



MÉTHODOLOGIE D'ANALYSE DES SYSTÈMES D'INFORMATION

INSA

INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Cyril Segretain

03/12/2018

Bonjour à tous

- Cyril Segretain

- cyril@segretain.fr ou cyril.segretain@uniglo.eu
- INSA CVL STI Promo 2016



- Harmonie Technologie (Paris)

- Consultant Gouvernance, Risque et Conformité en Sécurité des Systèmes d'Information
- Missions d'analyses de risques en secteur bancaire



- Novidys (Paris)

- Consultant GRC
- Accompagnement RSSI / Analyses de risques / Audit 27002



- Uniqlo Europe (Londres)

- Information Security Officer (Europe)
- GDPR, IS policies, Security Operation, Project assessment, PCI-DSS, Audit, ...

Plan des cours

- 1. Risques et sécurité du système d'information**
- 2. Méthodologies d'analyse de risques**
- 3. Normes ISO 27k**
- 4. Politiques de sécurité des systèmes d'information**
- 5. Conformité : les législations importantes (LPM, GDPR)**

Tout va bien.

- Un pays est relié à Internet via une seule fibre optique principale qui traverse des jardins de particuliers.
- Une entreprise internationale fonctionne avec des dizaines de milliers de postes de travail sous Windows XP et Windows 7 depuis plusieurs mois/années.
- Une société crée une API pour que des partenaires puissent faire des requêtes sur leur base de données de millions d'utilisateurs.
- Un centre de commande industriel installe une machine à café connectée.

Prenons le premier exemple

Objectif	Fournir un accès Internet à un pays		
Composants nécessaires	<ul style="list-style-type: none"> Fibre Routeur PC 	<ul style="list-style-type: none"> Câble Ethernet Ingénieur réseau Batiment 	
Les besoins	<ul style="list-style-type: none"> Accès Internet tout le temps Accès Internet pour tout le monde Confidentialité des échanges Suivi des accès à Internet et de la maintenance 		
Les risques	Description	Impact	Probabilité
	Coupure d'Internet car fibre HS	Très fort	Faible
	Coupure d'Internet car routeur HS par une attaque physique (femme de ménage par exemple)	Moyen	Haute
	Coupure d'Internet car routeur HS par une attaque logicielle (remote access pour installer un APT dans le firmware)	Fort	Moyenne
	...		

SÉCURITÉ DES SYSTÈMES D'INFORMATION

POURQUOI ?

Pourquoi protéger son système d'information

NotPetya

STUXNET

Wannacry

EQUIFAX

- L'actualité nous montre que la sécurité est nécessaire à la protection des systèmes d'information de chaque entreprise.
- Aucun système n'est parfait... (même les produits de sécurité) (même vivre dans une grotte)
- Se protéger principalement contre :
 - des attaques volontaires,
 - l'environnement,
 - des erreurs d'utilisation du SI.

Il faut avoir une sécurité adaptée à son SI

- Il est nécessaire de mettre en place une sécurité adaptée au SI de l'entreprise.
- Chaque mesure de sécurité mise en place doit répondre à un risque afin de le diminuer ou le supprimer.

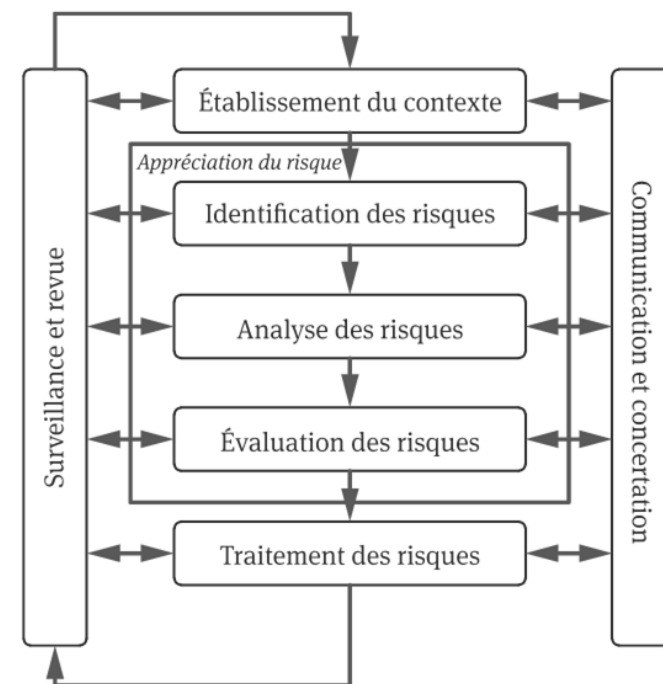


L'enjeu de la sécurité des systèmes d'information

- 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 sécurité des SI vise à protéger les intérêts des **métiers** utilisateurs des SI.
- La sécurité ne doit pas être un obstacle à l'utilisation du système d'information de l'organisation. Au contraire, la sécurité du SI doit :
 - Pouvoir répondre au **besoin de protection** souhaité par le métier utilisateur
 - Participer à la **qualité de service** attendue par le métier
 - **Couvrir les risques** que le métier craint

L'analyse de risques : pourquoi ?

