Gestion de projet IT

ynov CAMPUS

1-IceBreaker : **PRÉSENTATION CROISÉE SUPER-POUVOIR**

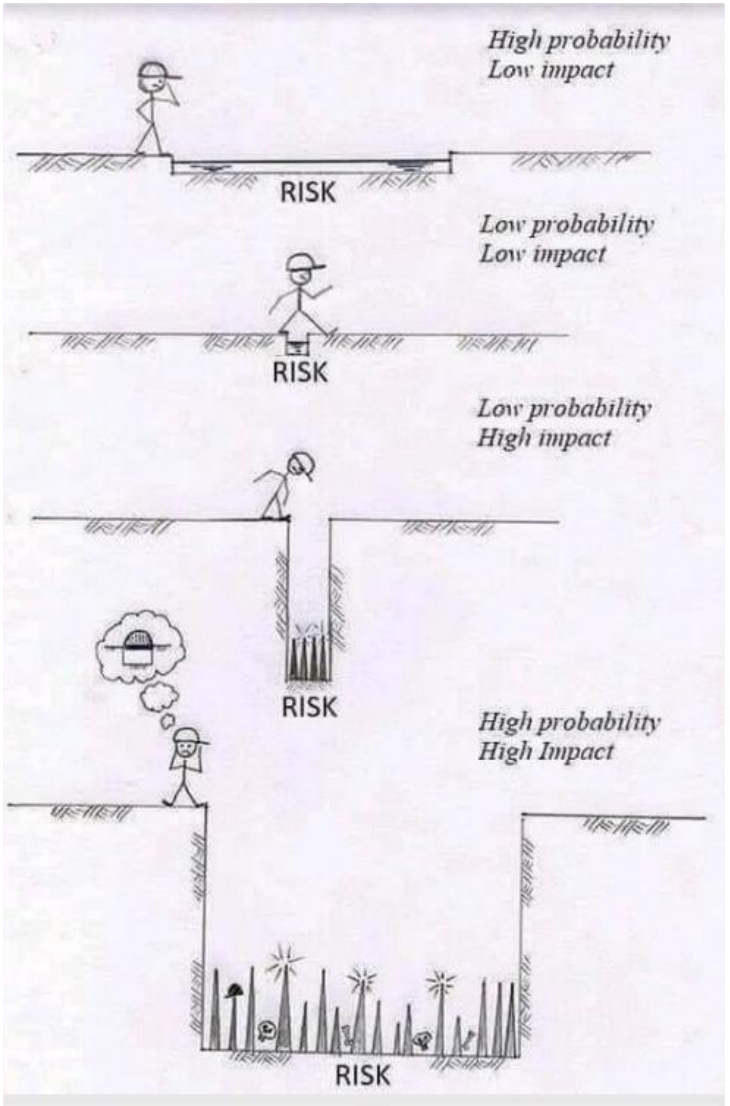
1-Définissez votre super héros en contexte professionnel.

2-Par binôme: présentation croisée dans vos groupe de 6.

- 🦸 **Nom de Super-héro(ïne)** : « *C'est le nom héroïque qui vous caractériserait le mieux en tant que super-héros* »
- 💪 **Super-pouvoir** : « *C'est la force, le talent ou l'aptitude dans laquelle vous excellez et dont vous êtes fier(e)* »
- ⚠️ **Kryptonite** : « *C'est l'élément que vous craignez le plus, qui vous insupporte ou qui vous fait perdre tous vos pouvoirs* »

3-Gestion des risques

Le risque ?
-Une probabilité
-Un impact



Actif

Tout élément (matériel ou immatériel) représentant de la valeur pour l'organisme

Primaires (Exemples: Processus, données, …)

Support (Exemples : Application, Infrastructure, Couche physique…)

Evènement redouté

« Peur » qu'un actif primaire « perde » un ou plusieurs **« besoins de sécurité »**

Qu'est ce qui vous empêche de dormir ?

Besoin de sécurité Expression d'une exigence de sécurité face aux risques identifiés

Exemples : Disponibilité, Intégrité, Confidentialité, Traçabilité/Preuve

Impacts, conséquences

Conséquence de l'évènement redouté

Exemples : impact financier, d'image, légal, etc

Menace

Cause potentielle d'un incident indésirable, qui peut engendrer des dommages à un actif.

- Evènements générateurs (Ex: Catastrophes naturelles)
- Effets de cause (Ex: Saturations de réseaux)
- Evènements qui rendent possible la dégradation (Ex: Défaut de sensibilisation)
- Comportements (Ex: Laxisme)

Environnementales
Accidentelles
Malveillantes

Vulnérabilité

Caractéristique d'un actif ou faiblesse d'un besoin de sécurité qui peut être exploitée par une menace

Exemples : faille logicielle, mauvaise configuration, zone inondable…

Concrètement

Menace

Evènement redouté
Perte intégrité tour

Vulnérabilité

Le toit ne peut pas supporter la menace

Actif primaire
Le toit

Actif support

Tous les matériaux qui composent la tour (béton, charpente, structure,…)

Impact
Des blessés si des personnes sont présentes

Besoin de sécurité
Le toit doit supporter une charge de plus de 900 tonnes…

Risques IT: aligner le besoin métier avec le niveau de sécurité, pas plus pas moins, au « juste prix »

