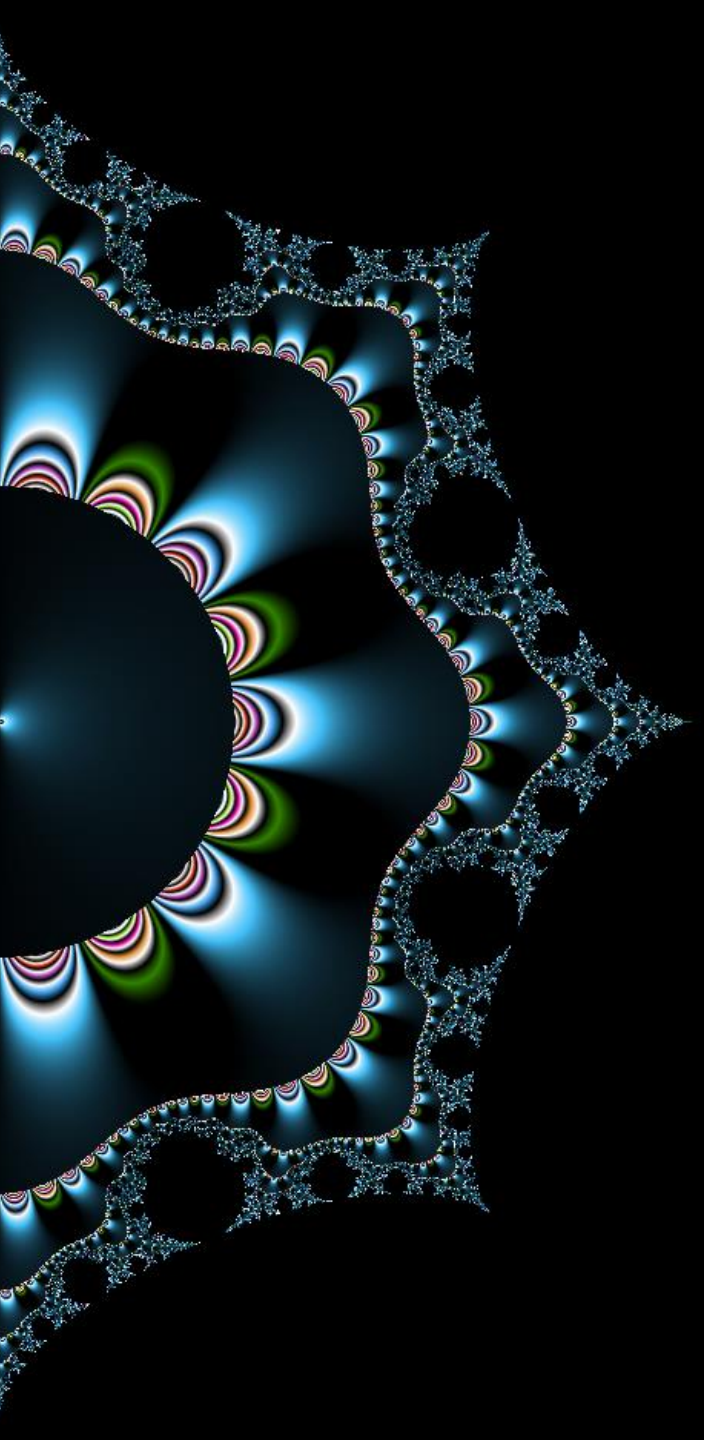


PSSI

Politique de Sécurité du Système d'Information

Thibaut HENIN

tbowan@arsouyes.org

C’est quoi la sécurité ?

Biens

Appelé aussi *ressources* ou *Assets*

Bien - définition

Une ressource

(de l'entreprise)

Qui doit être protégée

Des Informations

Documents, données

Savoirs, expertises

(Capital informationnel de l'entreprise)

Des Outils

Matériels

(Ordinateurs, serveurs, commutateurs, téléphones, machines)

Applications & Services

(Accès internet, messagerie, site web)

Propriétés de Sécurité

Qu’est-ce qu’on veut ?

