PCA
et
PRA

Définitions

- Le Plan de Continuité des Activités (PCA) représente les mesures à prendre pour maintenir et poursuivre les activités fonctionnelles de l'entreprise en cas de sinistre, notamment informatique
- Le Plan de Reprise des Activités (PRA) représente les mesures visant à rétablir les fonctionnalités du système d'information de l'entreprise au plus vite en cas de sinistre

PCA

Plan de Continuité des Activités

Les étapes du PCA

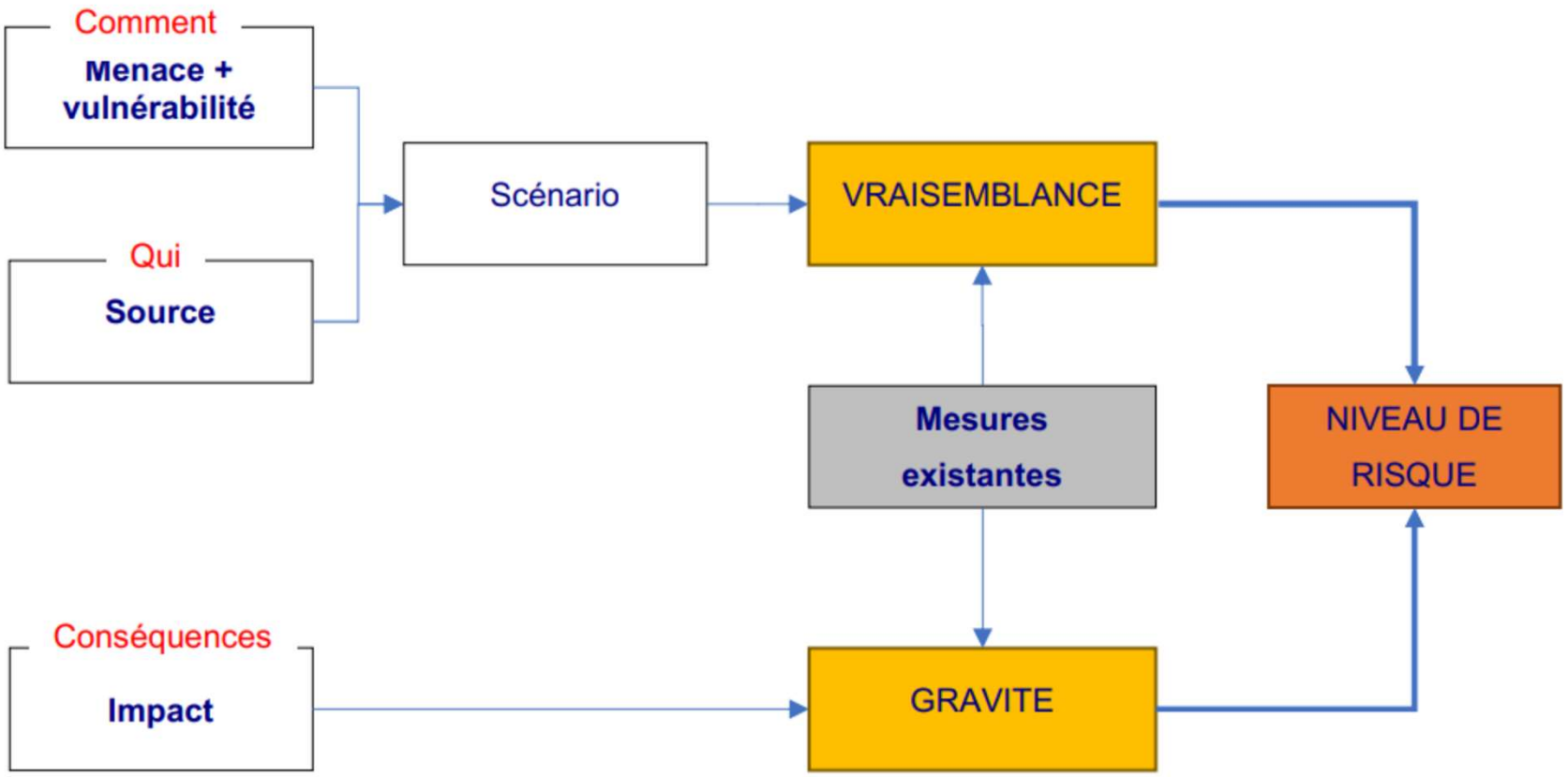
- identifier les fonctions et les ressources de l'entreprise par importance vitale
- détailler chaque fonction et préciser ce qui doit impérativement être maintenu en activité en mode dégradé
- organiser en identifiant les intervenants internes et externes qui vont mettre en place le PCA et l'appliquer en cas de crise = comité de mise en place
- former l'équipe qui va assurer la continuité, et soumettre cette équipe à des simulations régulières
- communiquer à l'ensemble de l'entreprise l'existence de ce PCA et comment il sera appliqué en cas de crise