Trouver les bons acteurs

- Un risque «est créé» par le service ou le produit mis à disposition des clients par l'entreprise
- Très souvent, ce service/produit est sponsorisé par la direction
- La menace «est créée» dès lors qu'un «bien essentiel» supporte le service ou le produit

Risque défini par l'ensemble [Actif; Menace;(Vulnérabilité)]

Actif: représentant de la valeur. ***Ex: Impressions papier***

Menace: Susceptible de causer un dommage à l'actif. ***Ex: Vol de documents***

Vulnérabilité: rend possible l'évènement. ***Ex: Employés non sensibilisés, Tiers présent dans les locaux sans badge***

Risque de fuite d'information

RISQUE = Impact * Vraisemblance

Principes de gestion

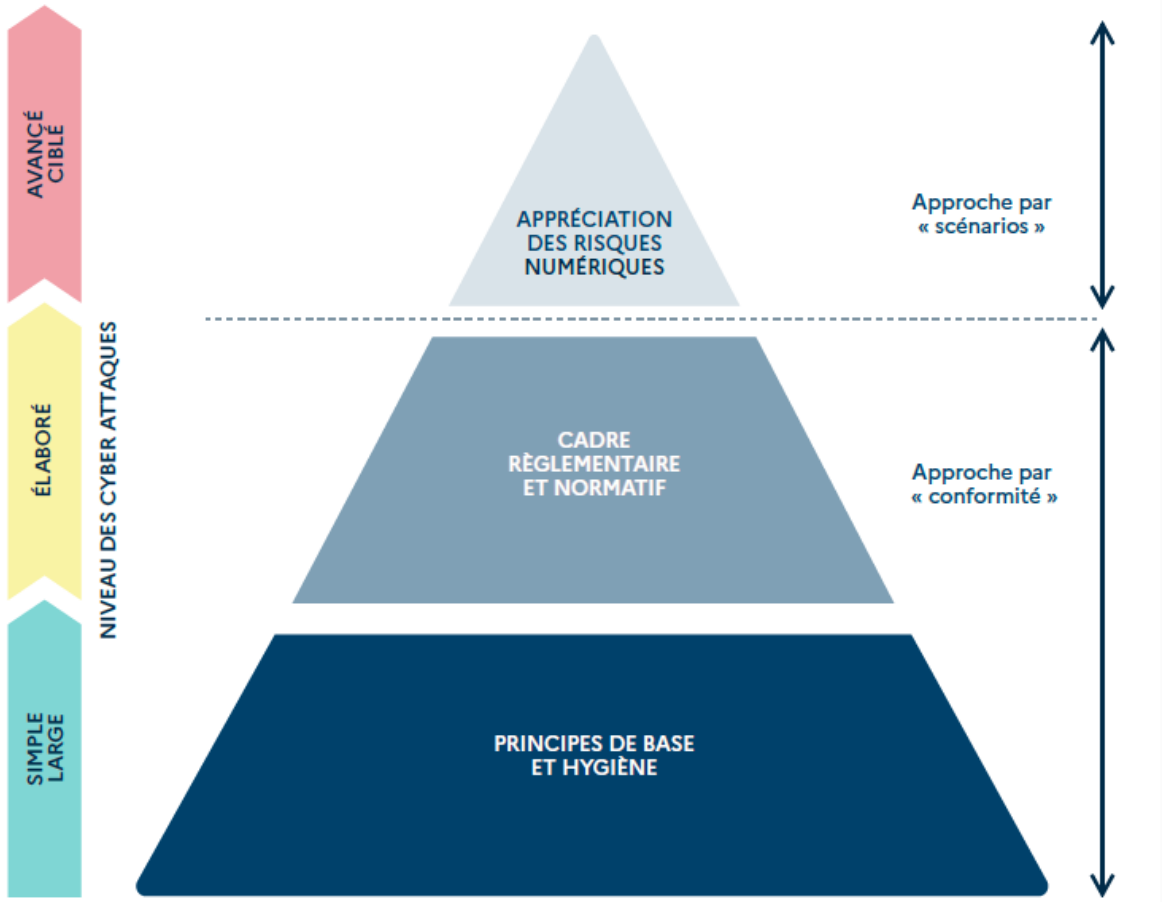


Figure 1 — Pyramide du management du risque numérique

Impacts

N°	Niveau de gravité	Description	Quelques exemples concrets
1	Négligeable	Les personnes concernées ne seront pas impactées ou pourraient connaitre quelques désagréments qu'elles surmonteront sans difficulté	Maux de tête passagers Réception de SPAMS Sentiment d'atteinte à la vie privée
2	Limitée	Les personnes concernées pourraient connaitre des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	Refus d'un service administratif ou commercial (ex : refus de prêt bancaire) Publicité ciblée sur un aspect que la personne souhaiterait garder confidentiel (ex : traitement pharmaceutique…)
3	Importante	Les personnes concernées pourraient connaitre des conséquences significatives, qu'elles devraient pouvoir surmonter mais avec des difficultés réelles et significatives	Chantage Interdiction bancaire Blessure physique Divorce Phishing
4	Maximale	Les personnes concernées pourraient connaitre des conséquences significatives, voire irrémédiables, qu'elles ne pourraient pas surmonter	Décès Sanction pénale Perte de preuve dans le cadre d'un contentieux