- L'analyse de risques est une étape incontournable de tout projet ayant un impact sur le système d'information.
- Elle permet :
 - D'identifier les menaces pesant sur votre projet,
 - De vérifier si le « cadre de sécurité prédéfini » couvre vos besoins de sécurité,
 - D'effectuer une évaluation objective du niveau de criticité de votre projet, à travers la description de son contexte applicatif et de ses enjeux principaux,
 - D'identifier les scénarios de risques et choisir les tâches, mesures et actions de contrôle à mettre en œuvre durant le cycle de vie de votre projet.
- L'objectif de l'analyse de risques est d'atteindre un « **niveau de sécurité adapté** » de l'application/système aux enjeux de la sécurité du projet.



Processus de management du risque d'ISO 31000:2009

LES BESOINS DE SÉCURITÉ



INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
CENTRE VAL DE LOIRE

Parlons en terme de besoin des entreprises

Comment définir le niveau de sécurité d'un bien du S.I. ?
Comment évaluer si ce bien est correctement sécurisé ?

- Le business doit définir ses **besoins** en termes de sécurité sur ses processus
 - Qualité de service à rendre
 - Sensibilité d'une information pour l'entreprise
 - Exigences réglementaires à respecter
 - Fonctionnement global d'un service
 - ...

Disponibilité, Intégrité, Confidentialité

DISPONIBILITÉ

- Propriété d'accessibilité à l'information souhaitée
- Garantie qu'une fonction rend le service attendu en temps voulu et dans les conditions d'usage prévues

INTÉGRITÉ

- Propriété d'exactitude et de complétude des biens et informations
- Garantie qu'une fonction fournit les résultats attendus

CONFIDENTIALITÉ

- Propriété des biens de n'être accessibles qu'aux personnes autorisées et ce dans les temps et conditions définies.

PREUVE / TRAÇABILITÉ

- Propriété d'un bien permettant de retrouver, avec une confiance suffisante, les circonstances dans lesquelles ce bien évolue.
- Traçabilité des actions. Imputabilité de l'acteur. Non-répudiation.

- Echelle globale de notation pour les critères de sécurité :



- *Certaines entreprises commencent à prendre en compte un critère de réglementation*
 - *RGPD, PCI-DSS, Loi Sapin II, SOX, HIPAA, ...*

Echelle besoin de sécurité

- Ces échelles sont à définir avec le contexte de l'entreprise pour établir les bons niveaux

Besoin		1	2	3	4
D	Disponibilité	Faible > 2 jours	Moyenne < 1 jour	Forte < ½ jour	Indisponibilité non tolérée < 4h
I	Intégrité	Aucune	Standard Détection des modifications	Renforcée Correction des modifications	Inaltérable Modification impossible
C	Confidentialité	Publique	Interne Interne à l'entreprise	Confidentiel Limité à un groupe de personnes	Secret Limité à une liste nominative de personnes
P	Preuve	Aucune	Minimale Présence (Qui s'est connecté)	Simple Actions réalisées	Détaillée Rejouer les actions