PCA

L'identification des risques

- C'est l'étape est la plus importante
- L'entreprise identifie tous les risques susceptibles d'affecter les opérations de l'entreprise :
  - catastrophes naturelles (inondation, incendie, météo …)
  - épidémie / pandémie
  - coupures de courant
  - coupures du réseau internet ou du réseau téléphonique
  - pannes de matériels
  - erreurs imputables aux collaborateurs
  - dysfonctionnements (bugs) du système informatique pouvant entraîner la perte de données importantes
  - cyberattaques

Détermination du niveau d'exposition au risque



Grilles d ’évaluation des risques

Détermination des risques potentiels

Numérotation du risque	Chemins d'attaques stratégiques	Vraisemblance
R 1	Mail avec fichier infecté en pièce jointe	V 4 - Quasi certain
R 2	Clé USB piégée installée sur un ordinateur	V 1 - Peu vraisemblable
R 3	Installation d'une porte dérobée (backdoor)	V 2 - Vraisemblable
R 4	Piratage du Wifi	V 4 - Quasi certain
R 5	Piratage d'un compte VPN	V 2 - Vraisemblable
R 6	Prise de contrôle des serveurs de fichiers	V 4 - Quasi certain
R 7	Attaque par DoS	V 2 - Vraisemblable
R 8	Phishing pour récupérer des identifiants	V 3 - Très vraisemblable
R 9	Attaque Injection SQL	V 2 - Vraisemblable
R 10	Attaque XSS	V 2 - Vraisemblable
R 11	Attaque par Brute force sur les mots de passe	V 2 - Vraisemblable
R 12	Installation de keyloggers	V 1 - Peu vraisemblable

Grilles d ’évaluation des risques

Niveaux de risque - Acceptabilité - Décisions

Niveau de risque	Acceptabilité du risque	Intitulé des décisions et des actions
Faible	Acceptable en l'état	Aucune action à entreprendre
Moyen	Tolérable sous contrôle	Suivi à mener - Actions à mettre en place dans le cadre d'une amélioration continue sur le moyen et le long terme
Elevé	Inacceptable	Mesures de réduction du risque à prendre impérativement sur le court terme

Gravité et vraisemblance

Gravité					
4	R 12	R 7	R 8	R 1	
3	R 2	R 3, R 10, R 9, R 11		R 4, R 6	
2		R 5			
1					
	1	2	3	4	**Vraisemblance**

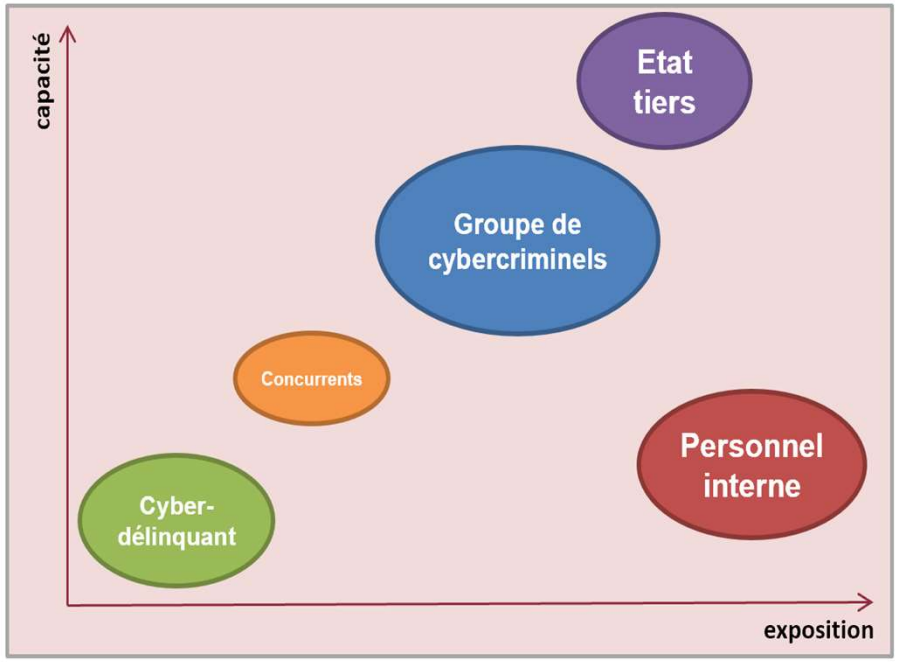
Exemple de synthèse des mesures de sécurité