Non respect règlement interne
Mention négtive en interne
Arrêt partiel d'un service
Perte <10k€

Sanction internes
Mention négative externe limitée
Arrêt total d'une direction
Entre 10 et 100k€ de perte

Responsabilité civile
Mention négative externe presse spécialisée, atteinte réputation
Arrêt total de 2 ou 3 directions
Entre 100 et 500k€ de perte

Responsabilité pénale
Mention négative externe presse grand public, atteinte réputation importante
Arrêt total des activités
Plus de 500k€ de perte

Vraisemblance

N°	Niveau de gravité	Description
1	Négligeable	Il ne semble pas possible que les sources de risques retenues puissent réaliser la menace en s'appuyant sur les caractéristiques des supports
2	Limitée	Il semble difficile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports
3	Importante	Il semble possible pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports
4	Maximale	Il semble extrêmement facile pour les sources de risques retenues de réaliser la menace en s'appuyant sur les caractéristiques des supports

Expert ayant de très bonne connaissance, moyens importants

Solide compétences avec moyens spécifiques (outils web, exploitation vulnérabilité, injections SQL, procédure complexe)

Niveau élémentaire informatique (changement configuration poste de travail, désactivation de services, commandes SQL, installation ou désinstallation de logiciels)

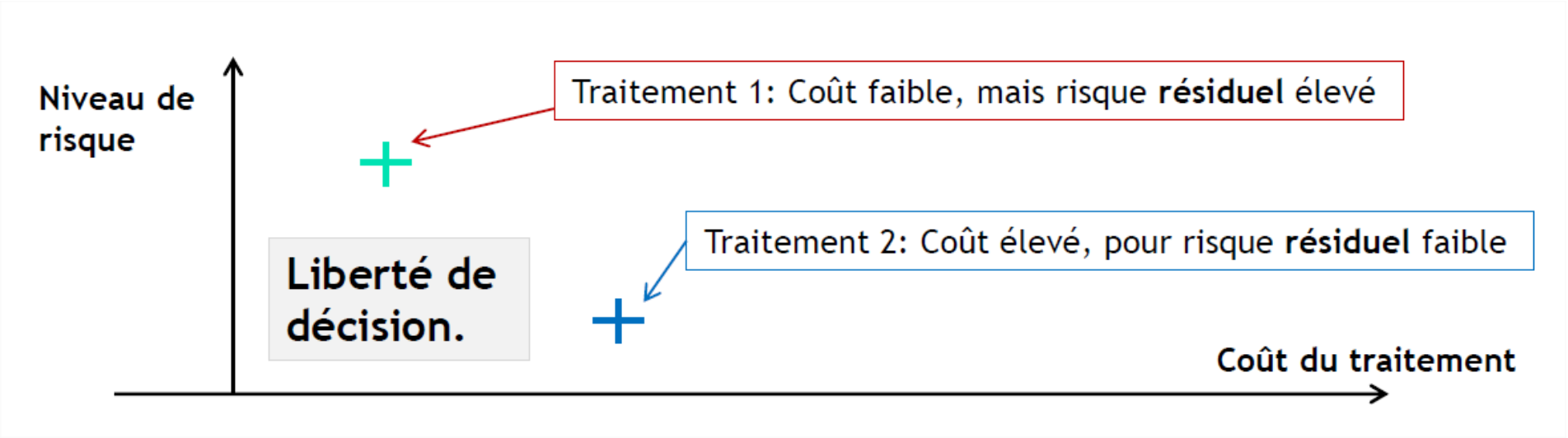
Tout public (accès dossier réseau, page web, ouverture de document, envoi de mail, document papier)

Risque

		Vraisemblance			
		1	2	3	4
Impact	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

	Risque à réduire de manière systématique
	Mode de traitement du risque à réduire
	Risque accepté de manière systématique

Traitement du risque



-Risque réel ?
-Coût et délai des solutions ?
-Culture de gestion du risque ?
-Critères d'acceptation du risque ?
-Risques secondaires induits par le traitement ?
- »Ce n'est pas mon risque » => Transversalité

1 – Gestion directe et individualisée des risques

-Risque de surchauffe de la salle informatique
=>Installation d'une climatisation

-Risque de vol de matériel informatique
=>Installation de badge d'accès aux portes

2 – Gestion globale et indirecte des risques

-Risque de surchauffe de la salle informatique
=>Mise en ouvre d'une procédure d'usage, d'acquisition et de maintenance

-Risque de vol de matériel informatique
=>Mise en œuvre d'une charte informatique

Méthodes pour gérer les risques IT

La méthode **EBIOS** Risk Manager (EBIOS RM) a été mise à jour en 2018, et **l'ISO 27005** en novembre 2022. Ces mises à jour sont majeures, et recentrent la gestion des risques autour des métiers, de la cybersécurité et de la protection de la vie privée

MEHARI
Méthode Harmonisée pour l'Analyse de Risques
Méthode publiée par le CLUSIF (France)
Version actuelle: MEHARI 2010