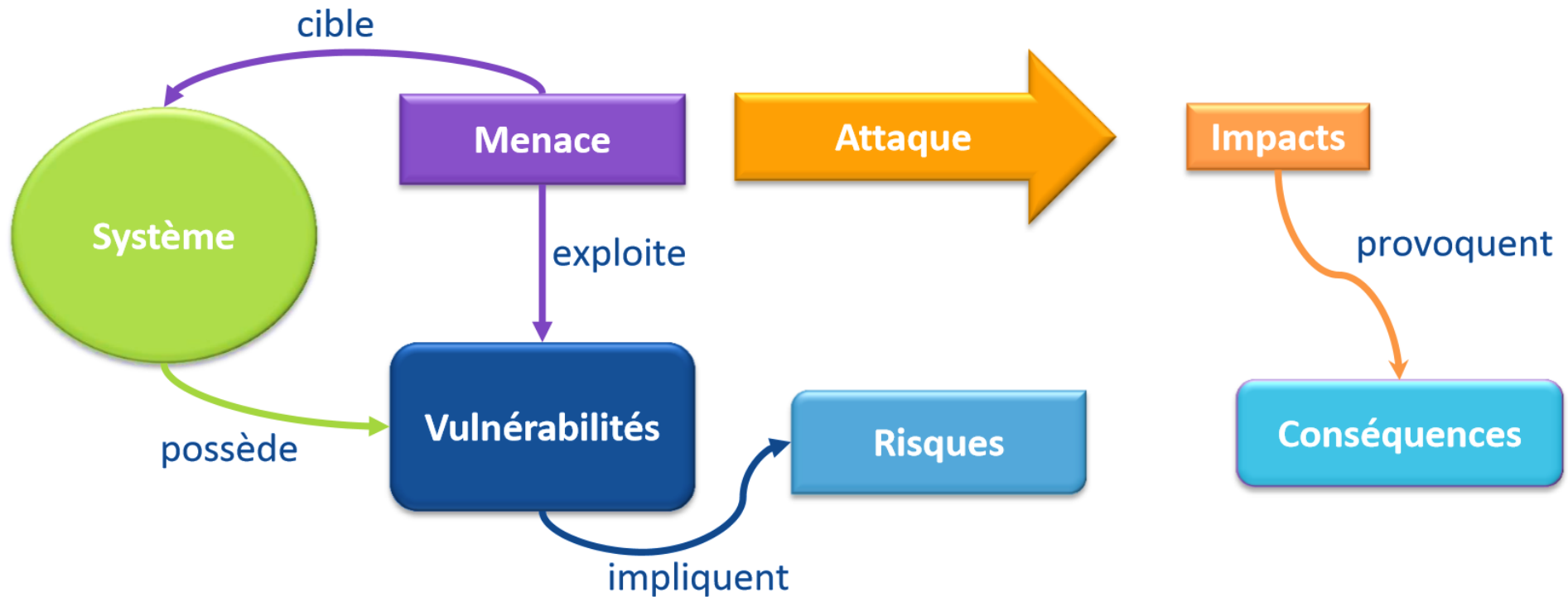
- Cette matrice est un exemple. Les valeurs doivent être définies par l'entreprise.

Exemple

- Webmail pour les étudiants de l'INSA CVL
 - Quels sont les besoins pour cette application ?
 - Qu'est-ce que l'Institut veut fournir comme qualité de service avec cette application ?

Besoin		Niveau	Explication
D	Disponibilité	3	Le service a besoin d'être accessible pendant les périodes d'ouverture de l'INSA (semaines de cours) et pour l'administration en permanence.
I	Intégrité	3	Les mails ne doivent pas pouvoir être modifiés ou supprimés, il doit être possible de détecter et corriger les erreurs.
C	Confidentialité	4	Les mails sont confidentiels entre l'expéditeur et le destinataire.
P	Preuve	2	Savoir qui accède au webmail pour investiguer en cas d'incident.

LES RISQUES



- Un scénario de risque, c'est la probabilité qu'une menace qui cible un système possédant des vulnérabilités exploite une vulnérabilité ayant des impacts qui provoqueraient des conséquences.

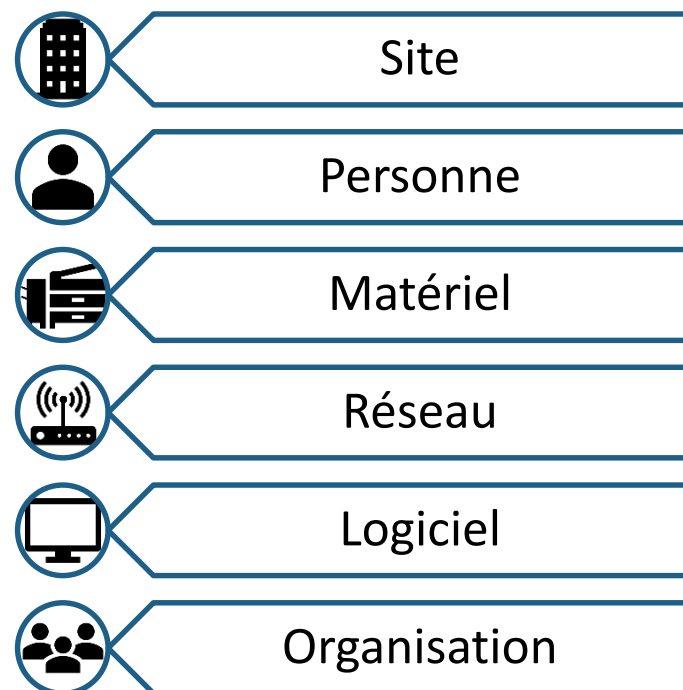
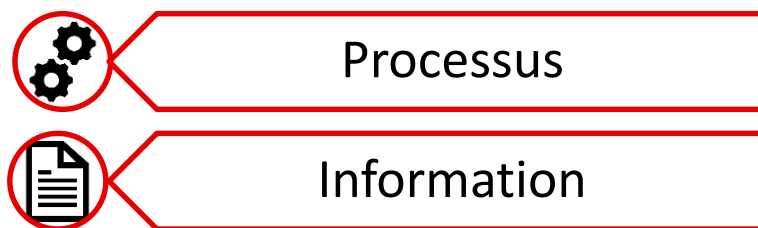
Un système d'information est composé d'actifs

- Un actif ou un bien est un élément représentant de la valeur pour l'organisation et nécessitant, par conséquent, une protection.

