommunication
  - …