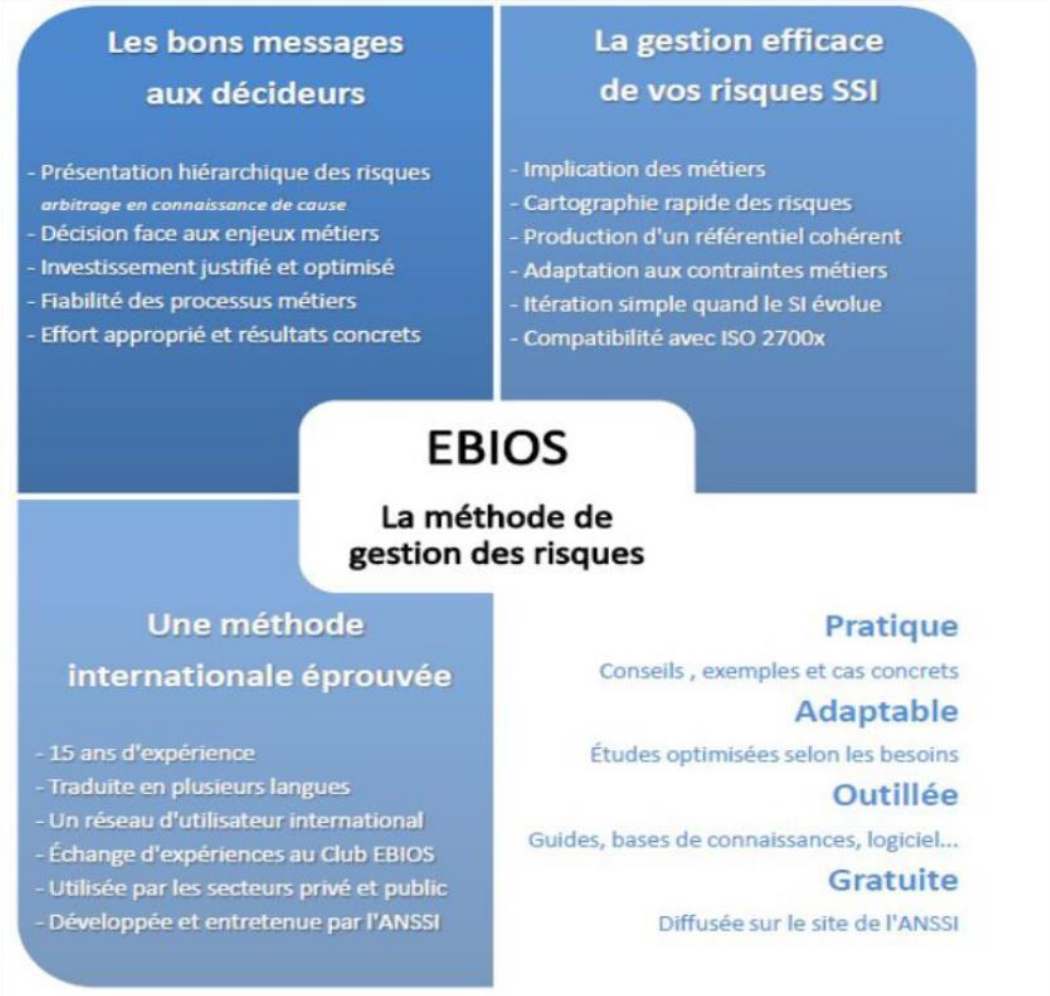
OCTAVE
Operationnally Critical Threat, Asset and Vulnerability Evaluation
Réalisée par l'université Carnegie Mellon (USA)
3 versions: OCTAVE, OCTAVE-S et OCTAVE Allegro

EBIOS RM (2018)

Expression de **B**esoins et **I**dentification des **O**bjectifs de **S**écurité

