Introduction Cyber Sécurité

Jean Louis Lassaigne 2020/2021

Sommaire

1 Introduction Sûreté/Sécurité

Culture Cyber - Introduction Sûreté/Sécurité

Suivant l'ISO 34001 sur les Systèmes de Management de la Sûreté

❑ Définitions

✓ Sûreté :

- La sûreté désigne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux actes spontanés ou réfléchis ayant pour but de nuire, ou de porter atteinte dans un but de profit psychique ou/et financier…

  => On cible ici la Malveillance

✓ Sécurité :

- La sécurité désigne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face aux risques techniques, physiques, chimiques et environnementaux pouvant nuire aux personnes et aux biens sans avoir un but de profit…

  => Nous sommes plus ici sur le périmètre de l'incident ayant pour cause origine toute autre volonté que la malveillance

❑ Pour aller plus loin

✓ Sécurité physique

La sécurité physique, est la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc. On va donc y retrouver en guise d'exemple

- la gestion et sécurisation des flux de biens et de personnes
- la surveillance de son bâtiment / patrimoine
- la protection périmétrique de son bâtiment / patrimoine
*- la prévention **des malveillances**...*

✓ Sécurité logique

La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation. On va donc y retrouver en guise d'exemple :

- la gestion et sécurisation des accès informatiques et des identités
- la protection des données et des systèmes d'informations
- la sécurisation des réseaux et des infrastructures IT
- la sécurité liée aux nouvelles technologies (applications...)...

Pour aller plus loin

Sécurité des activités et des process

Dans la sécurité des activités et des process, on peut intégrer :
- la continuité d'activité et gestion de crise
- la maîtrise et performance des installations et des systèmes d'organisation
- la sécurisation & traçabilité des marchandises / de la production
- la protection de l'environnement...

Continuité d'activité et gestion de crise

La gestion de crise est l'ensemble des modes d'organisation, des techniques et des moyens qui permettent à une organisation de se préparer et de faire face à la survenance d'une crise puis de tirer les enseignements de l'évènement pour améliorer les procédures et les structures dans une vision prospective.

Plan de continuité d'activité

Le plan de continuité ou plan de continuité d'activité (PCA) est à la fois le nom d'un concept, d'une procédure et du document qui la décrit.
Ce plan doit permettre à un groupe (gouvernement, collectivité, institution, entreprise, hôpital..) de fonctionner même en cas de désastre ; quitte à ce que ce soit en mode dégradé, ou en situation de crise majeure.

❑ Sûreté et sécurité, une Hiérarchisation ?

- ✓ Une approche possible est de positionner
  - la sûreté comme l'ensemble des processus mis en place pour lutter contre la malveillance
  - la sécurité comme la déclinaison technique de tout ou partie de ces processus
- ✓ Exemple:
  - La sécurité informatique consiste en la mise en place de moyens techniques et organisationnels pour lutter contre la survenance d'un incident « de sécurité » qui peut avoir pour origine un acte volontaire (malveillance) ou un acte involontaire une erreur
  - La sécurité des accès, la sécurité périmétrique sont tous deux des composantes de la sûreté bâtimentaire ou des sites

Patrimoine

- ✓ Peut être défini comme l'ensemble des valeurs produites par l'entreprise
  - Patrimoine informationnel,
  - Patrimoine Client,
  - Patrimoine financier,
  - Patrimoine humain,
  - Etc.

❑ La déclinaison de ces définitions au sein d'une entreprise

- ✓ Quelle organisation sécurité pour une entreprise ?
  - Le nécessaire besoin d'indépendance de la sûreté : rôle du gendarme
  - Le nécessaire besoin de rattachement direct à la plus haute instance de l'entreprise
  - « Le patrimoine de l'entreprise ne peut être considéré comme **sûre** que lorsque les menaces qui pèsent sur son environnement ont été identifiées au préalable et que les contre mesures nécessaires ont été mises en place avant que ces menaces ne puissent exploiter une vulnérabilité pour produire un incident »

Culture Cyber - Introduction Sûreté/Sécurité

La Sûreté de l'Information

- ✓ Un Directeur de la sécurité rattaché directement au Président
- ✓ Porter les 3 axes d'activités principales
  - Sécurité Informatique ou logique, pilotée par un RSSI directement rattaché au directeur de la sécurité
    - Prend en compte tous les aspects de la sécurité logique
  - Sécurité physique et bâtimentaires pilotée par un RSP directement rattaché au directeur de la sécurité
    - Prend en compte la sécurité des bâtiments et des personnes
  - La Continuité d'Activité et la gestion de crise, pilotée par le RPCA directement rattaché au directeur de la sécurité
    - Prend en compte la continuité d'activité
    - Et la gestion de crise
- ✓ Ne pas oublier le DPO (RGPD)

❑ Les référentiels et les normes

✓ Quelques directives et référentiels sur la sûreté et la sécurité

- Normes ISO
  - ISO 27001 : 2013 : Système de Management de la Sécurité de l'Information (revue en 2022)
  - ISO 27005 : 2008 : Gestion des Risques en Sécurité de l'Information
  - ISO 27005 : 2022 : Revoit et adapte la norme au management du risque (EBIOS RM)
  - ISO 27701 : 2019 : Gouvernance et mesures de sécurité pour le traitement des données à caractère personnel
  - ISO 34001 : 2016 : Système de Management de la Sûreté
  - ISO 22301 : 2012 : Système de Management de la Continuité d'Activité
- Directives
  - 2012 - Sur la PPST : Protection du Potentiel Scientifique et Technique de la Nation
  - NIS : Network Information Security : Assurer un niveau de sécurité commun et élevé pour les pays de l'UE

❑ Les référentiels et les normes (suite)

- ✓ Règlement
  - RGPD : Règlement Général sur la Protection des Données Personnelles
- ✓ Instruction
  - IGI 1300 : Instruction Générale Interministériel, portant sur la protection du secret de la Défense Nationale
  - IGI 6600 : Instruction Générale Interministériel, portant sur la protection des Secteurs d'Activité d'Importance Vitale

❑ Les organisations

- ✓ L'Agence Nationale à la Sécurité des Systèmes d'Information ANSSI
  - Rattachée au SGDSN (Secrétariat Général de la Défense et Sécurité Nationale (SGDSN) du 1er Ministre
- ✓ Les Services des Hauts Fonctionnaire de Défense (HFDS)
  - Se retrouvent dans chaque ministère, en lien avec l'ANSSI

=> *Le tout forme la voie fonctionnelle SSI, VFSSI*

- ✓ La Commission Nationale de l'Informatique et des Libertés (CNIL)
  - *Loi Informatique et Libertés du 06 janvier 1978*
- ✓ *L'OWASP* Open Web Application Security Project
  - communauté en ligne travaillant sur la sécurité des applications Web

Culture Cyber - Introduction Sûreté/Sécurité

❑ La veille

- ✓ La principale qualité nécessaire au métier de la sécurité est la curiosité
  - Rester à l'écoute des nouvelles technologies
  - Suivre l'évolution des menaces
  - S'instruire, partager..
- ✓ L'ANSSI
- ✓ LinkedIn
- ✓ Cybermalveillance.gouv.fr
- ✓ Les CERT (cert.ssi.gouv.fr)

Culture Cyber - Introduction Sûreté/Sécurité

❑ Les métiers

- ✓ L'ANSSI liste les métiers de la cyber sécurité
  - Le RSSI
  - L'analyse SOC
  - L'ingénieur Sécurité Applicative
  - L'auditeur pentester
  - L'auditeur infrastructure
  - L'auditeur gouvernance
  - Le risque manageur
  - Le consultant
- ✓ Tous ces métiers peuvent être classés dans deux grandes thématiques
  - La sécurité défensive
  - La sécurité offensive

Culture Cyber - Introduction Sûreté/Sécurité

- **Les menaces actuelles**
  - ✓ DDOS
  - ✓ Phishing
  - ✓ Ransomware

2 Introduction Gestion de risques

Sommaire

1. **Introduction à la Gestion de Risque**
2. **ISO 27005 : 2008**

Nota : Reste volontairement sur cette version, donne de bonnes pratiques pour débuter en gestion de risques

Introduction à la gestion de risques

La gestion des risques en sécurité de l'information, un processus perpétuel

- Question ouverte : Selon vous qu'est-ce qu'une analyse de risque et quel est son objectif ?

Introduction à la gestion de risques

La gestion des risques en sécurité de l'information, un processus perpétuel

- Pourquoi ?
  - ✓ L'entreprise est vivante, elle évolue dans un environnement sans cesse en mouvement
  - ✓ Les dirigeants doivent connaître le milieu dans lequel ils évoluent et pouvoir appréhender les interactions que celui-ci aura avec leur entreprise
  - ✓ L'entreprise est une somme de processus qui concourent tous vers le même objectif, son développement
  - ✓ La sécurité est un processus de l'entreprise, un processus particulier car elle se retrouve à tous les niveaux
    - La sécurité doit connaître avec la même finesse que le Président l'environnement de l'entreprise
    - La sécurité évolue donc parallèlement à l'entreprise,

La gestion des risques en sécurité de l'information, un processus perpétuel

- Comment qualifier les interactions ?
  - ✓ Opportunités
  - ✓ Incidents
  - ✓ Conflits,
  - ✓ Etc.

  - ✓ ***Elles sont multiples et difficilement quantifiables, par contre toutes absolument toutes sont porteuses de risques !***

- Exercice 1

Introduction à la gestion de risques

La gestion des risques en sécurité de l'information, un processus perpétuel

- De fait l'identification des risques doit être un processus
  - ✓ perpétuel,
  - ✓ flexible
  - ✓ Itératif

- Pourquoi Itératif ?
  - ✓ Améliorer le niveau de détails des risques au fil des itérations
  - ✓ Rester en liens étroit avec l'environnement évolutif de l'entreprise
  - ✓ Permettre d'apporter la **bonne réponse** au risque
    - Toujours résoudre l'équation entre le temps nécessaire et l'effort pour identifier comment traiter le risque
    - Ou si on parle sécurité comment identifier la bonne mesure de sécurité

Introduction à la gestion de risques

La gestion des risques en sécurité de l'information, doit TOUJOURS amener à une prise de décisions

- Le fait d'identifier un risque et de communiquer ce risque impose de caractériser le risque pour **donner au décideur la capacité à prendre la bonne décision**
  - ✓ Identification des risques
  - ✓ Estimation des risques
  - ✓ Evaluation des risques

- L'identification des risques et l'évaluation des risques font partie d'un processus que l'on appelle l'appréciation du risques et qui vient après l'établissement du contexte et avant le traitement du risque

- Communiquer sur un risque c'est mener à bien toutes ces étapes.

Introduction à la gestion de risques

Pour élargir : La gestion des risques dans l'entreprise

- L'organe décisionnel sera toujours au niveau de la Direction
- Comité de Pilotage des Risques
  - ✓ Définir le niveau d'acceptation des risques
  - ✓ Valider les plans de traitements des risques
- Typologie de risques
  - ✓ Juridique
  - ✓ Financiers
  - ✓ Pénal
  - ✓ Administratifs
  - ✓ De l'information
  - ✓ Technologique
  - ✓ Condition et sécurité des travailleurs,
  - ✓ etc
- Le support sera le plus souvent une matrice de risque « maison »

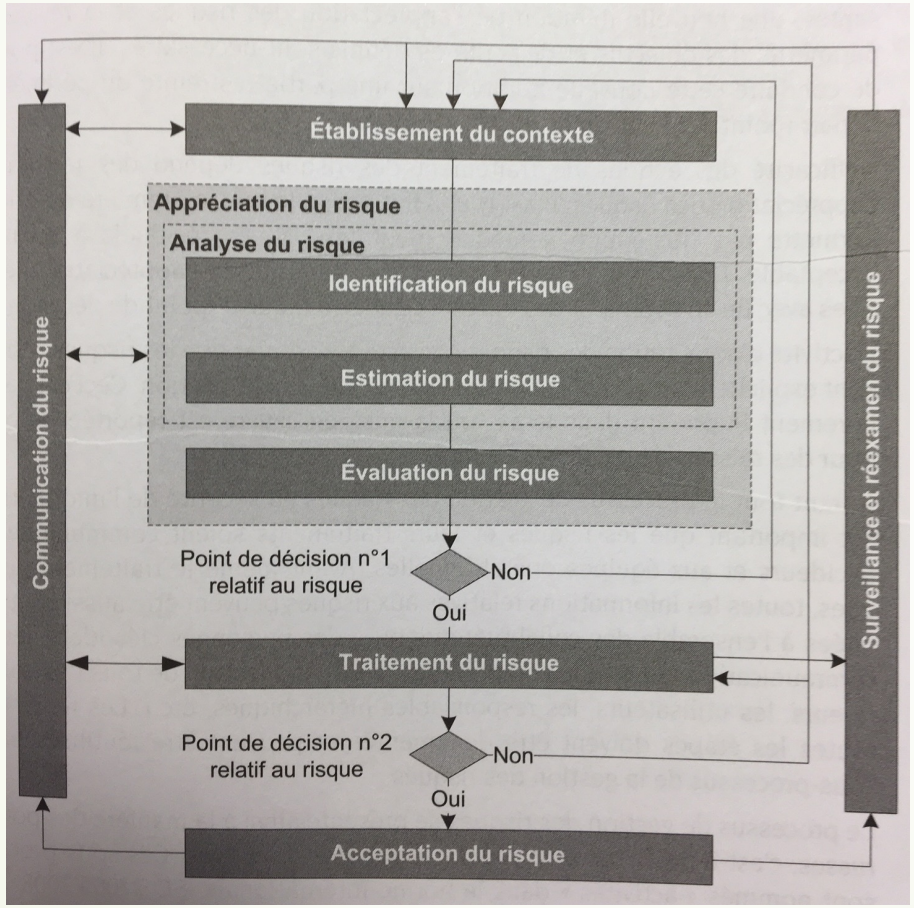
ISO 27005 : 2008

La norme ISO 27005 décrit le processus de gestion des risques en sécurité de l'information.