DES ACTIFS PRIMORDIAUX

et

DES ACTIFS SUPPORTS



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

Vulnérabilité

- Une vulnérabilité est une **faiblesse** sur un bien/actif qui peut être au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien.
- Exemples :
 - Backdoor, code non durci
 - Système obsolète
 - CVE
 - Porte de zone restreinte ouverte



- Une menace est une **cause** potentielle (interne ou externe) d'un incident indésirable, qui pourrait entraîner des dommages sur le système ou un de ses actifs.

- Exemples :

- Malveillance interne ou externe
- Erreur de manipulation
- Défaillance technique
- Environnement

Niveau des attaquant
Simple utilisateur (non informaticien)
« Bidouilleur » ou informaticien
Hacker expérimenté
Mercenaire de l'information

- Une menace peut se caractériser avec les critères suivants :

- Origine
- Type
- Source
- Motivation de la source



Scénario de risque

- Le risque est la **probabilité** qu'une menace exploite une vulnérabilité d'un actif afin de réaliser une action non souhaitée sur le SI.
- Un **événement redouté** représente la vision métier d'un scénario dont la survenance aurait un impact pour l'activité de l'entreprise.
- Chaque scénario de risque a des impacts identifiés sur un ou plusieurs actifs :
 - Financier, stratégique, d'image, juridique, ...
- La criticité d'un scénario de risque se calcule par :

$$\text{Criticité} = \text{Probabilité} \times \text{Impact}$$



Echelle de probabilité

- Il est nécessaire de définir une échelle pour évaluer la probabilité d'apparition d'un risque. Cette échelle doit être :
 - Explicite
 - Non ambigu
 - Avec des limites claires

Probabilité / Vraisemblance	Minime 1	Significative 2	Forte 3	Maximale 4
	< 25%	25-50%	50-75%	> 75%
	Moins d'une fois par an	Une fois par an	Une fois par mois	Une fois par semaine
	Cela ne devrait pas se (re)produire	Cela pourrait se (re)produire	Cela devrait se (re)produire un jour ou l'autre	Cela va certainement se (re)produire prochainement


Exemple échelle d'impact





Impacts Types d'impacts	1 Faible	2 Significatif	3 Fort	4 Majeur
Financier	< 100 000 €	Entre 100 000 € et 1 million €	Entre 1 million € et 10 millions €	> 10 millions €
Image	Protestation sans intervention des médias	Presse locale ou régionale	Médias nationaux Journal de 20h	Médias internationaux et nationaux sur plusieurs jours
Juridique	Résolution amiable	Tribunal civil	Tribunal civil avec sanctions importantes	- Tribunal pénal - Annulation de contrats importants
Opérationnel	- Retard et perturbation de courte durée - Impact business faible	- Retard et perturbation de moyenne durée - Impact moyen sur le business	- Incident grave - Fort impact sur le business - Dommages matériels et corporels	- Incident majeur - Impact majeur sur le business et les activités

- Chaque entreprise doit adapter ces échelles à son contexte et les ressources qu'elle doit protéger.

Exemple

- Arrêt du Webmail INSA CVL car un étudiant a mis le service KO par DDoS










Probabilité / Vraisemblance	Minime 1	Significative 2	Forte 3 	Maximale 4
	< 25%	25-50%	50-75%	> 75%
	Moins d'une fois par an	Une fois par an	Une fois par mois	Une fois par semaine
	Cela ne devrait pas se (re)produire	Cela pourrait se (re)produire	Cela devrait se (re)produire un jour ou l'autre	Cela va certainement se (re)produire prochainement

Impacts	1 Faible	2 Significatif	3 Fort	4 Majeur
Types d'impacts				
Financier	< 100 000 € 	Entre 100 000 € et 1 million €	Entre 1 million € et 10 millions €	> 10 millions €
Image	Protestation sans intervention des médias 	Presse locale ou régionale	Médias nationaux Journal de 20h	Médias internationaux et nationaux sur plusieurs jours
Juridique	Résolution amiable	Tribunal civil 	Tribunal civil avec sanctions importantes	- Tribunal pénal - Annulation de contrats importants
Opérationnel	- Retard et perturbation de courte durée - Impact business faible	- Retard et perturbation de moyenne durée - Impact moyen sur le business	- Incident grave - Fort impact sur le business - Dommages matériels et corporels 	- Incident majeur - Impact majeur sur le business et les activités