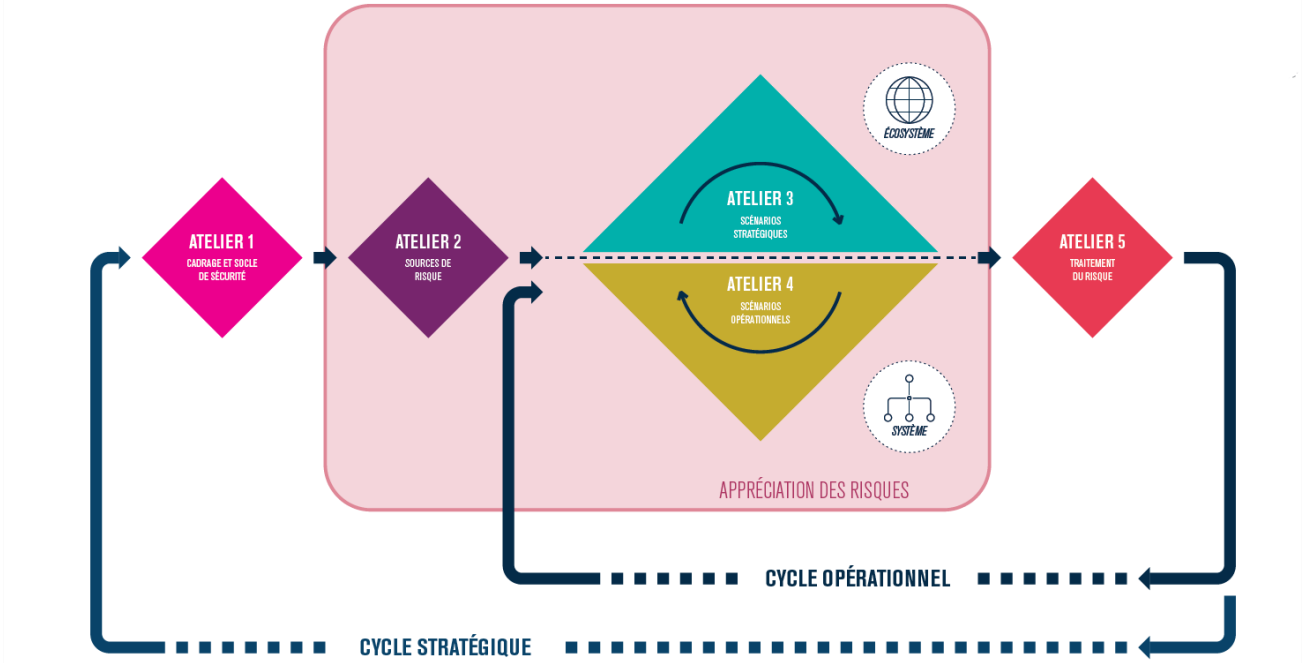
Méthodologie de l'ANSSI

EBIOS 2004, EBIOS 2010, EBIOS RM (2018)



EBIOS RM (2018)

Le point de vue du défenseur : Qu'est ce qui doit être protégé, et pourquoi ? L'atelier 1 est un atelier centré sur le périmètre de l'analyse. L'analyste cherche à y définir précisément les frontières (où commence et où se termine l'analyse), ce que les métiers craignent, et l'état d'application du cadre légal, normatif ou réglementaire (le socle de sécurité) sur le périmètre à analyser.



Qui est l'agresseur et pourquoi passe-t-il à l'acte ? L'atelier 2 est un atelier centré sur l'attaquant, qu'on va chercher à évaluer en termes de ressource & de motivation.

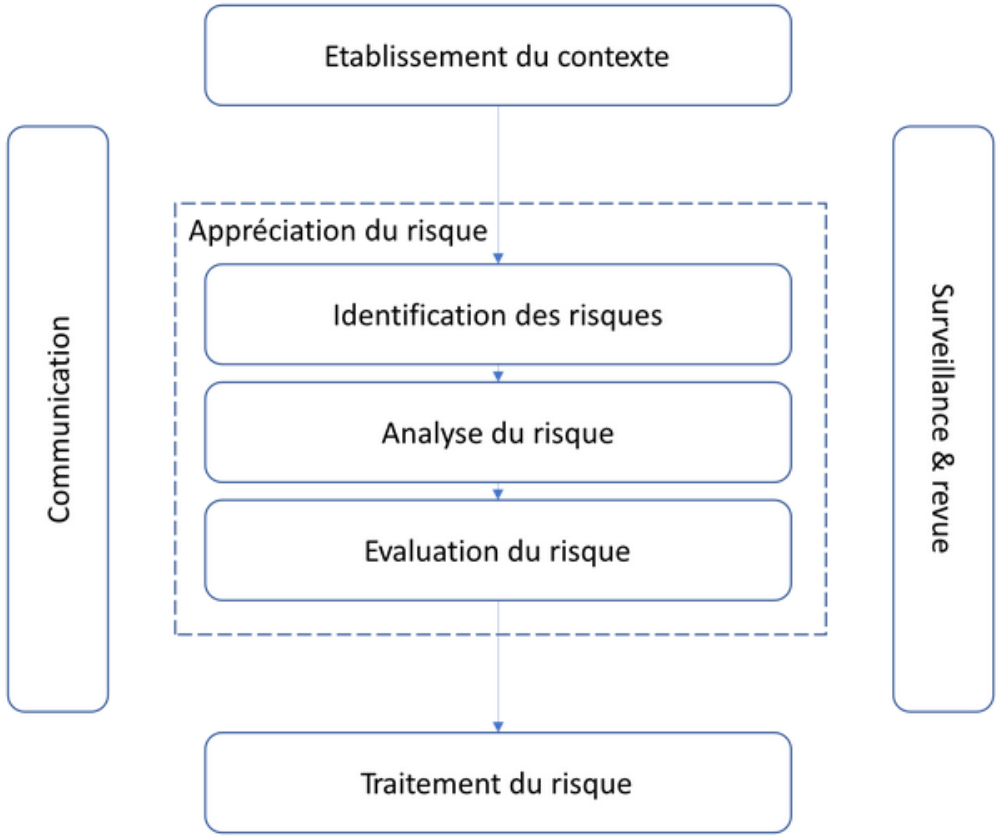
Par où l'attaquant va-t-il agir ? L'atelier 3 s'intéresse à l'écosystème (tout ce qui interagit avec le périmètre sans en faire partie) et à l'usage possible de cet écosystème par un attaquant pour atteindre son objectif.