- Elle est composée de 12 chapitres et 4 annexes
  - ✓ La description du processus débute réellement à partir du chapitre 6
    - Chap 6 : Présentation du processus
    - Chap 7 : Etablissement du contexte
    - Chap 8 : Appréciation du risque
    - Chap 9 : Traitement du risque
    - Chap 10 : Acceptation du risque
    - Chap 11 : Communication du risque (plan de …)
    - Chap 12 : Revue des risques
  - ✓ Les annexes
    - Annexe A : L'entreprise et la typologie ou les contraintes à prendre en compte
    - Annexe B : Identification des actifs
    - Annexe C : Catalogue de menaces
    - Annexe D : Catalogue de vulnérabilités et les menaces qui peuvent les exploiter

ISO 27005 : 2008

- **Modélisation du Processus**



ISO 27005 : 2008

Avant de mener une analyse de risque, il est nécessaire de savoir identifier un actif

- Un Actif c'est quoi ?
  - ✓ Selon la norme ISO 2700 : 2009 « Tout élément représentant de la valeur pour l'organisme »
  - ✓ Selon la norme ISO 27005 : 2008 « Un Actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant par conséquent une protection (8.2.1.2). »

- Les actifs primordiaux (ou essentiels EBIOS)
- Les actifs de supports ou physiques

ISO 27005 : 2008

Les propriétés d'un actif

- Tout actif dispose d'un propriétaire
  - « Personne ou entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des actifs. Bien dissocier la propriété de l'actif qui peut être différente.
- Tout actif est caractérisé par son besoin en CID qui va définir sa valeur
  - Confidentialité
  - Intégrité
  - Disponibilité
- Question ouverte : comment définissez vous CID ?
- Autre propriété …

  - Exercice 2

ISO 27005 : 2008

La motivation de la gestion de risques:
La Menace et la Vulnérabilité

- Une **menace** exploite une vulnérabilité, propriété d'un actif qui devient la cible de la menace. Dans l'annexe C de l'ISO 27005, une menace doit toujours être décrite suivant
  - ✓ son type
  - ✓ Sa nature
  - ✓ Son origine
  - ✓ Sa motivation

- La **vulnérabilité**, est une faille de l'actif dans une mesure de sécurité qui peut être exploitée par une menace (ISO 27000:2009). Bien voir la vulnérabilité comme une propriété de l'actif. Se rapporter aux propriétés de l'actif

ISO 27005 : 2008

Comment lié les risques à la réalité ?

La vraisemblance

Elle sera toujours la résultante de la facilité d'exploitation par la probabilité d'occurrence .

⇒ Probabilité d'occurrence de la menace

⇒ Facilité d'exploitation de la vulnérabilité

ISO 27005 : 2008

Des risques vers l'incident

Mesurer l'impact d'une menace sur un actif ne suffit pas pour construire une gestion de risques. Il est nécessaire de construire des scénarios. Ces scénarios sont la caractérisation de la relation entre menaces et vulnérabilités

- ✓ Par la description de la menace exploitant la vulnérabilité
- ✓ Par le type de relation
  - Une menace peut exploiter plusieurs vulnérabilités
  - Plusieurs menaces peuvent exploiter la même vulnérabilité

❑ Exercice 3

ISO 27005 : 2008

La Définition du risque

La norme ISO 27005 : 2008 définit le risque comme suit

« Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise donc à l'organisation. »

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte

Dans le processus de gestion des risques, établir le contexte c'est :

- ✓ Identifier le périmètre
- ✓ Identifier la faisabilité du projet
- ✓ Identifier les critères de base comme la hiérarchisation des risques, la valorisation des actifs
- ✓ l'organisation

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte :

- Les données en entrée du processus : ce seront toutes les informations nécessaires sur l'organisme
- Les activités :
  - ✓ Définir quels sont les objectifs de l'AR
  - ✓ Définir quels sont les critères de base
  - ✓ Définir le périmètre et surtout ses exclusions
  - ✓ Décrire ou étudier l'organisation
  - ✓ Identifier les actifs primordiaux
- Les données en sorties s
  - ✓ Les objectifs (de sécurité)
  - ✓ Les critères de bases
  - ✓ L'organisation de la gestion de risques

ISO 27005 : 2008

Processus de gestion des risques

Etablissement du Contexte – Qu'est-ce que les critères de bases ?????

Pour la norme ISO 27005 : 2008, ils sont au nombre de 3

- Les critères d'impact : il s'agit de la valorisation des conséquences des risques sur une activité
  - ✓ Par rapport à l'actif CID
  - ✓ Par rapport à l'organisme
- Les critères d'évaluation
  - ✓ Estimer le risque pour être en mesure de prioriser le traitement
- Les critères d'acceptation des risques
  - ✓ Choix du traitement du risque

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte – Qu'est-ce que les critères de bases ?????

Pour la norme ISO 27005 : 2008, ils sont au nombre de 3

- Les critères d'impact : il s'agit de la valorisation des conséquences des risques sur une activité
  - ✓ Par rapport à l'actif CID (mais pas que ☺)
  - ✓ Par rapport à l'organisme
- Les critères d'évaluation
  - ✓ Estimer le risque pour être en mesure de prioriser le traitement
- Les critères d'acceptation des risques
  - ✓ Choix du traitement du risque

ISO 27005 : 2008

Processus de gestion des risques

Etablissement du Contexte – Qu'est-ce que les critères de bases ?????

Rappel : Un risque c'est l'exploitation d'une vulnérabilité par une menace.

Pour identifier les critères d'évaluation des risques, il faut donc identifier les critères d'évaluation

- d'une menace : sur la probabilité d'occurrence de celle-ci
- d'une vulnérabilité : sur la facilité d'exploitation de celle-ci

- Donne la vraisemblance !

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte – Construire les échelles

Il faut au préalable se mettre d'accord sur la définition de celles-ci.

- La sécurité
- Le juridique
- Les finances
- La prod
- Etc.

Les échelles doivent être compréhensibles et acceptées de TOUS.

Limiter aussi le nombre de niveau, généralement quatre suffisent.

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte – Construire les échelles

Exemple d'échelle sur la vraisemblance

Niveau	Vraisemblance
4	Très probable
3	Probable
2	Possible
1	Très improbable

ISO 27005 : 2008

Processus de gestion des risques

Etablissement du Contexte – Construire les échelles

Exemple d'échelle sur la vraisemblance (suite) : résultat de la probabilité d'occurrence par la facilité d'exploitation

Niveau	PO	FE
4	Systématique	Facile, grand public, aisé
3	Fréquente (eg1/semaine)	Bidouilleur, simple
2	Régulière (eg 1/mois)	Connaissance universitaire, difficile
1	Très rare	Exerptise

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte – Construire les échelles

Exemple d'échelle sur la vraisemblance (suite) : Traduire le produit

PO/FE	1	2	3	4
1	1	2	2	3
2	2	2	3	3
3	3	3	3	4
4	3	3	4	4

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte – Construire les échelles

Echelle de conséquence des risques

Ici on peut trouver un cinquième niveau 0 : pas de conséquence

- exercice 4

Niveau	Descriptif
4	Conséquence inacceptable (faillite, etc.)
3	Conséquence majeur sur l'entreprise (perte de 30% de CA, plusieurs clients, etc.)
2	Conséquence moyenne (perte de 5% de CA, d'un client, etc.)
1	Conséquence mineure (négligeable, interne à l'entreprise, etc.)

ISO 27005 : 2008

Processus de gestion des risques
Etablissement du Contexte – Construire les échelles

Echelle des risques (question : méthode de calcul ?)

Vraisemblance		**1**				**2**				**3**				**4**			
Conséquence		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Valeur de l'actif	1	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	2	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10
	3	5	6	7	8	6	7	8	9	7	8	9	10	8	9	10	11
	4	6	7	8	9	7	8	9	10	8	9	10	11	9	10	11	12

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des risques

(Norme ISO 27005 : 2008 chapitres 8 - chapitre 8.2.1)

Il s'agit ici d'identifier

- Les actifs (rappel nous avons vu les actifs primordiaux) – 8.2.1.2
- Identifier les menaces – 8.2.1.3
- Identifier les mesures de sécurité existantes – 8.2.1.4
- Identifier les vulnérabilités – 8.2.1.5
- Identifier les conséquences – 8.2.1.6

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des risques

Les actifs

- Identifier uniquement les actifs qui sont dans le périmètre !
- Identifier un propriétaire pour tout actif et un par actif !
- Bien identifier la granularité de l'actif !
- Regrouper le actifs par grand types

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des risques

Les actifs

Pour récupérer la liste des actifs, la norme aplre de « source d'information ».

- Les actifs primordiaux: normalement réalisée lors de l'établissement du contexte, mais peut être portée à ce niveau
  - ✓ Nombre réduit
- Les actifs en supports
  - ✓ Toujours reliés à un actif primordial
  - ✓ Ils peuvent être revus lors des différentes itérations : il est préférable de commencer à un niveau « macro » puis de descendre par itérations successives

- Donner un valeur à ces actifs (CID), généralement sur un niveau de 1 à 4
- Ne garder que la valeur la plus forte qui caractérisera le niveau de sensibilité de l'actif en terme CID

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des risques

Les menaces

Quelles sont les menaces qui ciblent les actifs

- Origine naturelle
- Erreur ou action involontaire
- Etc…

Elles seront TOUJOURS de nature délibéré ou accidentelle

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des risques

Les menaces
Où les chercher ?

- Il existe des catalogues de menaces par type
- Sur les sites de veilles
- Dans la base d'incident de l'entreprise !

Une bonne pratique est d'alimenter son catalogue de menaces internes !

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des mesures de sécurité existantes

- Question ouverte :
  - ✓ Comment identifier une mesure de sécurité existante ?

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des mesures de sécurité existantes

- Comment identifier une mesure de sécurité existante:
  - ✓ Consulter la documentation existante (si elle existe ☺)
  - ✓ Questionner le propriétaire de l'actif et les utilisateurs de celui-ci
  - ✓ Effectuer un audit sur site avec audit documentaire

  Une prestation d'analyse de risque débutera TOUJOURS par un audit !

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des mesures de sécurité existantes

- Comment identifier une mesure de sécurité existante:
  - ✓ Consulter la documentation existante (si elle existe ☺)
  - ✓ Questionner le propriétaire de l'actif et les utilisateurs de celui-ci
  - ✓ Effectuer un audit sur site avec audit documentaire

  Une prestation d'analyse de risque débutera TOUJOURS par un audit !

- Pour aller plus loin:
  - ✓ Comment mener un audit ?

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des mesures de sécurité existantes

- Point d'attention sur les mesures de sécurité
  - ✓ Une mesure de sécurité peut consister en la mise en place de nouveaux actifs et ceux-ci peuvent être porteurs de vulnérabilités et de menaces !!
  - ✓ Cette problématique doit être adressée dans les itérations successives d'une Analyse de risques

- Exercice 5

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des vulnérabilités

- Rappel :
  - ✓ Qu'est-ce qu'une vulnérabilité ?

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des vulnérabilités

- Les vulnérabilités peuvent se rencontrer à de multiples niveaux, à savoir
  - ✓ Au niveau de l'organismes lui-même,
  - ✓ Au niveau de la gouvernance
  - ✓ Au niveau des activités
  - ✓ Au niveau du personnel
  - ✓ Au niveau de l'environnement
  - ✓ Au niveau du SI
    - Matériel
    - Applicatif
  - ✓ Au niveau des parties prenantes (?)