Confidentialité

La ressource n’est accessible
qu’à ceux qui y sont autorisés

Disponibilité

La ressource est accessible

Lorsque on en a besoin

Intégrité

La ressource n’est modifiée

Que par des actions légitimes

Authenticité

Intégrité chez les cryptographes

La ressource est celle

Que l'auteur m'a envoyée

Traçabilité

Garder la trace des événements

(journalisation)

Qui, Quoi, Où, Quand

(Comment, Pourquoi)

Non Répudiation

Traçabilité chez les cryptographes

Preuve de l'événement

Déni plausible

Preuve de l'événement impossible

Matrice de couverture

Des biens par les propriétés

Bien	Confidentialité	Disponibilité	Intégrité
Comptabilité	✓	✓	✓
Plans	✓	✓	
PC		✓	
NAS	✓	✓	
Accès Internet		✓	

Exemple fictif d'un cabinet d'architectes

Analyse de Risques

Quelles sont les menaces ?

Événement redouté

Ou « menace »

Volontaire ou accidentel

Exemple de menaces

Cas fictif d'un cabinet d'architecte

Cambriolage

Ransomware

Panne Internet

Matrice de couverture

Des biens par les menaces

Bien	Besoin	Cambriolage	Ransomware	Panne Internet
Comptabilité	Confidentialité	✓	✓	
	Disponibilité	✓	✓	
	Intégrité	✓		
Plans	Confidentialité	✓	✓	
	Disponibilité	✓	✓	
PC	Disponibilité	✓	✓	
NAS	Confidentialité	✓	✓	
	Disponibilité	✓	✓	
Accès Internet	Disponibilité	✓		✓

Exemple fictif d'un cabinet d'architectes

Point faible

« Gravité » de l'événement redouté

Tel incident

A de grosses conséquences

(sur un bien et son besoin)

e.g.

Sans connexion internet,

pas de visio-conférence

Fragilité

« Probabilité / Vraisemblance » de l'événement redouté

Tel incident

Est facile à obtenir

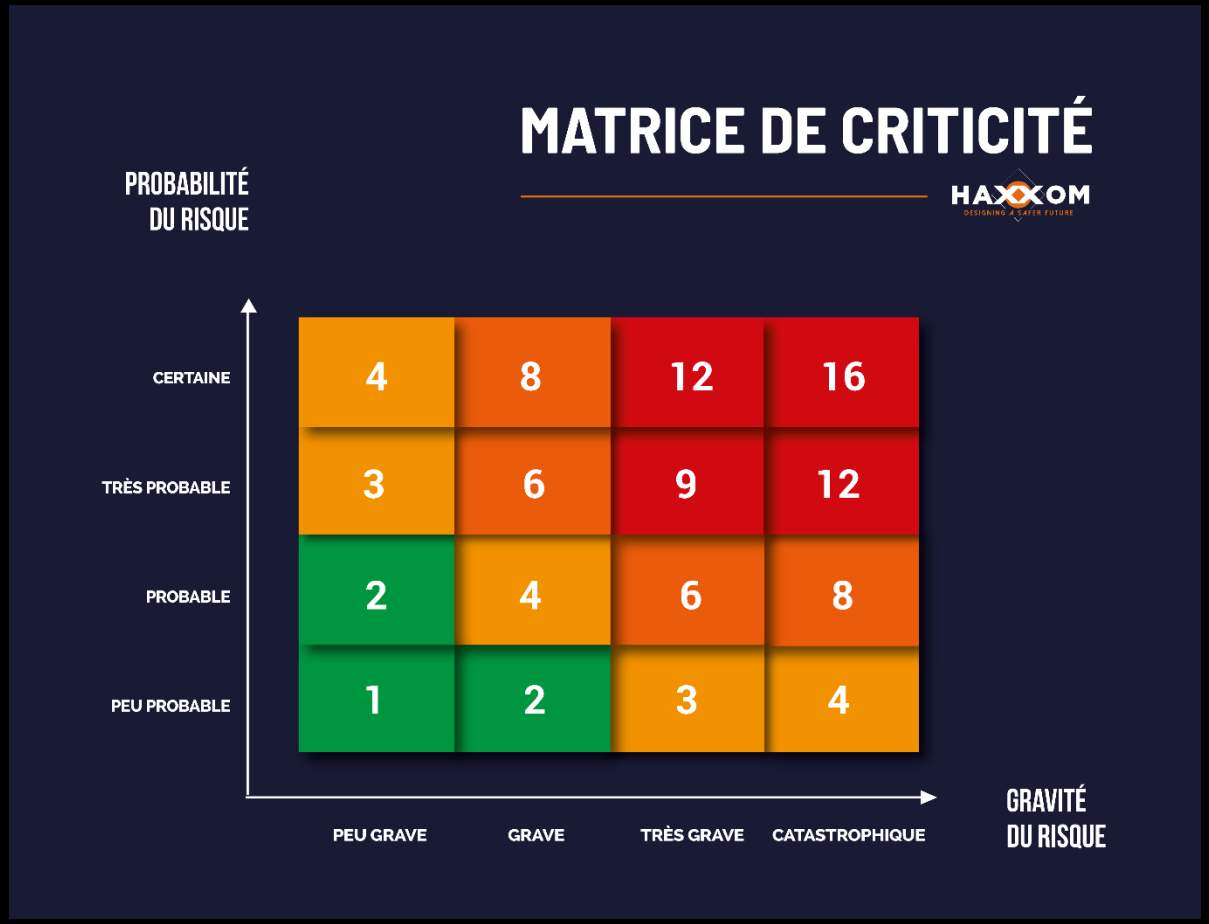
e.g.