Comment l'attaquant va-t-il agir ? L'atelier 4 cherche à évaluer la vraisemblance des attaques, en creusant les modes opératoires mis en œuvre par un attaquant et en appréciant leur probabilité de réussite.

Quelle stratégie de sécurité au regard des risques identifiés ? L'atelier 5 est une activité classique de remédiation : maintenant que les risques sont identifiés, comment réussir à les réduire ? Doit-on les traiter, les transférer, peut-on les accepter ?

ISO 27005

5 étapes également



Les étapes principales de la norme ISO 27005

ISO 27005

Etablissement du contexte	L'ISO 27005 appelle à identifier les exigences de base des parties intéressées, en intégrant à la fois des normes, de la réglementation, d'éventuels compléments provenant de la PSSI, etc.
Identification des risques	L'identification des risques au sens ISO 27005 est le processus consistant à rechercher, reconnaître et décrire les risques. Elle implique de déterminer les sources et ce qui peut se produire. La cible est d'avoir à l'issue de cette activité une liste de risques pouvant mener à la concrétisation de conséquences menaçant l'atteinte des objectifs de sécurité identifiés.
Identification des risques	Cette étape est destinée à évaluer, à travers un ensemble de critères déterminés en amont, les risques identifiés. Ce travail permettra de projeter chaque risque en termes de gravité et de vraisemblance lors de l'évaluation
Evaluation du risque	Cette étape est destinée à évaluer, à travers un ensemble de critères déterminés en amont, les risques identifiés. Ce travail permettra de projeter chaque risque en termes de gravité et de vraisemblance lors de l'évaluation.
Traitement du risque	L'ISO 27005 propose un traitement général du risque décomposé en plusieurs étapes : • Choisir l'option de traitement, en partant du principe que la réduction est l'option prioritaire • La préparation d'une déclaration d'acceptabilité (DdA), en lien avec l'annexe A de l'ISO 27001 • La formalisation d'un plan de traitement du risque • L'acceptation des risques résiduels
Communication	L'ISO 27005 présente le processus de communication de la manière suivante : « les informations sur les risques, leurs causes, leurs conséquences, leurs vraisemblances et les moyens de maîtrise mis en œuvre pour les traiter sont communiqués […] aux parties intéressées ».
Surveillance	La surveillance et la revue des risques sont, tout comme la communication sur les risques, un processus transverse et continu. C'est pourquoi il convient de surveiller et d'examiner régulièrement les risques pour s'assurer que les hypothèses les concernant et sur lesquelles repose l'évaluation du risque sont toujours valides. Il s'agira également de s'assurer que les résultats attendus sont atteignables et sont en bonne voie, que les techniques d'évaluation des risques sont correctement appliquées et que les traitements sont efficaces.

4-Conduire une réunion

Préparer la réunion

Les facteurs de réussite:

- Un objectif bien définit;
- Une liste de participants adaptée;
- Une logistique maitrisée;
- Des horaires et des durées maitrisées et réalistes;
- Etc.

Définir l'objectif de la réunion:

«Quel est l'objectif de ma réunion / quel doit en être le résultat? ».
Cette simple question vous permet d'évaluer les différentes ressources auxquelles vous allez faire appel:

- si des décisions immédiates doivent être prises, un décideur doit être présent;
- si des discussion techniques doivent être menées, un expert est nécessaire;
- Etc.

Choisir le modèle de réunion:

Le modèle de réunion découle de l'objectif de la réunion:

- Réunion de service;
- Réunion de conception;
- Réunion de design;
- Etc.

Les différents types de réunion ne sont pas abordés de la même façon.

Choisir les participants:
«Qui peut contribuer à l'objectif de la réunion / qui sera un frein à l'atteinte de l'objectif? »
Des réponses à ces deux questions découlera la liste des participants.

Planifier la réunion:
Assurez vous que l'ensemble des participants puisse être présents et, le cas échéant,assurez-vous que les participants clés puissent y assister

Préparez les documents de travail et les équipements:
- Votre power point;
- Le tableau blanc;
- Le vidéoprojecteur;
- Etc.

Rédiger un ordre du jour:
Un ordre du jour se prépare en amont: il permet aux participants de se préparer à la réunion, de venir avec des éléments concrets, préparés, vérifiés, etc

> ***Définition:*** *c'est une invitation à participer à une rencontre avec d'autres personnes nommées et présentées, dans un lieu, à une date et un horaire sur un thème et avec un objectif précis.*

• Il permet aux participants de déterminer si oui ou non leur présence est nécessaire: une information technique pouvant être diffusée par e-mail ne nécessite peut-être pas la présence à la réunion;
• Il permet à chacun de préparer les documents, les informations ou les questions;
• Il cadre le déroulement de la réunion et permet d'éviter tout débordement;
• Il constitue l'axe pour l'animateur de la réunion;
• Il permet d'évaluer la réussite, ou non, de la réunion;
• Il permet d'estimer le temps à mobiliser pour la réunion.