- Exercice 6

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques - Identification des conséquences

- Point d'attention : Conséquences vs impacts

  Selon l'Iso 27005 : 2008

  - ✓ l'impact est la perte exprimée en termes d'atteintes aux critères CID
  - ✓ La conséquence est la perte ou le dommage exprimée en termes d'atteintes à l'activité et ou à l'organisme

- Nous allons vulgariser ces termes en conséquences

- Exercice 7

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques – Estimation des risques

(Norme ISO 27005 : 2008 chapitres 8 - chapitre 8.2.2)

Il s'agit ici

- D'estimer les conséquences **du risque** – 8.2.2.2
- La vraisemblance des scénarios – 8.2.2.3
- Le niveau du risque – 8.2.2.4

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques – Estimation des risques

Les conséquences du risque

Il s'agira ici de mesurer l'atteinte aux critères de sécurité de l'information sur le métier et l'organisme pour chaque scénario d'incidents.

- Identifier les impacts/conséquences directes
- Identifier les impacts/conséquences indirectes

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques – Estimation des risques

Les conséquences du risque

Il s'agira ici de mesurer l'atteinte aux critères de sécurité de l'information sur le métier et l'organisme pour chaque scénario d'incidents.

- Identifier les impacts/conséquences directes
- Identifier les impacts/conséquences indirectes

- A noter : Ce sont des scénarios d'incidents !!

- Exercice 8

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques – Estimation des risques

La vraisemblance des scénarios

Il faudra identifier

- Probabilité d'occurrence des menaces
- Facilités d'exploitation des vulnérabilités
- En déduire la vraisemblance

- Et dans les itérations suivantes
  - ✓ Prendre en compte la réduction des facteurs de risques

- Exercice 9

ISO 27005 : 2008

Processus de gestion des risques
Appréciation des risques – Estimation des risques

Le niveau de risque

Il s'agit ici de valoriser le niveau de risque

- De façon qualitative
- Méthode Arithmétique
  - ✓ Addition
  - ✓ Produit
  - ✓ Vous êtes libre d'inventer une formule, mais toujours faire simple !!

- Exercice 10

ISO 27005 : 2008

Processus de gestion des risques

Appréciation du risque - Evaluation du risque – Norme ISO 27005 : 2008 Chap 8.3

Cette étape consiste en l'ordonnancement des risques par rapport à leur estimation.

- La liste des risque et les niveaux associés
- La décision face au risque

- On fini ici le processus d'évaluation du risque

Exercice 11

ISO 27005 : 2008

Processus de gestion des risques
Traitement du risque – ISO 27005 : 2008 – chap 9

Que faire face aux risques : **la décision**

- Il s'agit du choix du traitement du risque !
  - ✓ Réduire le risque : mettre en place une mesure de sécurité apte à réduire celui-ci
  - ✓ Transférer le risque , vers un tiers
  - ✓ Supprimer le risque : il s'agit de supprimer l'activité qui est à l'origine du rlsque
  - ✓ Accepter le risque

Exercice 12

ISO 27005 : 2008

Processus de gestion des risques
Traitement du risque – ISO 27005 : 2008 – chap 9

- Il faut ensuite analyser le risque résiduel
  - ✓ Entre dans la boucle de l'AR
  - ✓ Décision sur le risque résiduel
- Sortie
  - ✓ **Le plan de traitement du risque !!**

ISO 27005 : 2008

Processus de gestion des risques
Les autres processus –

- **La communication du risque – ISO 27005 : 2008 chap 11**

La communication a pour objectif principal l'aide à la prise de décision

- **Le contrôle et la révision des risques – ISO 27005 : 2008 chap 12**

Mise sous surveillance, révision des risques en fonctions de plusieurs critères

- ✓ Environnement,
- ✓ temporalité,
- ✓ Etc.

A savoir : Une AR se revisite toujours tant qu'existe l'activité en support

ISO 27005 : 2008

Processus de gestion des risques
Acceptation du risque– ISO 27005 : 2008 – chap 10

Dernier processus de la norme

- En entrée
  - ✓ Le plan de traitement des risques
  - ✓ Les risques résiduels appréciés
- Sortie
  - ✓ **Les risques acceptés avec la justification de ceux-ci**

ISO 27005 : 2008

Exemple simple Matrices de risques

Matrice des risques

Projet : [Nom_Projet]

					Evaluation brute du risque							Réévaluation			
N°	Projet / composant	Typologie du risque	Détail du risque	Actif impacté	Valeur de l'actif	Vraisemblance	Conséquence	Indice de criticité	Actions correctives/préventives envisagées/planifiées	Type de l'action	Porteurs	Valeur	Vraisemblance	Conséquence	Indice de criticité résiduelle
1															
2															
3															
4															
5															
6															
7															
8															

ISO 27005 : 2008

Processus de gestion des risques

Exercice 13

3 Gestion des Risques - Découverte EBIOS

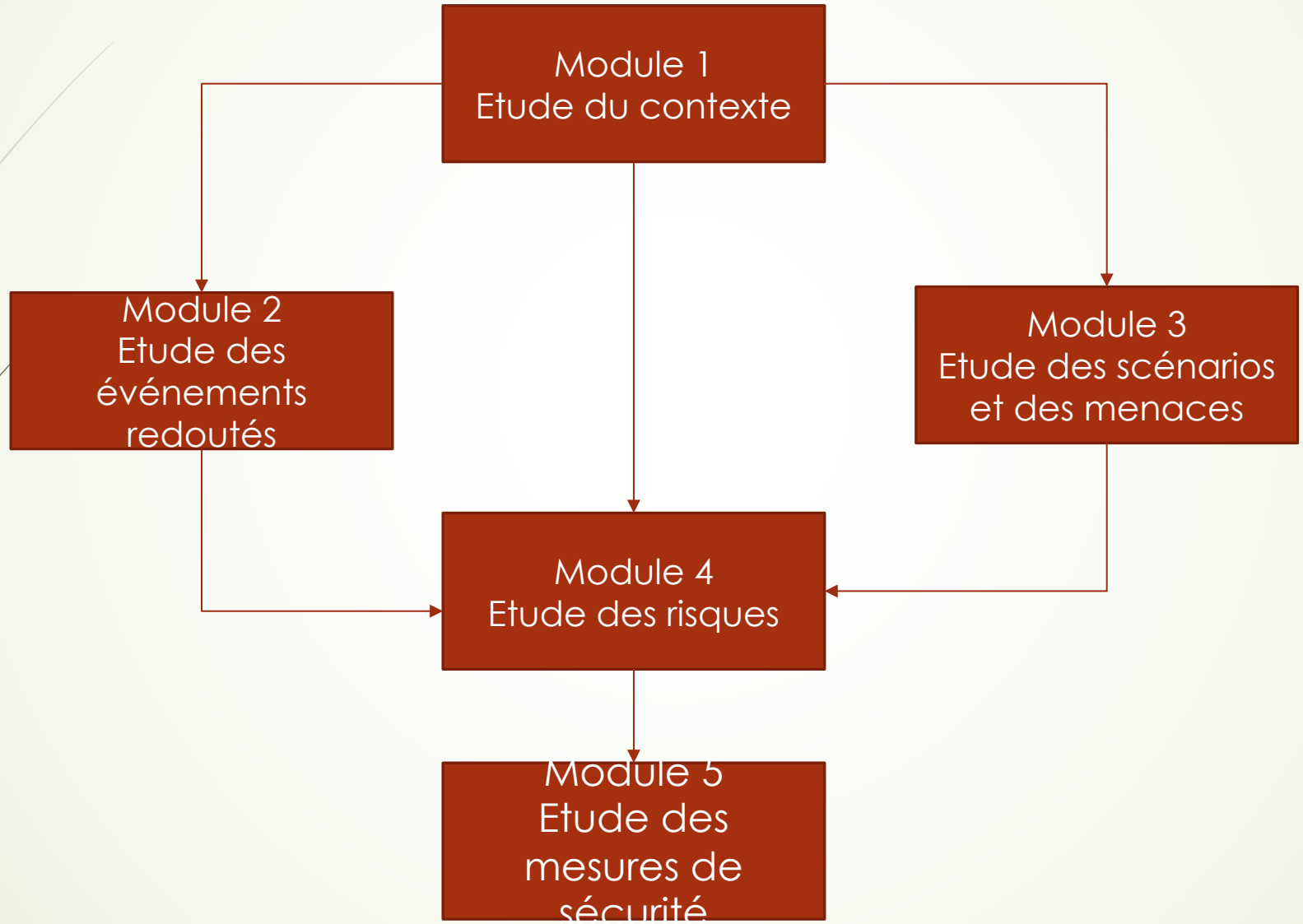
EBIOS

- Créée en 1995 par l'ANSSI, EBIOS pour Expression des Besoins et d'Identifications des Objectifs de Sécurité,
- Méthode d'analyse de risque française de référence, permet aux organisations d'apprécier et de traiter les risques,
- Evolue en 2010 sous la version EBIOS 2010. Principale évolution, rend la méthode itérative
- 2018 : Octobre 2018 EBIOS devient le Management du Risque
  - ✓ COMPRENDRE POUR DECIDER

La transformation numérique bouleverse et enrichit nos activités en rendant les systèmes, dont nous dépendons, toujours plus évolutifs et interconnectés. Nous évoluons au sein d'écosystèmes particulièrement stimulants mais aussi complexes et mouvants. Les menaces n'échappent pas à ce constat, faisant de la sécurité numérique un véritable enjeu économique et stratégique. Pour y faire face, l'ANSSI encourage la création et la mise en œuvre d'une politique de management des risques numériques complète, adaptée et intégrée au plus haut niveau des organisations. L'analyse de risque est au cœur de ce dispositif

EBIOS 2010

EBIOS 2010 – Approche Module



EBIOS

Module 1 - Etablissement du contexte

- Le cadre mis en place pour gérer les risques
- Les critères à prendre en considération
- La description du périmètre de l'étude et de son environnement

3 activités

- ACT 1 – Définir le cadre de la gestion des risques
- ACT 2 – Préparer les métriques
- ACT 3 – Identifier les biens

Module 2 – Etude des événements redoutés

- **Appréciation des risques**
  - ✓ Identifier et estimer les besoins des sécurité des biens essentiels en termes de CID
  - ✓ Tous les impacts en cas de non respect des ces besoins
  - ✓ Les sources des menaces susceptibles d'en être à l'origine
  - ✓ Et d'en tirer les événements redoutés

- ACT 2 – Apprécier les événements redoutés
  - ✓ Analyse
  - ✓ Evaluation

Module 3 – Etude des scénarios et des menaces

Fait aussi parti de l'appréciation des risques

- Estimer et identifier les scénarios qui peuvent engendrer les événements redoutés
- Obtenir de fait les risques
  - ✓ Étude des menaces pouvant être engendrées par les sources de menaces
  - ✓ Etudes des vulnérabilités exploitables

- ACT 3 – Apprécier les scénarios des menaces
  - ✓ Evaluation
  - ✓ Analyse de chaque scénario

Module 4 – Etude des risques

- Le quatrième module met en évidence les risques pesant sur l'organisme en confrontant
  - ✓ les événements redoutés
  - ✓ aux scénarios de menaces.
- décrit également comment estimer et évaluer ces risques, et enfin comment identifier les objectifs de sécurité qu'il faudra atteindre pour les traiter

- ACT 1 – Apprécier les risques
- ACT 2 – Identifier les objectifs de sécurité

Module 5 – Etude des mesures de sécurité

- C'est le traitement des risques. Il explique comment
  - ✓ spécifier les mesures de sécurité à mettre en oeuvre,
  - ✓ comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques et les risques résiduels.