Criticité = Probabilité x Impact


3 x 3

Webmail INSA CVL: scénarios de risques

	Type	Type d'actif	Description du scénario de risque
	R1 - Défaillances techniques	Hébergement	Dimensionnement insuffisant de l'infrastructure
	R1 - Défaillances techniques	Hébergement	Défaillance électrique (foudre, perte de puissance, ...)
	R3 - Pertes et vols de données	Données	Perte/Vol de documents papiers en situation de mobilité
	R3 - Pertes et vols de données	Données	Incapacité à restaurer les sauvegardes
	R3 - Pertes et vols de données	Données	Suppression des données par un administrateur malveillant
	R4 - Indisponibilité de l'application	Applicatif	Indisponibilité d'un processus/de l'application suite à une attaque (déni de service, etc.)
	R4 - Indisponibilité de l'application	Applicatif	Indisponibilité d'un processus/de l'application suite à une opération perturbatrice (audit, maintenance, etc.)
	R5 - Réglementations et lois	Données	Non respect des lois et réglementations en vigueur (pénalités régulateurs, AMF, CNIL, ...)
	R7 - Attaque	Données	Espionnage à distance des actions d'un intervenant dans une situation de mobilité (lieu public, télétravail, ...)
	R7 - Attaque	Applicatif	Intrusion sur le système par un attaquant (Exploitation de failles applicatives (par exemple cross-site scripting) pour effectuer des opérations frauduleuses)
	R7 - Attaque	Applicatif	Ecoute des flux
	R7 - Attaque	Applicatif	Corruption du site pour diffusion de logiciel malveillant dans le SI ou pour propagation aux utilisateurs se connectant au site infecté

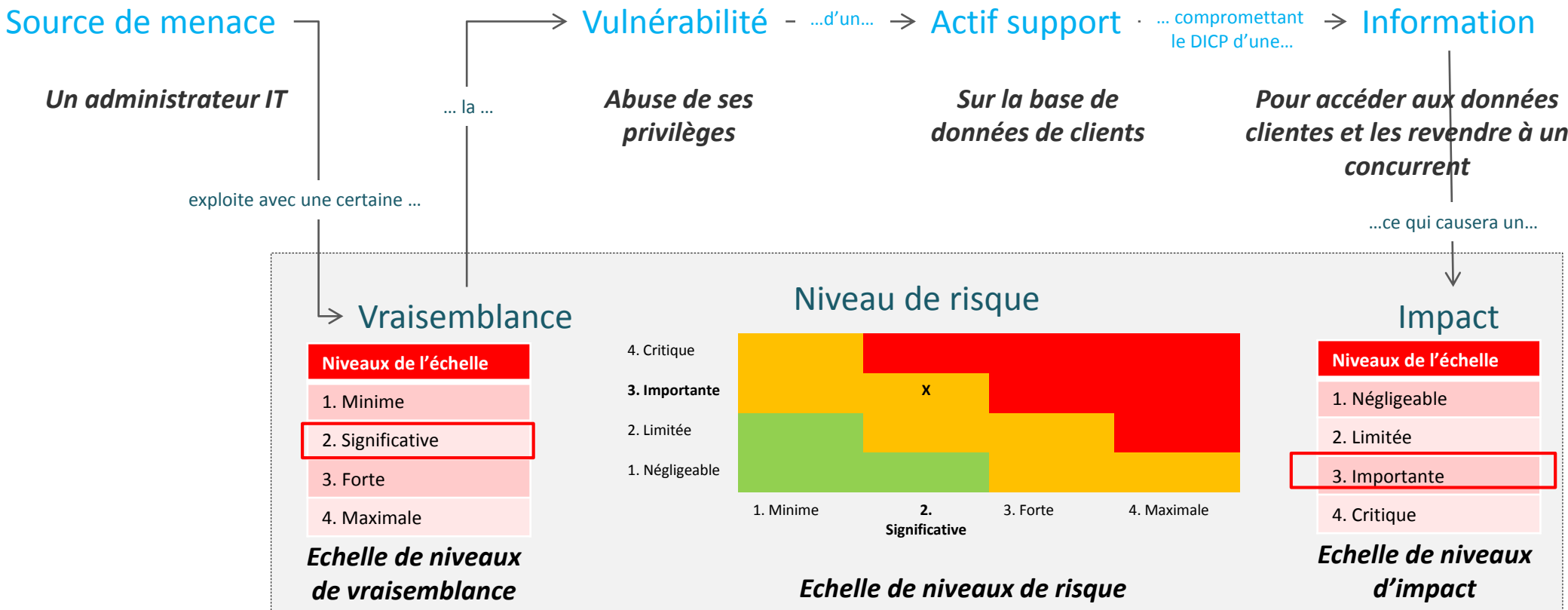
Matrice de risques

- Une matrice de risques permet de visualiser les différents risques qui pèsent sur le système.