Il contient:

• Le titre (l'objet) de la réunion;
• Le type de réunion: réunion de travail, réunion stratégique, réunion de cadrage, etc.
• L'objectif global de la réunion pour que tout le monde aille dans le même sens;
• Le lieu, la date et l'heure;
• Présentation des participants: qui? (collègue, supérieur hiérarchique, fournisseur, client, etc.) et pourquoi (rôle, fonction, etc.);
• Présentation des items qui seront abordés ainsi que de leur objectif: présentation de chaque item, des temps prévus et des personnes qui traiteront le sujet (à elles de définir le temps);
• Si besoin, prévoyez des réunions qui permettront d'être exploitées en cas de débats plus longs que prévus;
• Pensez à prévoir des temps d'échanges;
• Relisez et faites vous relire: c'est votre image qui est en jeu;
• Diffusez l'ordre du jour dans un délai raisonnable pour que les points puissent être préparés.

Animer la réunion

Ca y est, le résultat de votre préparation se concrétise (serait-ce un projet?)! Il faut maintenant animer la réunion. Vos objectifs sont:

- Aider à la production pour atteindre les objectifs fixés et attendus de tous;
- Structurer et coordonner le groupe: chacun peut donner son avis, tempérer les caractères dominant, laisser leur place aux introvertis, etc.

3 phases:

- La phase d'introduction: présenter les sujets, les méthodes de travail, etc. vous vous positionnez comme l'architecte de la réunion;
- La phase d'aide à la production: stimuler le groupe, gérer les prises et temps de parole, aider les membres en difficulté face au groupe, contrôler et recadrer les participants « difficiles », traiter les conflits entre participants et recentrer les débats;
- Conclure la réunion et les phases suivantes: et oui, **vous n'avez pas fini!**

Un bon animateur, dispose de nombreuses qualités:

- sens du contact et de l'empathie;
- sincérité et une transparence;
- Capacité à manier l'humour et la rigueur;
- Leadership pour être écouté et crédible;
- Tolérance;
- Sens des responsabilités;
- Curiosité positive et capacité à remettre en question ses positions et ses avis.

Bien que souvent innées, ces qualités se travaillent: la communication est le principal axe pour s'améliorer.

Rédiger le compte rendu

Votre réunion est terminée, il convient maintenant de formaliser et de sécuriser les décisions qui ont été prise: **place au compte-rendu de la réunion**.

Après les discussions, place à l'action. Votre compte rendu doit:

- Etre rédigé le plus tôt possible pour ne rien oublier;
- Etre diffusé au plus tôt (dans la semaine qui suit);
- Etre concis, clair et efficace. Pour cela reprenez la structure de l'ordre du jour, la mise en parallèle des deux documents n'en sera que plus simple.

Au cours d'un projet, évitez de changer de présentation ou d'organisation de vos compte-rendu: la lecture globale de votre projet s'en retrouvera grandement améliorée.

Les décisions et leurs formalisations placées toujours au même endroit et présentées toujours de la même façon seront nettement plus simples à retrouver dans le temps.

Le compte rendu contient

- Le titre (l'objet) de la réunion;
- La date de la rencontre;
- La liste des présents (et leur rôle si besoin);
- La liste des destinataires;
- La liste des absents;
- Les sujets abordés: la synthèse des discussions, les conclusions et les décisions prises, les actions à mener en nommant les responsables des actions et les délais de réalisation;
- La date et le lieu de la prochaine réunion;
- D'éventuels commentaires et appréciations générales: soucis d'organisation, ambiance générale, etc.

Organiser la réunion à distance

A l'heure du télétravail, l'organisation d'une réunion à distance se développe et peut déstabiliser les participants:

• La personne introvertie sera plus dure à déceler;

• Le non respect des temps de parole des uns et des autres peut créer de lourdes frustrations qui nuiront au développement de votre objectif.

La planification de la réunion ressemble beaucoup au premier point de ce document. Il est tout de même **nécessaire de penser, en sus, à:**

• Le décalage horaire de certains de vos participants (si décalage horaire il y a)!

• La disponibilité pour tout les participants des outils de télécommunications nécessaires.

La planification de la réunion ressemble beaucoup au premier point de la conduite de réunion.
Il est tout de même **nécessaire de penser, en sus, à:**

• La disponibilité pour tous les participants des outils de télécommunications nécessaires et de savoir s'en servir;
• Le bon fonctionnement des outils et des connexions: à l'avance testez les liaisons vidéos ou téléphoniques;
• La localisation des participants:
• Un télétravailleur qui travaille depuis chez lui acceptera-t-il de filmer son domicile et donc option micro ou caméra ? Pensez à ce point, que faut il exiger ?
• Attention au décalage horaire de certains participants;
• La sécurisation du flux de données et des échanges: certaines réunion à distance peuvent avoir une importance stratégique: attention à ne pas mener des discussions sensibles dans une bibliothèque ou dans un open-space!
• Pensez aux outils nécessaires (teams, gotomeeting, etc…)

Peur de parler en public

https://www.facebook.com/lp2s59/videos/tedx-nabla-leviste-2020/574077556477279/

TD Réunion

Groupe Bayonne doit organiser une réunion de 10 minutes pour expliquer au **Groupe Toulouse** qu'il n'y aura pas de primes sur les projets cette année 2024. **Intervention du (de la) PDG et du (de la) DRH et du (de la) chef(fe) de projet pizza new**