- ACT 1 – Formaliser les mesures de sécurité à mettre en œuvre
- ACT 2 – Mettre en œuvre les mesures de sécurité

EBIOS

Comment utiliser EBIOS

- Il faut voir EBIOS comme un formidable outil de gestion de risques
  - ✓ Il Est possible de tout utiliser
  - ✓ De n'utiliser qu'une partie
  - ✓ De l'intégrer dans un processus ISO 27005 : 2008
- EBIOS est totalement compatible avec le norme ISO 27005 : 2008

Comment utiliser EBIOS

- EBIOS base de connaissance
  - ✓ Liste de types de biens supports
    - Question : pourquoi pas une liste des biens essentiels ?
  - ✓ Liste types d'impacts
  - ✓ Liste types de sources de menaces
  - ✓ Liste sur les menaces et vulnérabilités génériques
  - ✓ Liste de mesures de sécurité génériques

EBIOS RM

EBIOS RM

- EBIOS Risk Manager (EBIOS RM) est la méthode d'appréciation et de traitement des risques numériques publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS .
- EBIOS RM permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser.
- Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue.
- Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires.
- Alignement de la nouvelle version de l'ISO 27005/ 2022

EBIOS RM

Carte d'identité

CIBLE

Risk managers

RSSI

Chefs de projet

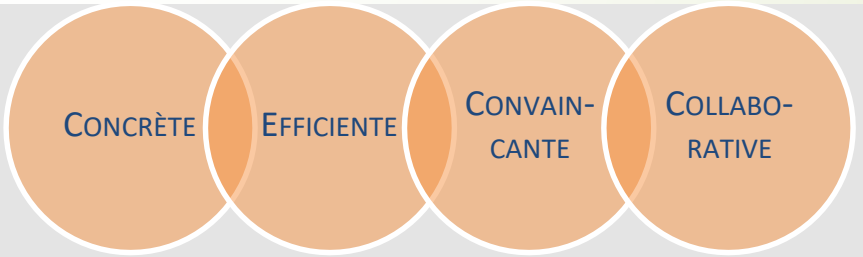
VISION

Offrir une compréhension partagée des risques cyber entre les décideurs et les opérationnels

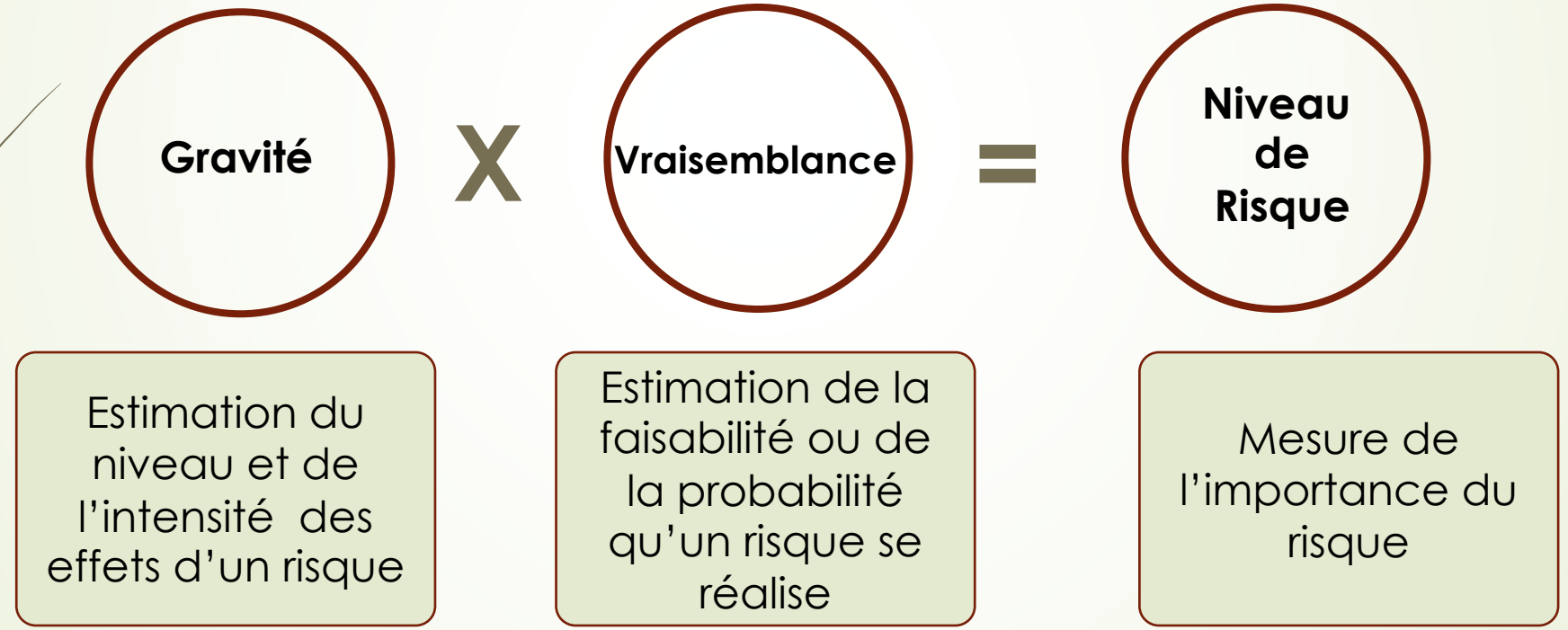
FONDAMENTAUX

- Une synthèse entre conformité et scénarios
- Une valorisation de l'état de la menace
- Une prise en compte de l'écosystème
- Un moteur de l'organisation de management du risque