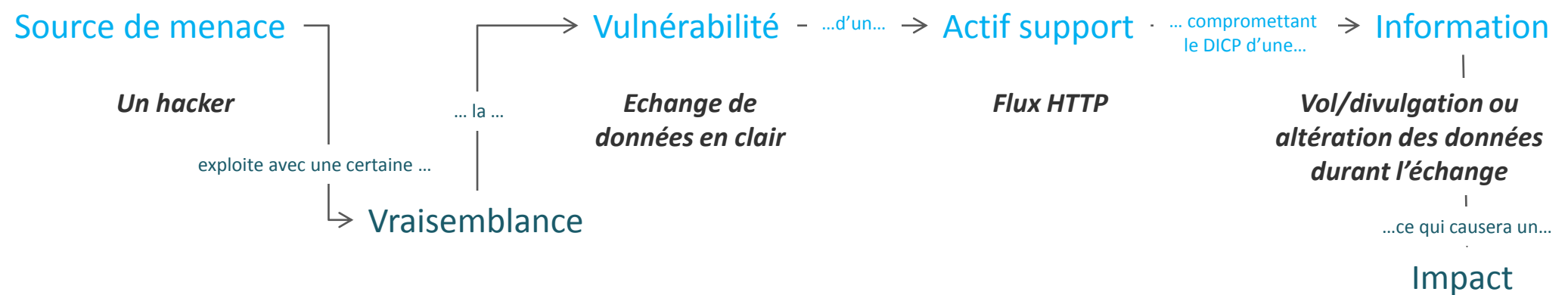
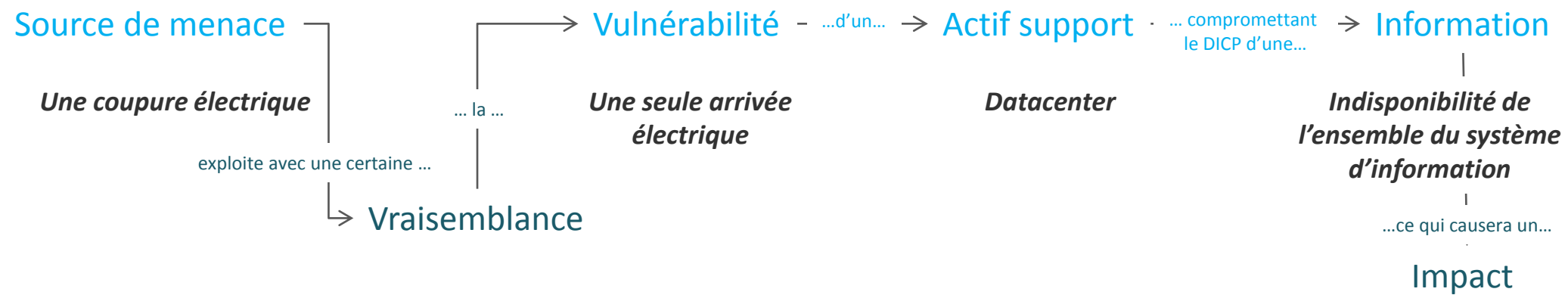
<div> <div>Probabilité</div> <div>Impact</div> </div>	Minime 1	Significative 2	Forte 3	Maximale 4
Critique 4	Significatif 4	Fort 8	Majeur 12	Majeur 16
Important 3	Significatif 3	Fort 6	Fort 9 	Majeur 12
Significatif 2	Faible 2	Significatif 4	Fort 6	Fort 8
Faible 1	Faible 1	Faible 2	Significatif 3	Significatif 4

- En se basant sur cette matrice, il est plus facile de faire un choix sur le traitement des risques.

Schéma récapitulatif



Exemples



Traitement des risques

- Lorsque les scénarios de risques menaçant le SI sont identifiés, il est nécessaire de traiter les risques en faisant un des choix suivants :

RÉDUIRE LE RISQUE

Mise en place de mesure afin de réduire le risque à un niveau acceptable

ACCEPTER LE RISQUE

Pas d'action sur ce risque.
Responsabilité d'acceptation de ce risque.

ÉVITER LE RISQUE

Supprimer l'actif, l'évènement ou la situation concernée par le risque.

TRANSFÉRER LE RISQUE

Utiliser un tiers qui est en mesure de traiter le risque afin de déplacer la responsabilité.

- Le traitement des risques se fait en se basant sur la matrice de risques mais également en prenant en compte les coûts et délais projet.