Des chutes de neiges,

Cassent des câbles téléphoniques.

Matrice de criticité

« Gravité » de l'événement redouté



https://www.haxxom.com/processus-management-des-risques/

Exemple

Cas fictif d'un cabinet d'architecte

Menace	Cambriolage	Ransomware	Panne Internet
Gravité	4 - Catastrophique	4 - Catastrophique	2 - Grave
Vraisemblance	3 – Très Probable	2 - Probable	4 - Certain
Criticité	12	8	8

Exemple « non risque »

Cas fictif d'un cabinet d'architecte

Defaçage

(site web statique)

Exemple « non risque »

Cas fictif d'un cabinet d'architecte

Criticité nulle

Menace	Defaçage
Gravité	1 – Peu grave
Vraisemblance	1 – Peu probable
Criticité	1

Événement hors sujet

Bien	Besoin	Defaçage
Comptabilité	Confidentialité	-
	Disponibilité	-
	Intégrité	-
Plans	Confidentialité	-
	Disponibilité	-
PC	Disponibilité	-
NAS	Confidentialité	-
	Disponibilité	-
Accès Internet	Disponibilité	-

Politique de sécurité

Comment gérer ces risques

La PSSI…

Plan d'actions définies
pour maintenir
un certain niveau de sécurité

(wikipedia)

Point de vue

Différent suivant les interlocuteurs

Stratégique

(CoDir)

Opérationnel

(DSI, RH)

Commercial

(Client & partenaires)

Mesures de base

Pour TPE/PME

Contrôle d'accès

(physique, réseau, applications)

Sauvegardes

(sur place, distante, hors ligne)

Mises à jours

(système et applications)

Mesures avancées

Pour TPE/PME

Détection

(AV, IDS, SIEM)

Surveillance

(Monitoring, SOC)

Sensibilisation

(Chartes, formations)

Matrice de couverture

Des menaces par les protections

Mesure	Risque 2 (cambriolage)	Risque 3 (Ransomware)	Risque 1 (Panne internet)
Sauvegardes externes	✓	✓	
Serrures & Alarmes	✓		
Redondance internet			✓