VALEURS

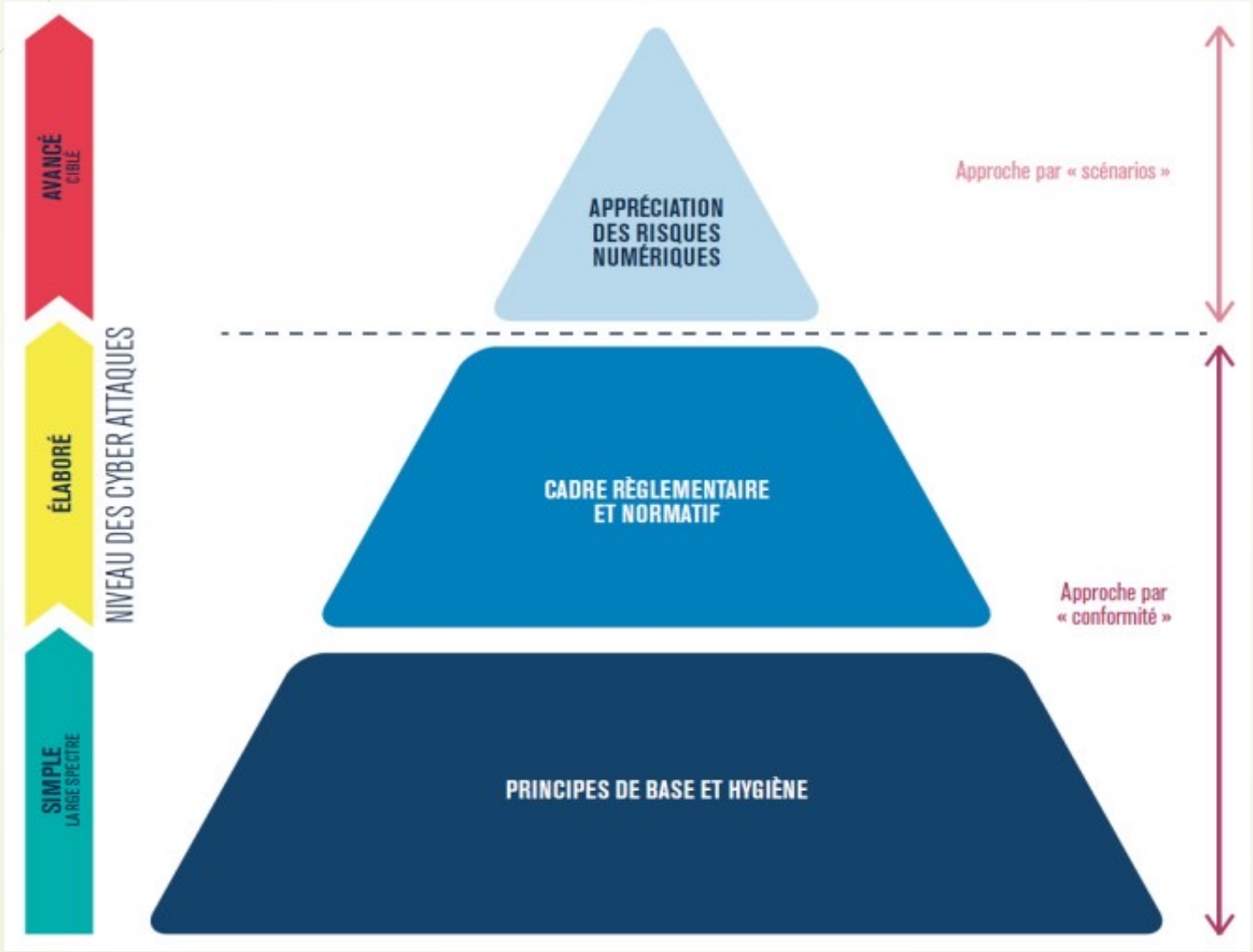


Le risque chez EBIOS Risk Manager



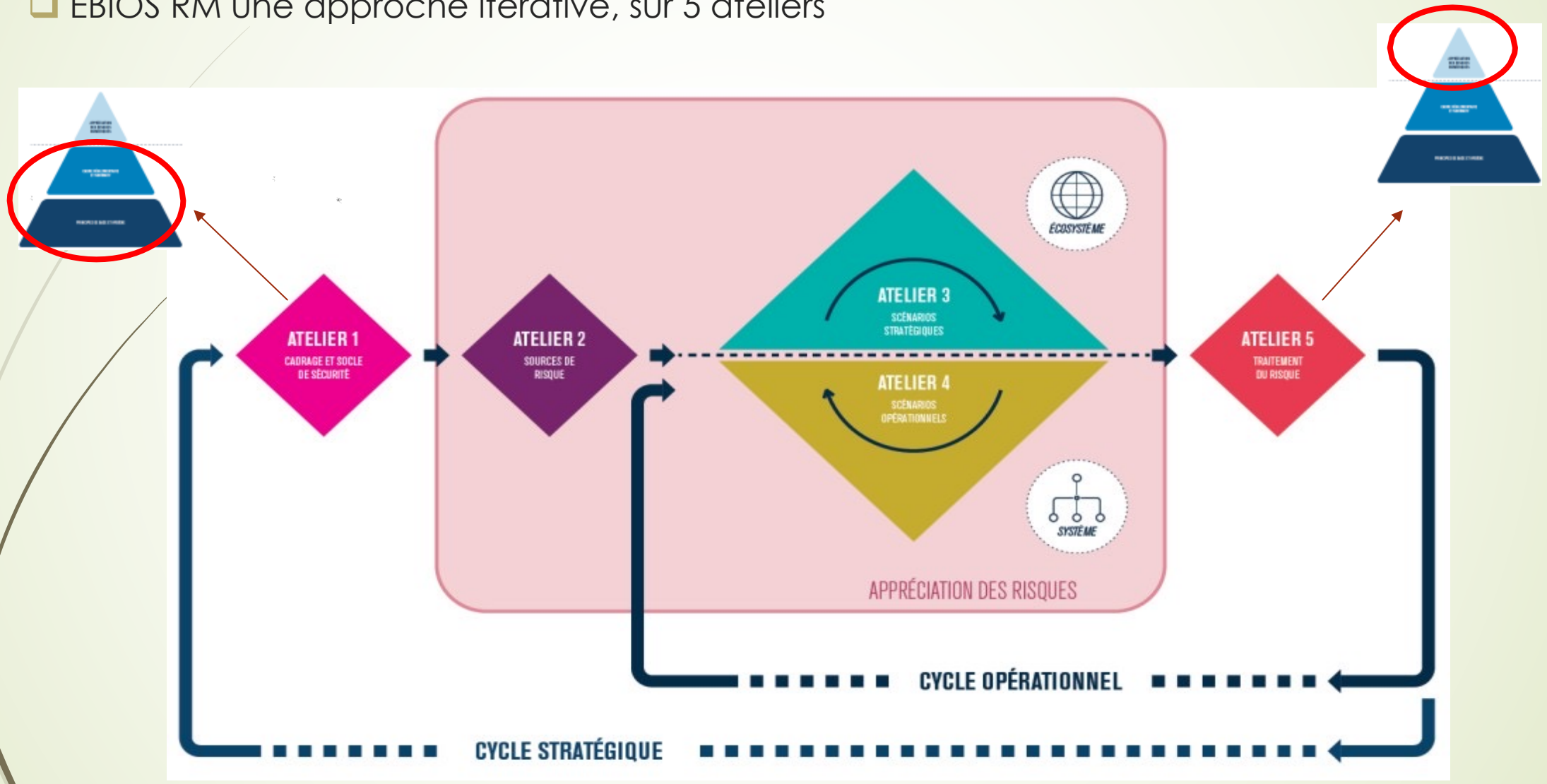
EBIOS RM

- La Pyramide de management du risque



EBIOS RM

- EBIOS RM une approche itérative, sur 5 ateliers

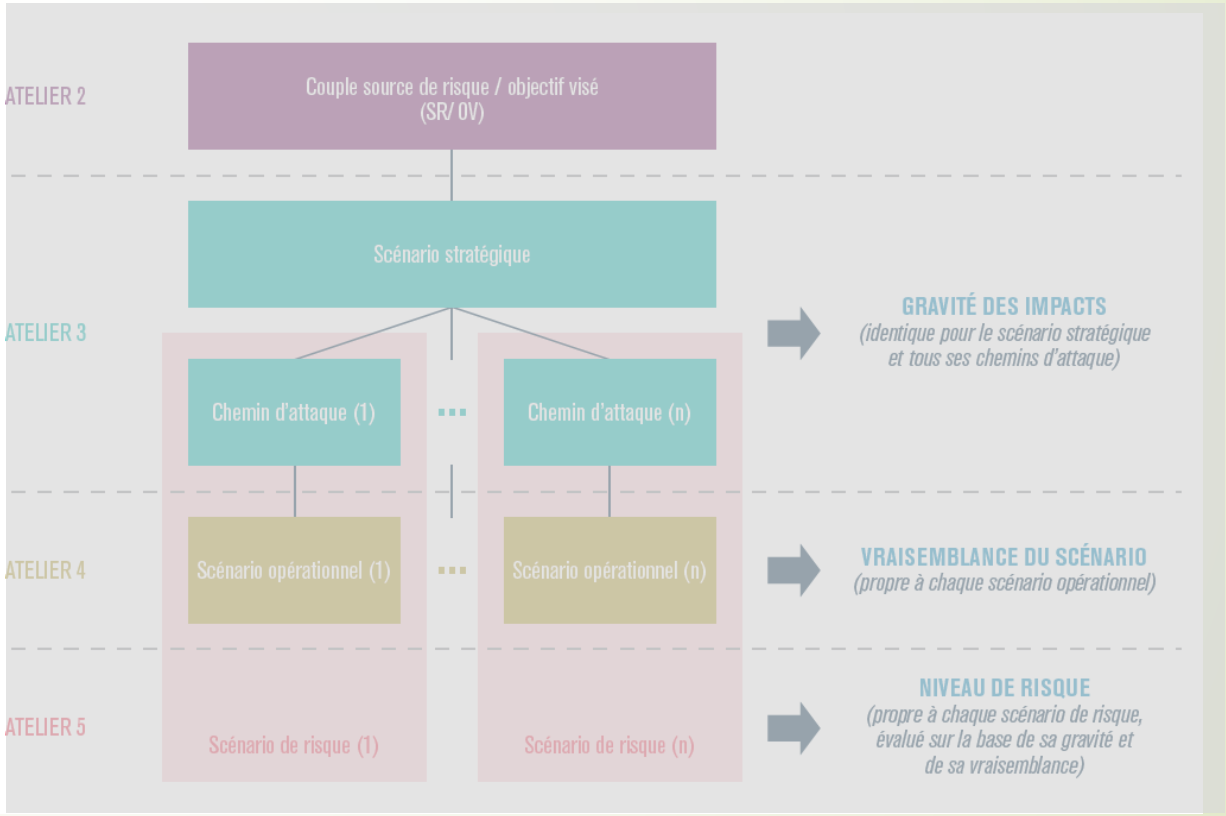


EBIOS RM – Atelier 1

- La démarche prévoit deux cycles, dont les durées sont définies lors du premier atelier :
  - ✓ un cycle stratégique revisitant l'ensemble de l'étude et en particulier les scénarios stratégiques ;
  - ✓ un cycle opérationnel revenant sur les scénarios opérationnels à la lumière des incidents de sécurité survenus, de l'apparition de nouvelles vulnérabilités et de l'évolution des modes opératoires.

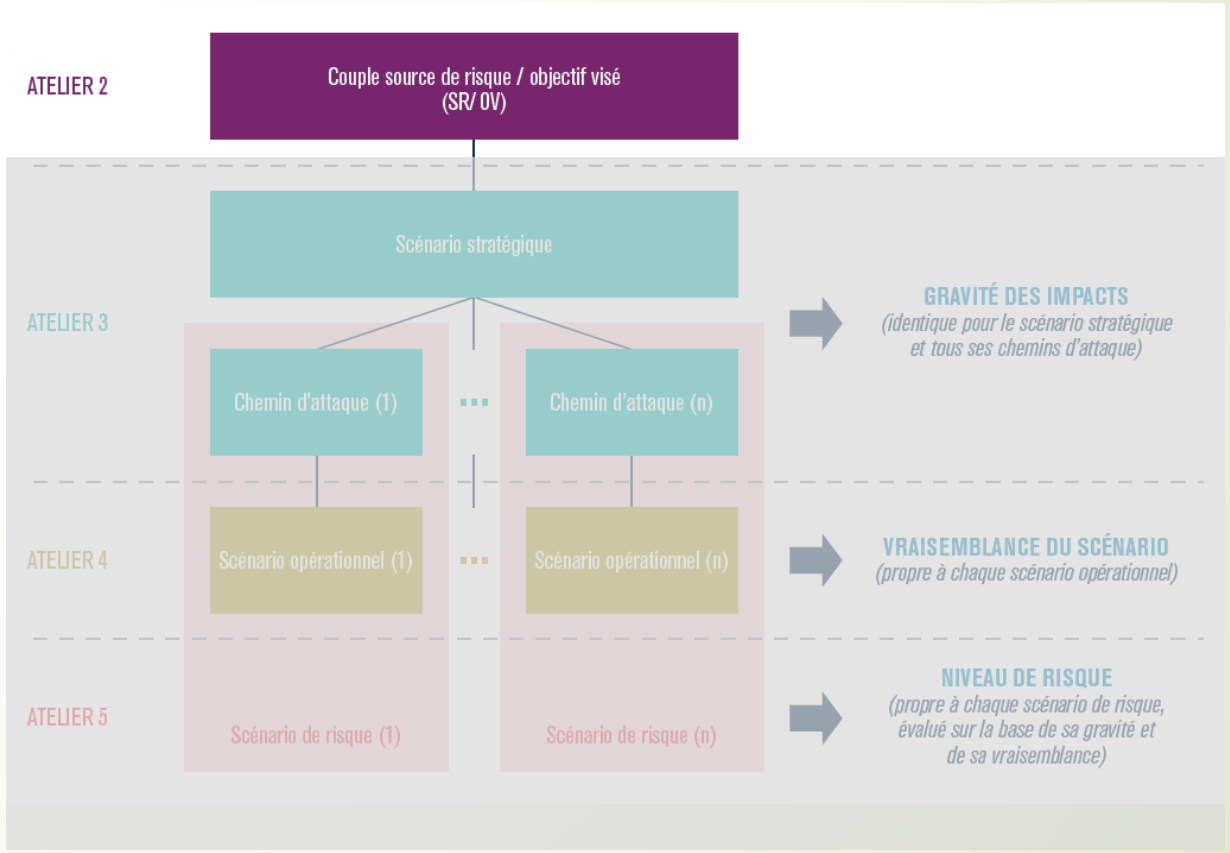
EBIOS RM – Atelier 1

- L'objet de l'étude, participants aux ateliers et le cadre temporel
- Mission, Valeurs métier, biens supports
- Évènement redoutés au valeurs métier
- Gravité et impacts
- Socle de sécurité et les écarts



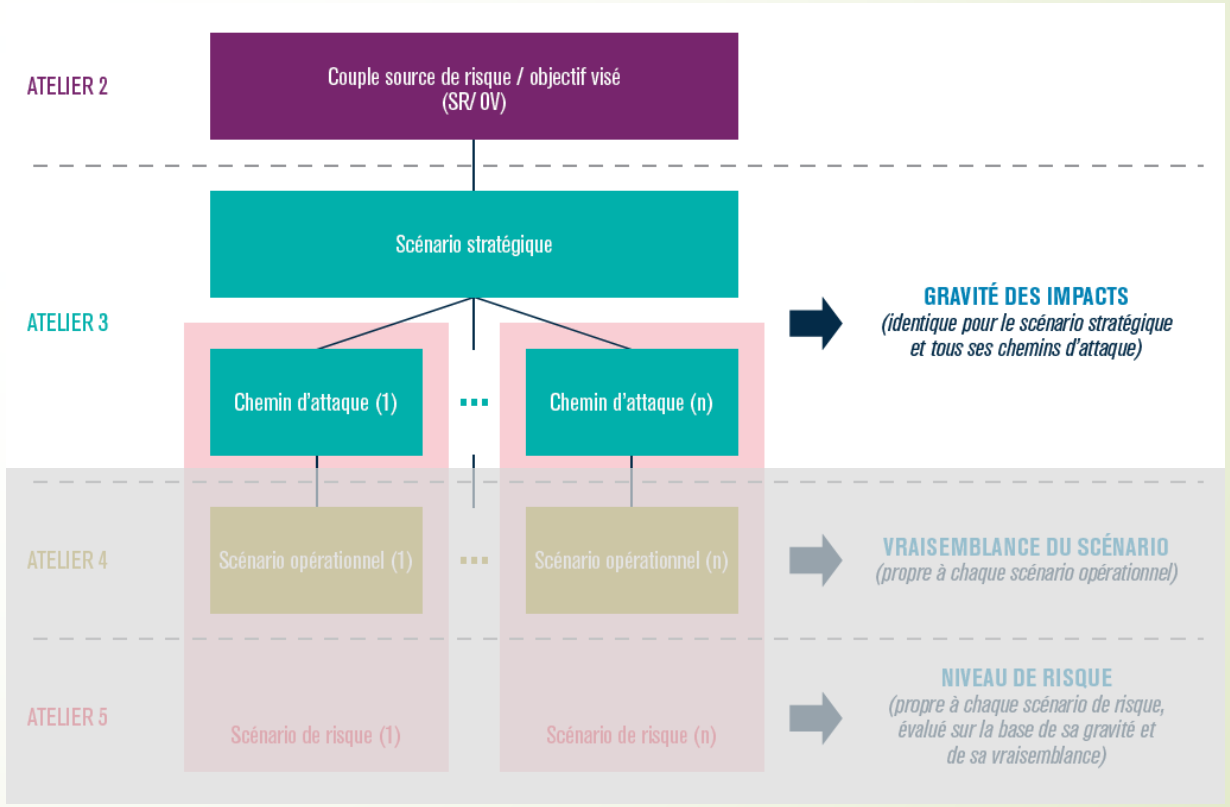
EBIOS RM – Atelier 2

- Les sources de risque (SR) et leurs objectifs de haut niveau, appelés objectifs visés (OV).
- Les couples SR/OV jugés les plus pertinents.
- Cartographie des sources de risque.



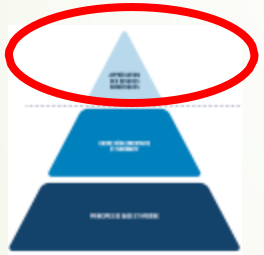
EBIOS RM – Atelier 3

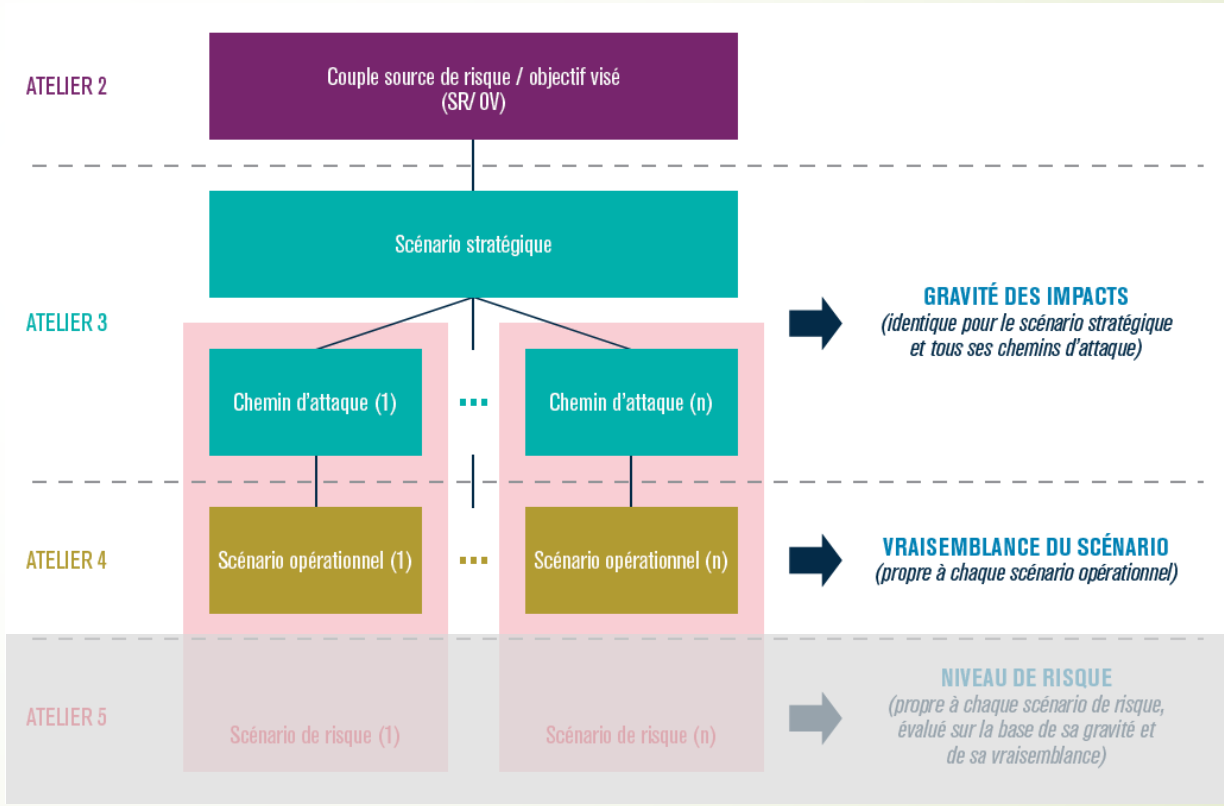
- Ecosystème
- Cartographie de menace numérique.
- Scénarios stratégiques et les chemins d'attaque qu'une source de risque est susceptible d'emprunter pour atteindre son objectif.
- Définir des mesures de sécurité sur l'écosystème