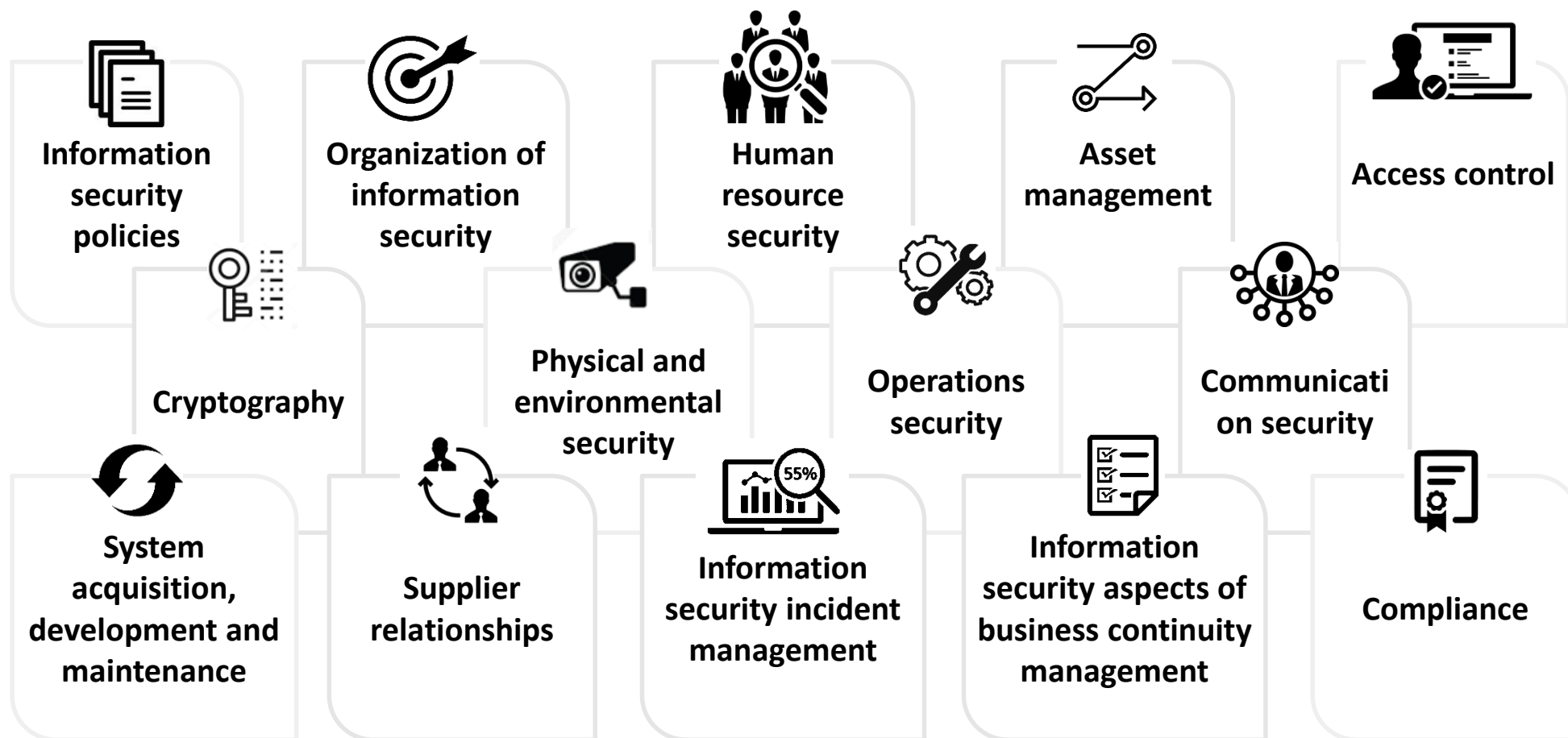
Mise en place de mesures de sécurité

- Dans le traitement des risques, il faut prendre en compte les mesures de sécurité permettant de réduire, éviter ou transférer le risque.
- Une mesure de sécurité s'applique sur un actif/bien support.

Mesure de prévention	Mesure de détection	Mesure de réaction
Avant l'évènement	Au moment de l'évènement	Après l'évènement
<ul style="list-style-type: none"> ■ Dissuasion ■ Robustesse et Protection ■ Formation et Sensibilisation 	<ul style="list-style-type: none"> ■ Détection ■ Alertes ■ Communication 	<ul style="list-style-type: none"> ■ Cloisonnement, Limitation ■ Correction ■ Récupération ■ Assurance
Réduire les vulnérabilités Eviter l'apparition d'incident	Bloquer, contenir et détecter les événements	Limiter les Impacts Revenir à l'état normal

Les mesures de sécurité à travers les chapitres de l'ISO

- Dans l'ISO 27001:Annexe A (aussi appelée ISO 27002), les mesures de sécurité (bonnes pratiques actuelles) se décomposent en **14 chapitres** – 35 objectifs de sécurité – 114 mesures de sécurité :



Exemples de mesures de sécurité

■ Mesures techniques

- **Infrastructure** (virtualisation, haute disponibilité, multi-sites, ...)
- **Hébergement** (on-premise, SaaS, Cloud, ...)
- **Exploitation** (MCO, MCS, systèmes, ...)
- **Architecture** (3-tiers, API, web, authentification, ...)
- **Réseau** (protocoles sécurisés, redondance, supervision, droit d'accès, ...)
- **Développement** (OWASP)
- **Chiffrement** (protocole, implémentation, gestion des clés, ...)
- ...