Groupe Toulouse doit organiser une réunion de 10 minutes pour expliquer au **Groupe Fonsorbes** qu'il faut sécuriser le site web contre les attaques, nouvelle contrainte technique (double authentification des clients). **Intervention du (de la) DSI et du (de la) RSSI et du (de la) chef(fe) de projet pizza new**

Groupe 1 Fonsorbes doit organiser une réunion de 10 minutes pour un point d'étape sur le projet Pizza new du **groupe Marseille**. « Groupe Marseille ne comprend rien à Agile et trouve que c'est trop long comme démarche». **Intervention du (de la) PDG et du (de la) Directeur (trice) marketing et du (de la) chef(fe) de projet**

Groupe Marseille doit organiser une réunion de 10 minutes pour présenter l'outil de gestion RH envisagé au groupe Bayonne. Beaucoup de réticence, crainte de flicage. **Intervention du (de la) PDG et du (de la) Directeur (trice) RH et du (de la) chef(fe) de projet**

5-Note de cadrage

La note de cadrage est un document qui reprend les éléments essentiels d'un projet. Elle est importante, car elle permet de communiquer rapidement les informations aux différentes parties prenantes.

La note de cadrage reprend brièvement les éléments clés de votre projet. Rédigée par le chef de projet, elle répond aux questions **qqoqcp (« Qui ? Quoi ? Où ? Quand ? Comment ? Pourquoi ? »)**.
Elle décrit les différentes étapes nécessaires à la réalisation du projet.
En somme, il s'agit d'un résumé destiné aux parties prenantes du projet et aux collaborateurs inter-fonctionnels.

La note doit mentionner les exigences du projet, sans pour autant noyer vos collaborateurs sous les détails.

Qui ?	• De qui ? • Avec qui ? • Pour le compte de qui ?
Quoi ?	• Avec quoi ? • En relation avec quoi ?
Où ?	• Par où ? • Vers où ?
Quand ?	• A partir de quand ? • Jusqu'à quand ? • Dans quel délai ?
Comment ?	• De quelle façon ? • Dans quelles conditions ? • Par quel procédé ?
Pourquoi ?	• Cause • Facteur déclencheur • Justifications (ce qui a amené ce résultat)

Quand faire la note de cadrage ? Au début du projet

Il n'y a pas de format « officiel », elle doit comprendre les objectifs, chronologie, planning, cible et équipes mobilisées avec charges globales.

Ne pas confondre avec un cahier des charges ou CCTP (fonction publique) qui contient les spécifications précises et exigences qui donneront lieu à un chiffrage financier.

Ne pas confondre non plus avec la fiche projet qui elle identifie la raison d'être d'un projet. Cela peut être la fiche de demande d'une direction métier. Ou une synthèse qui sera la carte d'identité du projet dans un outil de gestion de projet (Project Monitor).
La note de cadrage réalisée par le chef de projet IT constitue déjà une évaluation du périmètre et un cadre de réponse à la fiche projet.

1-Le Projet

- Le sujet
- Description de l'organisation cible
- Enjeux (pourquoi on le fait ?)
- Problématique (quels freins on peut rencontrer ?)
- Objectifs (comment on le fait ?). On pourrait définir au niveau des objectifs des indicateurs de réussite ou des pourcentage d'avancement (notion de Definition Of Done)

2-Contexte

- Périmètre du projet (ce qu'on l'on fera dans le cadre de ce projet)
- Suites prévues (ce que l'on ne fera pas dans le cadre de ce projet mais qui pourrait être des extensions intéressantes)
- Les acteurs et leur rôles dans le projet

3-La réponse au besoin (comment on va travailler et quand on va le faire ?)

- Méthode de travail (mode projet)
- Définition des scénarios possibles
- Estimation des charges globales (en jour homme j/h)
- Macro planning du projet

6-Projet

Contexte du PDG: société **Pizza New** veut innover en proposant des commandes de pizzas sur la base d'ingrédients
Principe: le client choisit des ingrédients et le site web propose des pizzas contenant ces ingrédients qu'il peut commander. Il peut aussi créer sa propre pizza.

Organisation: 4 groupes de 6 (pas les mêmes que vos groupes habituels). Marseille, Fonsorbes, Bayonne, Toulouse

1 product owner (en lien avec la stratégie du PDG)
1 scrum master
1 stakeholder (responsable du magasin (Marseille, Fonsorbes, Bayonne, Toulouse)
3 development team

J1: equipe et backlog / J2: iteration 1 / J3: iteration 2 / J4: documentation et restitution

Evaluation projet
-Dossier de synthèse (10pts - groupe): cadrage projet, détail des itération (backlog, expression de besoin des users stories, planification, risques, suivi global du projet, arbitrage des choix (on fait / on fait pas), architecture technique envisagée, maquette des écrans et des livrables, maintenance envisagée. Qualité de communication du document
-Fiche de bilan (5pts – individuel): bilan de votre participation dans votre rôle. Avantages et inconvénients d'avoir travaillé dans ce mode projet. 2 pages A4.
-Communication orale (5pts – individuel): capacité à présenter son action de manière claire et fluide

Evaluation exos conduite de réunion

Itération 2 –
Note de cadrage du projet
Gestion de risques
Montrer les réalisations du sprint backlog
Bilan oral de chaque participant dans le groupe