EBIOS RM – Atelier 4

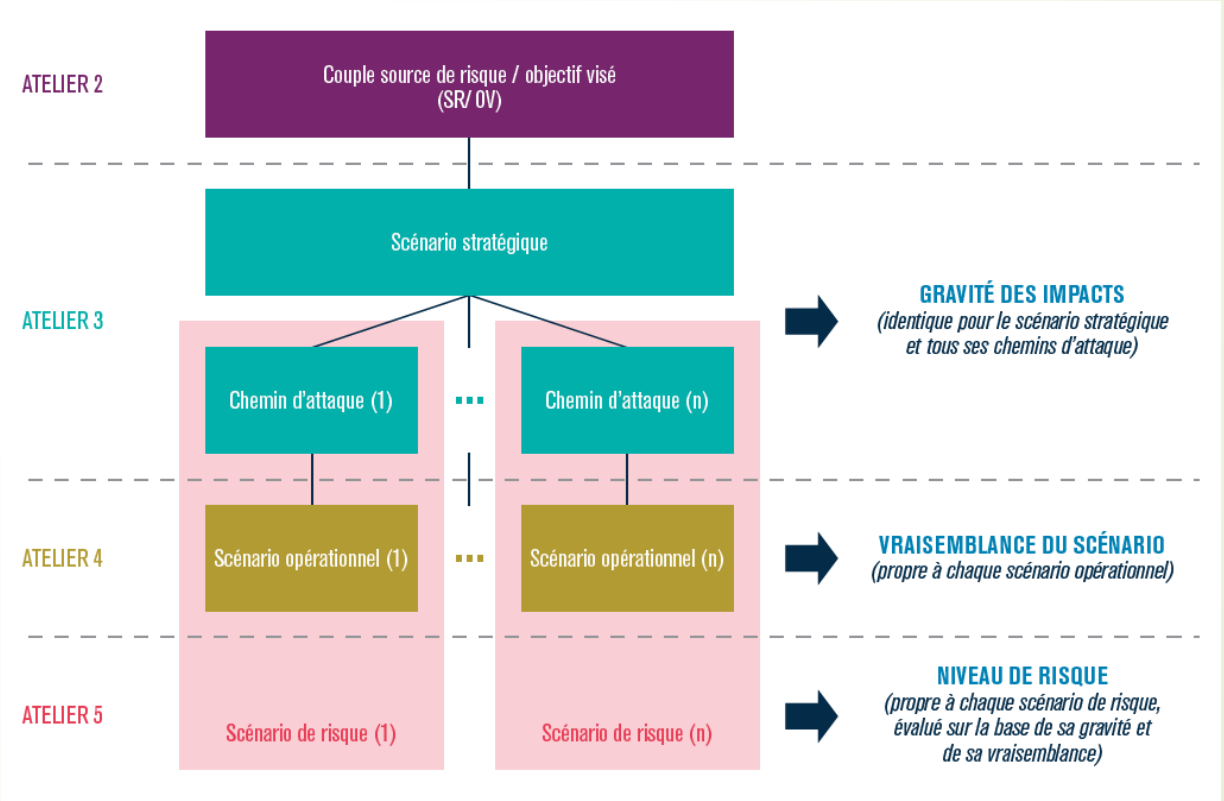
- Scénarios opérationnel et les modes opératoires susceptibles d'être utilisés par les sources de risque pour réaliser les scénarios stratégiques.
- Vraisemblance des modes opératoires





EBIOS RM – Atelier 5

- Synthèse des risques étudies
- Stratégie de traitement du risque
- Mesures de sécurité
- Synthèse des risques résiduels

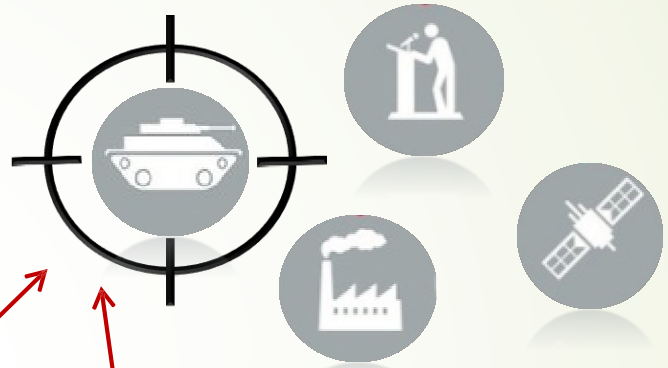


… pour construire des scénarios du point de vue de l'attaquant

Un ou plusieurs attaquants

QUI ?

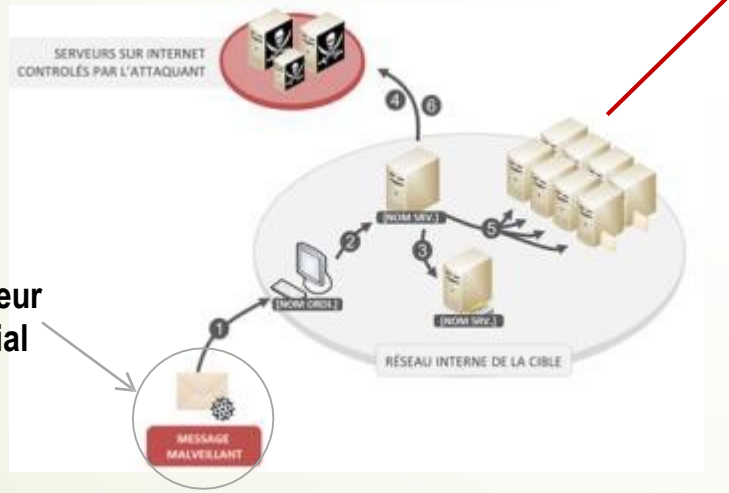
Une cible



COMMENT ?

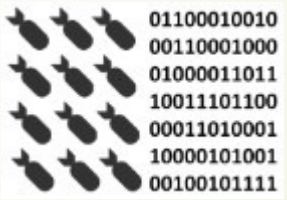
POUR FAIRE QUOI ?

Un chemin d'attaque exploitant généralement plusieurs vecteurs et/ou vulnérabilités



vecteur initial

Une ou plusieurs finalités



EBIOS RM
Cas d'usage

Mettre en place ou renforcer le processus de ***management*** *des risques numériques de mon organisme*

Analyser et traiter les risques numériques sur mes ***projets SI****, dans l'objectif d'une* ***homologation*** *de sécurité*

Définir le niveau de sécurité à atteindre pour un ***produit de sécurité****, selon les cas d'usage envisagés et les menaces à contrer*

Elle s'applique aussi bien aux organisations publiques ou privées, quels que soient leur taille, leur secteur d'activité et que leurs systèmes d'information soient en cours d'élaboration ou déjà existants.

EBIOS RM

Quizz : différents usages d'EBIOS RM

	ATELIERS PRINCIPAUX À CONDUIRE OU EXPLOITER				
OBJECTIF DE L'ÉTUDE	1	2	3	4	5
Identifier le socle de sécurité adapté à l'objet de l'étude	X				
Être en conformité avec les référentiels de sécurité numérique	X				X
Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			X *(note 1)*		
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		X	X		
Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité	X *(note 2)*	X	X		X *(note 3)*
Conduire une étude de risque complète et fine, par exemple sur un produit de sécurité ou en vue de l'homologation d'un système	X	X	X	X	X
Orienter un audit de sécurité et notamment un test d'intrusion			X	X	
Orienter les dispositifs de détection et de réaction, par exemple au niveau d'un centre opérationnel de la sécurité (SOC)			X	X	

4 Gestion de la Sécurité du SI

Gestion de la sécurité du SI

- La Sécurité des Systèmes d'Information doit s'inscrire dans un Plan d'Amélioration Continue de la Sécurité – PACS
  - ✓ Tout l'intérêt de EBIOS RM
  - ✓ De mettre en place un Système de Gestion de la Sécurité des Systèmes de l'Information (SGSSI) ou Système de Management de la Sécurité de l'Information (SMSI).

- La Sécurité de l'Information doit être « l'affaire de tous », elle ne peut être la seule préoccupation d'une équipe de sécurité, par ailleurs souvent réduite. La Sécurité des Systèmes d'Information (SSI) doit être
  - ✓ Transverse
  - ✓ Engageante pour la Direction d'entreprise
  - ✓ Comprise et accepter de tous.

Gestion de la sécurité du SI

- La meilleure réponse à toutes ses contraintes est de mettre en place un Système de Management de la Sécurité de l'Information. Le SMSI
  - ✓ Permet d'engager la Direction
  - ✓ Rend la sécurité du SI cohérente avec la stratégie d'entreprise
  - ✓ S'appuie sur l'approche par les risques
  - ✓ Implique la sensibilisation des parties prenantes
  - ✓ Permet à travers le cycle PDCA (Plan Do Check Act)
    - Le contrôle des mesures de sécurité
    - L'amélioration continue
  - ✓ S'appuie sur un catalogue de mesures, Annexe A ou ISO 27002, qui permet d'adresser les différents domaines d'application de la sécurité du SI.

Gestion de la sécurité du SI

- Historique rapide de l'ISO 27001
  - ✓ 1995 British Standard BS7799
    - Propose 10 mesures clés pour la sécurité du SI
    - 100 mesures détaillées, potentiellement applicables
  - ✓ 1998 Ajout d'une partie 2 BS7799-2
    - Plus courte elle pose les exigences pour mettre en place un système de gestion de la sécurité
    - Voit apparaître la notion de SMSI
    - Un objectif : Apporter un schéma de certification
  - ✓ 2000 : ISO 17799 : 2000
    - Correspond à la BS 7799 partie 1
    - Pas de notion de SMSI
    - Pas de certification possible
  - ✓ 2002 BS7799-2 : 2002
    - Seconde version de la BS 7799-2

Gestion de la sécurité du SI

- Historique (suite)
  - ✓ Juin 2005 ISO 17799 : 2005
    - Nouvelle version de l'ISO 17799 : 2000
  - ✓ Octobre 2005 ISO 27001 : 2005
    - Adoption par l'ISO de la BS 7799-2 : 2002
    - Amélioration de la BS 7799-2
    - Notion de SMSI
    - Possibilité de certification
  - ✓ Juillet 2007 : ISO 27002
    - ISO 17799 devient ISO 27002
    - Rentre dans la terminologie de la série ISO 27000 sans changement
  - ✓ Décembre 2013 ISO 27001 : 2013
    - Impose la cohérence entre la stratégie d'entreprise et le SMSI
  - ✓ 2020 : ISO 27701
    - Complément en lien avec le RGPD sur la protection des données à caractère personnel

Gestion de la sécurité du SI

ISO 27001 : 2013

- Objectif général de la norme
  - Spécifier les exigences pour
    - Mettre en place
    - Exploiter
    - Améliorer
  - Un SMSI documenté

- Spécifier les exigences pour la mise en place de mesures de sécurité
  - En fonction des risques
  - Adaptées aux besoins de l'organisation
  - Adéquates
  - Proportionnées

Gestion de la sécurité du SI

- Modèle PDCA
  - En entrée prendre en compte les attentes des parties prenantes
    - Direction avec la stratégie
    - Partenaires
    - Fournisseurs
    - Clients
    - Pouvoirs publics
    - Services (de l'entreprise)
  - En sortie, disposer d'une sécurité effective inscrite dans un Plan d'Amélioration de la Sécurité livrée pour les mêmes parties prenantes

Gestion de la sécurité du SI

- Phase Plan
  - ✓ Cadrer le SMSI
    - Note de cadrage en lien avec la stratégie de certification (pourquoi je me fais certifier)
    - Disposer d'un BMC (Business Model Canevas) et d'un BSC (Balance Score Card)
    - Poser la PGSI (Politique de Gouvernance du SI) avec le périmètre du SMSI clairement défini
    - Fournir la Politique de sécurité PSI
    - Plan de gestion des risques
      - Méthodologie d'appréciation des risques
      - Identification et évaluation des risques
      - Traitement des risques
    - Objectifs de sécurité et mesures de sécurité
    - Programmer organiser la gouvernance CPS et CPO (Comités de Pilotage Stratégiques et Opérationnels)
  - ✓ Les Objectifs de sécurité et mesures de sécurité sont listés dans une matrice de Déclaration d'Applicabilité ou DDA (Statement of Applicabilité ou SOA)
    - Lister les mesures de sécurité
    - Justifier les exclusions sur les mesures de sécurité