■ Mesures fonctionnelles

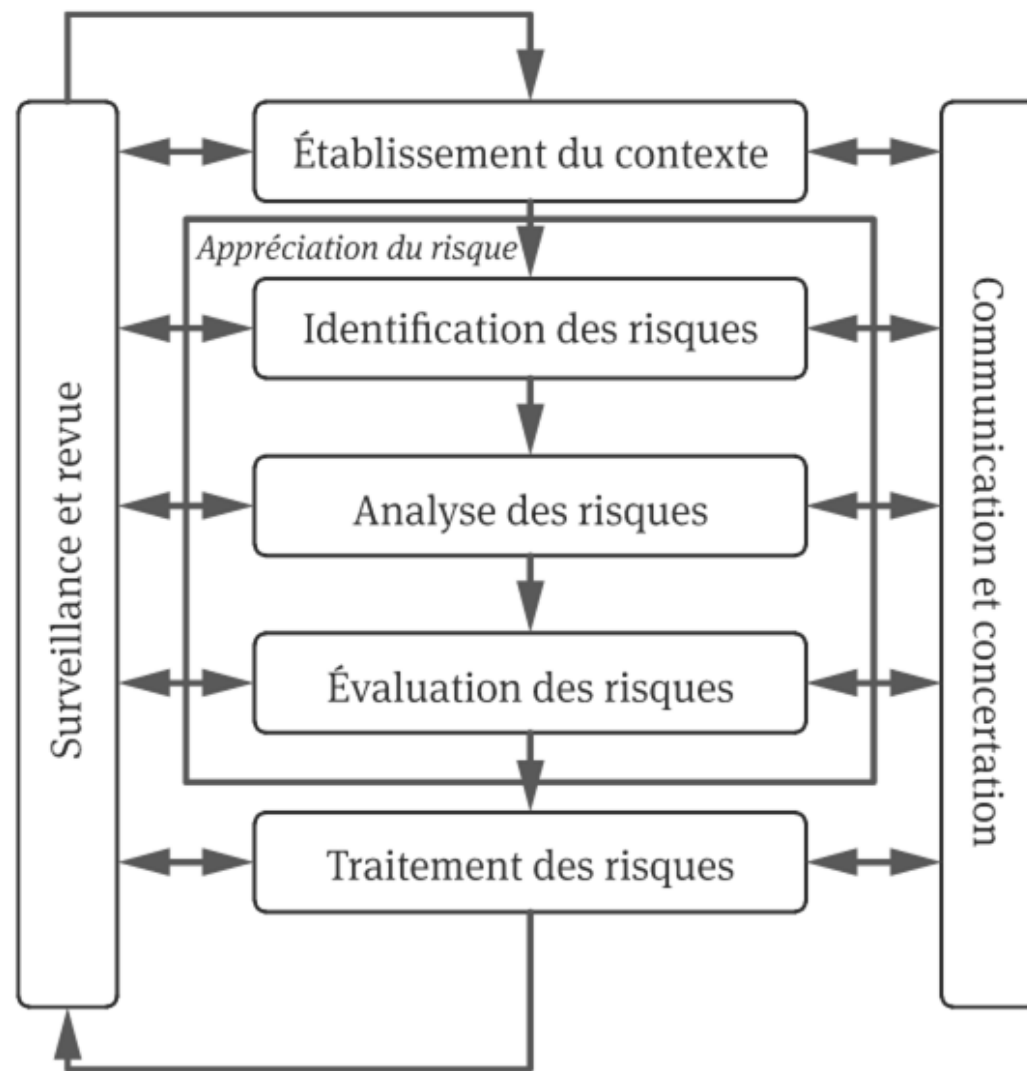
- **Habilitation** (gestion des droits, des accès, procédures, ...)
- **Sauvegarde** (fréquence, test, ...)
- **Archivage** (externalisation, support, test, validité, ...)
- **Procédures** (politique de sécurité, fournisseurs, ...)
- **Formation** (utilisateurs, admin, développeurs, ...)
- ...

Risque résiduel

- Les risques résiduels sont les risques subsistant après le traitement des risques.
- D'une manière générale, les risques résiduels sont mis en évidence selon le choix de traitement :
 - un risque évité ne génère aucun risque résiduel s'il est complètement évité ; sinon, les risques résiduels correspondent à ce qui n'est pas évité ;
 - un risque réduit mène à des risques résiduels s'il n'est pas totalement réduit ;
 - un risque pris constitue un risque résiduel à part entière ;
 - un risque transféré n'induit aucun risque résiduel s'il est totalement transféré ; sinon, les risques résiduels correspondent à ce qui n'est pas transféré.
- Les risques résiduels devront être acceptés par un responsable de l'entreprise.



L'analyse de risques



Processus de management du risque d'ISO 31000:2009

FIN DE LA 1^{ÈRE} PARTIE