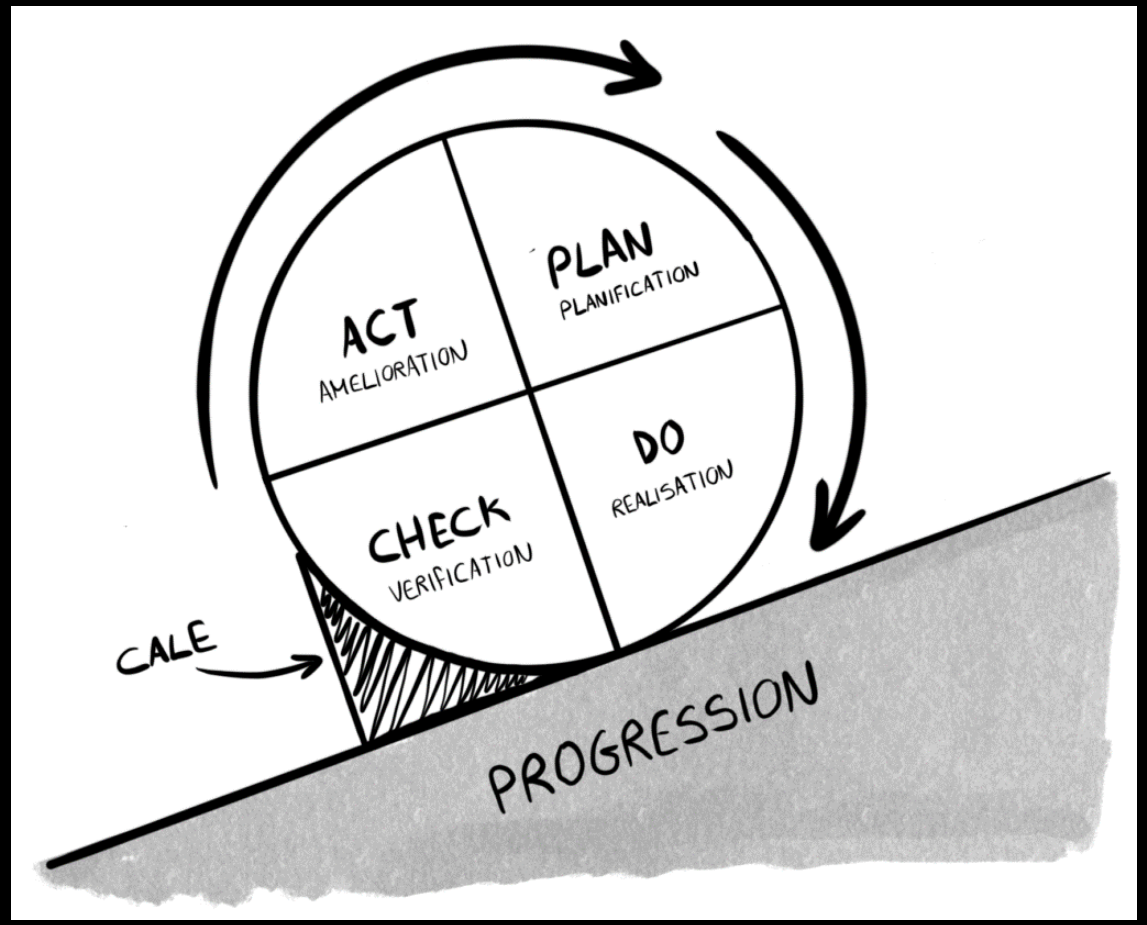
Exemple fictif d'un cabinet d'architectes

Criticité résiduelle

Cas fictif d'un cabinet d'architecte

Menace	Cambriolage	Ransomware	Panne Internet
Gravité	4 ↘ 2 – Grave	4 ↘ 1 – Peu grave	2 → 2 - Grave
Vraisemblance	3 ↘ 2 – Probable	2 → 2 – Probable	4 ↘ 1 – Peu probable
Criticité	12 ↘ 4	8 ↘ 2	8 ↘ 2

Amélioration continue



https://blog-gestion-de-projet.com/suivons-la-roue-de-deming-ou-cycle-de-shewart-deming/