Gestion de la sécurité du SI

- Phase DO
  - ✓ Allocation et gestion des ressources
    - Personnes, temps, argent
  - ✓ Formation du personnel concerné
  - ✓ Gestion des risques
    - Pour les risques à réduire :
      - Implémenter les mesures de sécurité identifiées dans la phase précédente
      - Assignation des responsabilités
      - Identifier des risques résiduels
    - Pour les risques transférés : assurance, sous-traitance, etc.
    - Pour les risques acceptés et refusés : rien faire ou presque ☺
  - ✓ Tenir les comités de pilotage
    - Stratégiques CPS
    - Opérationnels CPO

Gestion de la sécurité du SI

- Phase Check
  - ✓ Vérification de routine ou contrôle permanent
  - ✓ Apprendre des autres (veille)
  - ✓ Audit du SMSI
    - Audits réguliers
    - Sur la base de
      - Documents, politiques, procédures
      - Traces et enregistrements
      - Tests techniques
  - ✓ Conduit à
    - Constatations que les mesures de sécurité ne réduisent pas de façon effective les risques pour lesquels elles ont été mises en place
    - Identification de nouveaux risques non traités
    - Tout autre type d'inadaptation de ce qui est mis en place

Gestion de la sécurité du SI

- Phase Act
  - ✓ Prendre les mesures résultant des constatations faites lors de la phase de vérification
  - ✓ Actions possibles
    - Passage à la phase de planification
      - Si de nouveaux risques sont identifiés
    - Passage à la phase d'action
      - Si la phase de vérification en montre le besoin
    - Si constatation de non conformité
      - Actions correctives ou préventives
        - Actions entreprises immédiatement
        - Planification d'actions sur le moyen et long terme

Gestion de la sécurité du SI

- La norme ISO 27002
  - Parallèle avec l'Annexe A de la norme ISO 27001
  - Chapitres 5 à 18 qui présentent les domaines des différentes mesures
  - Représente l'ensemble des mesures de sécurité pouvant être appliquées
  - Recommandations ou exigences de sécurité
  - Reprennent les recommandations classiques des experts en sécurité
    - Certaines mesures de sécurité sont très générales, d'autres très précises
    - Certaines mesures de sécurité sont applicables à tout l'organismes, d'autres à un serveur ou à une application particulière
    - Donnent des recommandations parfois très larges pouvant inclure d'autres mesures de sécurité
  - Sélectionnées pour réduire un risque à un niveau acceptable à l'issue d'une appréciation des risques
- La version 2022 apporte entre autres les mesures de sécurité liées au Cloud
  - Passe de 114 mesures à 93 mesures suivant 4 chapitres
    - L'organisation
    - Les personnes
    - Le Physique
    - Le technologique
  - Chaque mesure se mesure sur 5 attributs liés aux fonctions de sécurité

Gestion de la sécurité du SI

- Exemple d'utilisation sur un actif
  - ✓ Appréciation des risques en amont
    - Identification de l'actif : serveur sensible
    - Vulnérabilité : serveur dépendant de l'électricité
    - Menace : Défaillance technique, défaut d'alimentation
    - Risque : Perte de disponibilité et d'intégrité sur le serveur
    - Niveau de risque important qui nécessite un traitement
  - ✓ Traitement sélectionné : Réduction du risque
  - ✓ Choix de la mesure de sécurité (ISO 27002)
    - Article 11 Sécurité physique et environnementale
    - Objectif de sécurité : 11.2 – Sécurité du matériel
    - Mesure de sécurité : 11.2.2. Services généraux
      - Il convient de protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux.
      - Il convient que tous les services généraux, tels que l'électricité… soient correctement dimensionnés pour les systèmes pris en charge.

Gestion de la sécurité du SI

- ISO 27002 - Article 5 - Politique de sécurité
  - ✓ Document qui doit fixer
    - Cadre d'application de la sécurité de l'information
    - Objectifs (conformité)
    - Approche de gestion du risque
    - Vue globale des politiques sectorielles
    - Responsabilités en termes de sécurité
    - Applicable et communiqué à tous
  - ✓ Doit être réexaminé pour l'amélioration
    - De l'approche de gestion de la sécurité de l'information
    - Des mesures et objectifs de sécurité
    - De la gestion des ressources et responsabilités
    - De la qualité du document

Gestion de la sécurité du SI

- ISO 27002 - Article 6 – Organisation de la sécurité de l'information
  - ✓ Engagement de la direction vis à vis de la sécurité de l'information
    - Soutien de la PSI
    - Définition des responsabilités et tâches associées
    - Mise à disposition des ressources appropriées
  - ✓ Coordination de la sécurité de l'information
    - Encadrement des démarches en sécurité
    - Suivi et contrôle
    - Communication sur l'importance de la sécurité
  - ✓ Attribution des responsabilités en matière de sécurité de l'information
    - Formalisation des responsabilités

Gestion de la sécurité du SI

- ISO 27002 - Article 6 – Organisation de la sécurité de l'information
  - ✓ Organisation interne
    - Système d'autorisation concernant les moyens de traitement de l'information
      - Responsabilité de la direction: autorisation et vérification de compatibilité
      - Désigner le RSSI
    - Engagement de confidentialité
      - Conformité à la législation
      - Prise en compte des informations à protéger
      - Dispositions à prendre pour protéger l'information
      - Revues régulières
    - Relation avec les autorités
      - Maintien d'une liste à jour
      - Gestion des incidents à communiquer (identification, canal de communication)
    - Relation avec des groupes de spécialistes
      - Associations de professionnels (RSSI, club ISO 27001), Forum de discussions, etc.
    - Revue indépendante de la sécurité de l'information
    - Relation avec les tiers
      - Inclure les tiers dans l'appréciation des risques
      - Prendre en compte la sécurité des clients
      - Inclure la sécurité dans les accords conclu avec les tiers

Gestion de la sécurité du SI

- ISO 27002 - Article 7 – Sécurité des ressources humaines
  - ✓ Avant le recrutement
    - Définir les rôles et responsabilités
    - Sélection du ou des candidats
    - Conditions d'embauche
  - ✓ Pendant la durée du contrat
    - Responsabilités de la Direction
    - Sensibilisation , qualification et formations en matière de sécurité de l'information
    - Processus disciplinaire
  - ✓ Fin ou modification du contrat
    - Les responsabilités en fin de contrat
    - La restitution des biens
    - Le retrait des droits d'accès

Gestion de la sécurité du SI

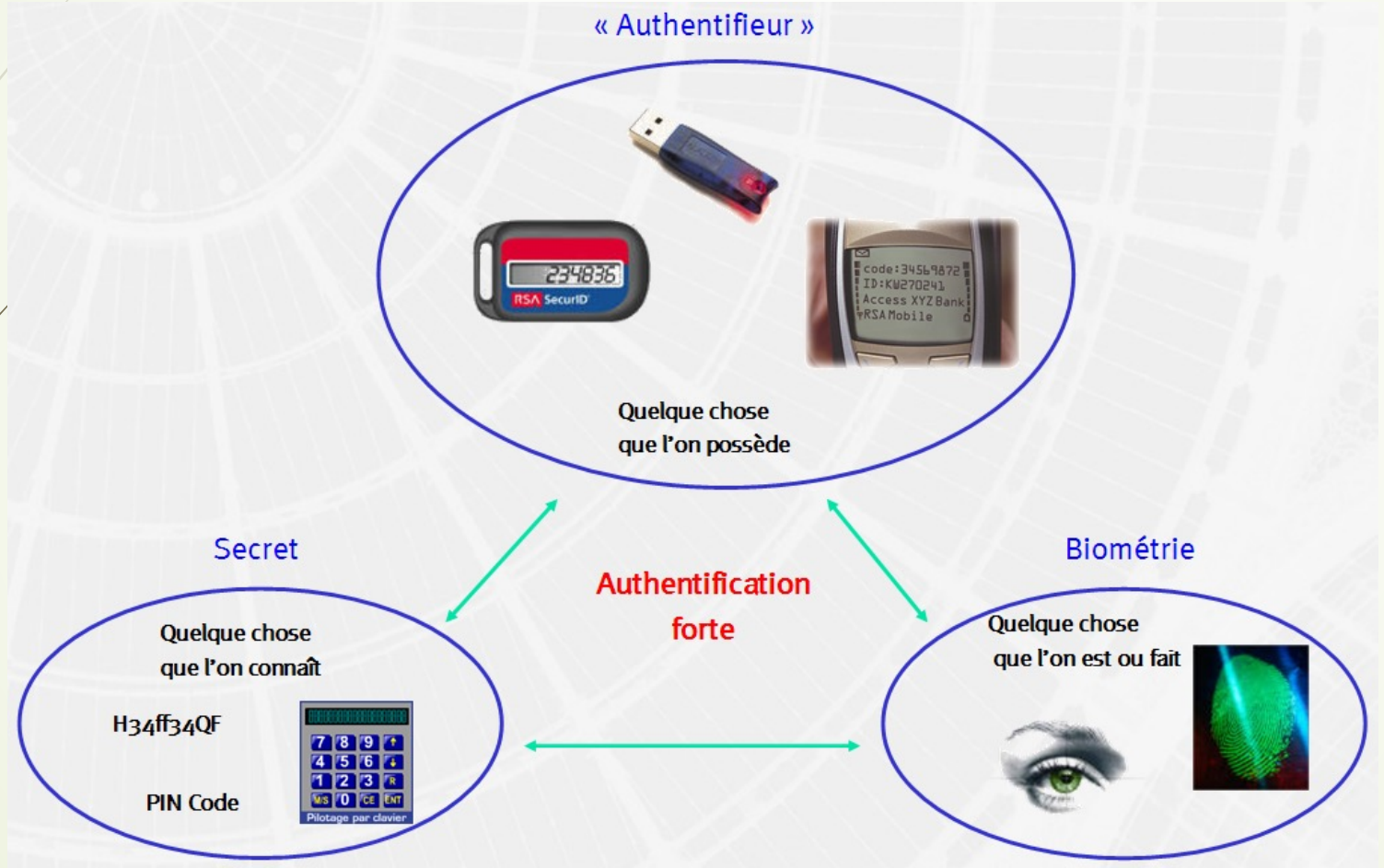
- ISO 27002 - Article 8 – Gestion des actifs
  - ✓ Responsabilités relatives aux actifs
    - Identifier les actifs importants
    - Identifier les propriétaires des actifs
    - Consigner les informations essentielles à la gestion
  - ✓ Classification des informations
    - Critères : valeur, exigences légales, sensibilité et criticité
    - Fournie par le propriétaire
    - Prend en compte les contraintes business
    - Exprimée en termes de DIC et/ou catégories
    - Inclut la gestion du marquage et de la manipulation des actifs
  - ✓ Manipulation des supports
    - Gestion des supports amovibles
    - Destruction recyclage des supports
    - Protection des supports pendant leur transfert

Gestion de la sécurité du SI

- ISO 27002 - Article 9 – Contrôle d'accès
  - ✓ Exigences relatives au contrôle d'accès
    - Politique de contrôle d'accès (PSI ou sectorielle)
    - Accès aux réseaux et services (demande d'attribution des ouvertures d'accès fonction du besoin d'en connaître) - matrice
  - ✓ Gestion de l'accès des utilisateurs
    - Contrôler les accès autorisés et empêcher les accès non autorisés
    - Enregistrement et désinscription des utilisateurs
      - Mesure organisationnelle
      - Procédures pour les ouvertures et fermetures des comptes des utilisateurs
        - Systèmes multi-utilisateurs, domaines Windows, annuaire, applications
      - Besoin d'une approbation de la direction
        - Se conformer à la politique et à la notion de séparation des tâches
      - Signature d'une charte spécifique pour l'accès
      - Buts : pas de redondance, d'accès inutiles, de comptes de groupes (mauvais pour la traçabilité)
      - Désactivation (ou désinscription) importante – la procédure doit inclure ce point, à faire immédiatement
      - Fréquent d'avoir des users qui n'ont pas utilisé leur compte depuis longtemps (accès toujours existants, pwd ancien ou connu, propriétaire plus sous contrat, comptes temporaires)
      - Gestion des accès à privilège (restreints et contrôlés)
      - Gestion des informations secrètes d'authentification des utilisateurs
      - Revues des droits d'accès des utilisateurs, périodique (6 mois)
      - Suppression ou adaptation des droits d'accès toujours en fonction du besoin d'en connaître

Gestion de la sécurité du SI

- ISO 27002 - Article 9 – Contrôle d'accès (suite)



Gestion de la sécurité du SI

- ISO 27002 - Article 9 – Contrôle d'accès (suite)
  - ✓ Responsabilité des utilisateurs
    - Réduire les risques liés aux utilisateurs
    - Concerne l'utilisation de mot de passe (mot de passe fort) , MFA
    - Le matériel utilisateur laissé sans surveillance
    - Le bureau propre (politique de bureau propre physique et logique)
  - ✓ Contrôle de l'accès au SI
    - L'accès au système et aux fonctions d'application doit être restreint (moindre privilège)
    - Procédure de connexion sécurisée notamment depuis l'externe (TLT)
    - Système de gestion de mot de passe interactif (SSO)
    - Gestion des sessions (ouverture de sessions sécurisées, identification et authentification des users, déconnexions automatique des sessions)
    - L'utilisation des systèmes permettant de contourner les mesures doit être strictement limité et contrôlé
    - Protection des ports de diagnostic et de configuration à distance (ports de télémaintenance)
    - Cloisonnement des réseaux (problématique des réseaux partagés)
    - Contrôle des connexions et du routage réseau
    - Contrôler et restreindre l'accès aux codes sources

Gestion de la sécurité du SI

- ISO 27002 - Article 10 – Cryptographie
  - ✓ Mettre en place une politique d'utilisation des mesures cryptographie (sectorielle)
  - ✓ Gestion des clés Politique sur l'utilisation, la gestion la protection des clés tout au long de leur cycle de vie,
    - symétrique ou asymétrique
    - Attention à la durée de vie des certificats, politique de gestion des certificats
      - Révocation
      - Renouvellement
      - Publication

Gestion de la sécurité du SI

- ISO 27002 - Article 11 – Sécurité Physique et environnementale
  - ✓ Protection du personnel et des actifs matériels
  - ✓ S'articule sur deux axes
    - Zones sécurisées
      - Protection périmétrique
      - Contrôle d'accès
      - Protection contre les événements environnementaux
    - Sécurité du matériel
      - Placer le matériel dans une zone non exposée
      - Disponibilité de l'alimentation (ASI)
      - Mise au rebut et réutilisation
        - Politique de recyclage destruction
        - Enregistrement traçabilités
      - Inventaire et prévention des vols

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation
  - ✓ Procédures et responsabilités liées à l'exploitation
    - Procédures
      - Couvrent l'ensemble des opérations
      - Définissent les responsabilités et assurent la séparation des tâches
      - Formalisées, tenues à jours, auditables
    - Management des modifications, gestion des changements
      - Procédure de changement formalisée
      - Réduire les risques liés aux changements
      - Processus transversal
    - Bien gérer les dimensionnements futurs, gestion de la performance
    - Gestion des environnements,
      - Séparation des environnements de dev, test, pre-prod, prod

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation (suite)
  - ✓ Protection contre les logiciels malveillants
    - Politique et procédures mises en place
    - Lutte anti-virale et anti-spyware
    - Couvre la détection, la prévention et le recouvrement
    - Poste de travail tout environnement
    - Serveurs tout environnement
    - Toute application (messagerie, notamment)
    - Vérifier la compatibilité de la solution avec les différents environnements
    - Configuration
      - Modes de protection : permanente, scan ponctuel ou récurrent
      - Exclusions à gérer
      - Contrôle d'accès aux paramètres d'administration
      - Contrôle des mises à jours
      - journalisation
    - Critiques car en constante évolution et tend à être transverse (patch management, etc.)
    - Remonter des logs sur les SIEM, penser au solutions EDR et DLP

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation (suite)
  - ✓ Sauvegardes
    - Concerne aussi bien les informations que les logiciels
    - Nécessite des tests réguliers: sauvegarde, restauration
    - Protéger les flux de sauvegarde
    - S'assurer de la protection des sauvegardes externalisées
    - Etre cohérent dans la gestion des procédures de sauvegarde

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation (suite)
  - ✓ Journalisation et surveillance
    - Journaux d'événement enregistrant l'activité des utilisateurs (remontée vers les SIEM)
      - Créer les règles de journalisation qui? Ou? Quand ? Quoi? Qui a fait quoi ? Quoi a fait quoi ?)
      - Les revoir fréquemment ou à échéances régulières
    - Protéger les moyens et enregistrement liés à la journalisation traçabilité
      - Contre toute suppression, modification
      - Conservation protégée pour investigation
      - Fixer les règles de conservation (durée : protection : cadre réglementaire) doivent généralement être légers
      - Penser la journalisation au début des projet
      - Produire des journaux
        - Systèmes
        - Applicatifs (attention à la charge des logiciels BdD Oracle accouting)
        - Journaux des applications (ex log de serveur web)
        - Les envoyer vers une machine d'archive
    - La gestion des horloges est capitales sur ces sujets ☺

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation (suite)
  - ✓ Que journaliser
    - Ex dans le cas du Contrôle d'accès
      - Identification de l'utilisateur
      - Horodatage du début et de la fin
      - Le terminal
      - Accès rejeté ou accepté
      - Éventuellement l'utilisation de privilèges, d'actions
  - ✓ Maîtrise des logiciels à installer
    - Procédure de validation avant l'installation des logiciels
      - Contexte
      - Besoin (peut être déjà un outil qui répond au besoin)
      - Libre ou propriétaire
      - Impacts, notamment sur le patch management ensuite

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation (suite)
  - ✓ Gestion des vulnérabilités techniques
    - Patch management à mettre en place
    - Implique de connaître les actifs
    - Mettre en place une veille via le soc sur des CERT en lien avec les CVE
    - Mettre en place des revues périodique sous forme de scan de vulnérabilité
    - Le patch management devient de plus en plus critique en entreprise
      - Parfois pas possible de tout patcher, impact for sur la prod
      - Implique de connaître les risques résiduels
  - ✓ Maîtriser la relation avec les tiers
    - S'assurer de la mise en place
      - des exigences de sécurité
      - Des définitions de services
      - Des niveaux de prestation
    - Procédure de surveillance et de réexamen
    - Gestion des modifications

Gestion de la sécurité du SI

- ISO 27002 - Article 12 – Sécurité liée à l'exploitation (suite)
  - ✓ Manipulation des supports
    - Gestion des supports amovibles
    - Mise au rebut des supports (recyclage destruction)
    - Procédure de manipulation des informations sur les supports
    - Gérer et sécuriser le supports physique en transit (externalisation physique de sauvegarde)

Gestion de la sécurité du SI

- ISO 27002 - Article 13 – Sécurité des communications
  - ✓ Gérer et contrôler les réseaux pour protéger l'information
    - Poser les règles sur la gestion des flux , entrée/sortie/transit
      - Fw
      - Ids
      - Ips
    - Séparation des tâches sur la fermeture de flux
    - Cloisonner les réseaux
    - Dimensionner correctement les réseaux
  - ✓ Transfert de l'information
    - Mettre en place les politiques et procédures de transfert d'information
    - Mettre en place des passerelles mails avec des règles de surveillance
    - Protéger l'information transitant par la messagerie électronique
    - Pour les transactions en lignes, s'assurer du CID de l'information
    - Mettre en place des engagements de confidentialité avant tout transfert
    - Inclure la messagerie dans le charte informatique

Gestion de la sécurité du SI

- ISO 27002 - Article 14 – Acquisition développement et maintenance des systèmes
  - ✓ La sécurité du SI et en particulier de l'information doit être intégrée nativement tout au long du cycle de vie du projet
  - ✓ Les exigences de sécurité doivent être intégrées dès le début (DA, DAT)
    - Prévention des pertes en CID de l'information
  - ✓ Le bon fonctionnement des applications doit intégrer la sécurité
    - Qualité du développement mais aussi sécurité du développement
    - Vérification des données en entrée et en sortie
      - Prévenir les injections de codes
      - Éviter les erreurs grotesque comme des pwd codés en durs
      - Prévenir les débordement de tampon, de piles ou de tas
      - Se protéger contre un fonctionnement non déterminé
        - Deni de service
        - Comportement erratique
        - Erreurs
      - Les données en sortie doivent être conformes au résultat attendu
        - Exemple typique des applications web : exécution croisée de code (cross site scripting ou XSS)
        - Un attaquant arrive à injecter du code javascript dans une page web qui sera renvoyé à la victime à partir d'un formulaire, dans un lien, etc.
    - S'assurer de l'authenticité et de l'intégrité des messages
      - Information bien du type attendu

Gestion de la sécurité du SI

- ISO 27002 - Article 14 – Acquisition développement et maintenance des systèmes (suite)
  - ✓ Sécurité en matière de développement et d'assistance technique
    - S'assurer de la sécurité des applications – test ou pentests récurrents, ans tous les cas avant la MEP
    - Gestion des modifications
      - Définir les procédures de contrôle
      - Effectuer des réexamens techniques après modification
      - Restrictions relatives à la modification des progiciels
    - Prévention des fuites d'information
      - Canaux cachés dans un canal autorisé (ex IP dans DNS) , cheval de Troie qui crée un canal caché
    - Gestion des sous-traitants pour l'externalisation du développement du logiciel en tout ou partie
    - Les environnements de développements doivent être sécurisés

Gestion de la sécurité du SI

- ISO 27002 - Article 14 – Acquisition développement et maintenance des systèmes (suite)
  - ✓ Gestion des vulnérabilités techniques
    - Rejoint le patch management et la veille du SOC
    - Mesures relatives aux vulnérabilités techniques
    - Evaluation des vulnérabilités affectant les actifs en support des développement
      - Estimation du risque induit en fonction du contexte
    - Choix et mise en place de mesures adaptées
  - ✓ Sécurité de la donnée
    - Données de test différentes des données en prod
    - Données de test doivent être tout autant protégées
    - Intégrer nativement les problématiques liées
      - Aux données de santé
      - Au RGDP plus globalement

Gestion de la sécurité du SI

- ISO 27002 - Article 15 – Relation avec les fournisseurs
  - ✓ Mettre en place une politique de sécurité dans les relations avec les fournisseurs
    - Les exigences de sécurité doivent être clairement définies et contrôlables
      - Accéder
      - Traiter
      - Stocker
      - Communiquer
      - Fournir
      - … des composants ou services, etc.
    - Préciser les exigences sur le traitement des risques liés à leur activité
  - ✓ Gestion de la prestation de service
    - Surveiller, contrôler et auditer à intervalle régulier la prestation de service fournie
  - ✓ La gestion des changements doit être intégrée dans la relation avec les fournisseurs
  - ✓ Les exigences qui s'appliquent doivent être imposées dans la relation avec les fournisseurs

Gestion de la sécurité du SI

- ISO 27002 - Article 16 – Gestion des incidents liés à la sécurité de l'Information
  - ✓ Politiques et procédures doivent être rédigées et établir les responsabilité en termes de gestion des incidents
    - Les procédures doivent permettre l'identification, la qualification, la collecte
    - Les informations collectées et pouvant servir de preuves doivent être protégées
  - ✓ Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais
    - Sur les failles de sécurité et faiblesses découvertes
    - Survenance d'un incident probable, quasi certain, certain
    - Vers les personnes concernées
  - ✓ Le traitement et la remédiation des incidents doivent permettre
    - D'alimenter une base de connaissance
    - Intégrer la remédiation immédiate
    - L'identification de la cause racine
    - Mesurer l'efficacité du traitement de l'incident et de al contre mesure
  - ✓ Les collaborateurs doivent être informés sur l'obligation de signaler un incident de sécurité ou un comportement anormal

Gestion de la sécurité du SI

- ISO 27002 - Article 17 – Sécurité de l'information dans la Continuité d'Activité
  - ✓ Une politique de continuité de l'information doit être établie
    - Fixer es exigences en matière de CA et de continuité du management de la sécurité du SI
    - Disposer de processus, procédures permettant de disposer du niveau de sécurité nécessaire en cas de crise
      - Prise en compte des menaces qui peuvent causer des interruptions de services dans l'appréciation des risques
      - Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité d'activité
    - Dans l'idéal mettre en place un SMCA
  - ✓ Redondance
    - Mettre en place les moyens nécessaires permettant d'assurer la continuité de l'information et de sa sécurité
  - ✓ Mettre en place des tests récurrents

Gestion de la sécurité du SI

- ISO 27002 - Article 18 – Conformité
  - ✓ S'articuler autour des exigences réglementaires et légales
    - Texte de lois (RGPD)
    - Les directives (PPST, ICPE, etc.)
    - Les normes (ISO 27001, HDS, etc.)
  - ✓ Formaliser un procédure de gestion des exigences
    - Nécessite de les lister
      - Connaître
      - Mettre à jour
  - ✓ Indépendance des revues de la sécurité de l'information

MERCI