Mesures de sécurité	Risques associés	Responsables	Freins et difficultés	Coût et complexité	Échéance	Statut
GOUVERNANCE						
Sensibilisation renforcée au phishing	R 1, R 7, R 8, R 9	RSSI	Validation du CHSCT	++	6 mois	A faire
Entraînement aux risques cyber	R 1, R 8, R 9, R 10, R 11, R 12	DSI		+	6 mois	A faire
Audit de sécurité technique et audit organisationnel	R 2, R 4, R 11, R 12	PASSI		+++	9 mois	A faire
Veille technologique	R 6, R 9, R 10, R 11	RSSI	Reflexion sur le mode de diffusion	++	6 mois	En cours
Mise en place de procédures de signalement d'incident	R 6, R 9, R 10, R 11	Equipe juridique		+++	12 mois	En cours
PROTECTION						
Renforcement des droits sur les données partagées	R 6, R 9	RSSI		+	3 mois	En cours
Renforcement des mots de passe (préconisations ANSSI)	R 4, R 5, R 6, R 9, R 10, R 11	RSSI	Utilisateurs	+++	3 mois	En cours
Protection des données (chiffrement, VPN ...)	R 6, R 10, R 11	RSSI, DSI	Revoir l'architecture du SI	++	9 mois	En cours
Renforcement des accès physiques	R 2, R 12	Equipe sécurité		++	3 mois	En cours
Gestion de l'obsolescence	R 6, R 9	RSSI, DSI	Budget	+++	9 mois	A faire
Mise en place d'une politique de sauvegardes	R 1, R 2	Administrateur	Budget	+++	6 mois	A faire
Segmentation des droits des utilisateurs	R 6, R 9, R 10	Administrateur		+	1 mois	Terminé
DEFENSE						
Surveillance renforcée des flux entrants et sortants	R 6, R 9, R 10	RSSI, Administrateur	Achat d'un logiciel	++++	6 mois	A faire
Système de surveillance des équipements sensibles	R 6, R 9	Equipe sécurité	Achat d'un logiciel	++++	6 mois	A faire
RESILIENCE						
Gestion de crise	R 4, R 6, R 7, R 9	RSSI, DSI, Direction		++++	6 mois	A faire
Mise en place d'un plan de continuité des activités (PCA)	R 1, R 2, R7, R 9	RSSI, DSI, Direction	Budget	++++	6 mois	A faire
Mise en place d'un plan de reprise des activités (PRA)	R 1, R 2, R7, R 9	RSSI, DSI, Direction	Budget	++++	6 mois	A faire

RSSI = Responsable Sécurité du Système d'Information
DSI = Direction des Systèmes d'Information
PASSI = Prestataire d'Audit de la Sécurité du Système d'Information

Cartographie des sources de menaces

Il est aussi possible de classer les sources de menaces selon leurs capacités et l'exposition de l'organisation



Exemple d'une cartographie des principales sources de menaces qui pèsent sur un S.I.

Capacité
degré d'expertise et ressources de la source de menaces

Exposition
opportunités et intérêts de la source de menaces

PCA

Déroulement

Une fois les risques identifiés, le PCA doit :

- déterminer comment chaque risque peut affecter le fonctionnement de l'entreprise
- mettre en œuvre des solutions de protection et des moyens pour diminuer les risques → prévention
- déterminer des procédures pour tester que ces solutions sont opérationnelles
- documenter chaque procédure
- former les collaborateurs à l'exécution de ces procédures
- revoir les procédures pour s'assurer qu'elles sont à jour techniquement

PCA

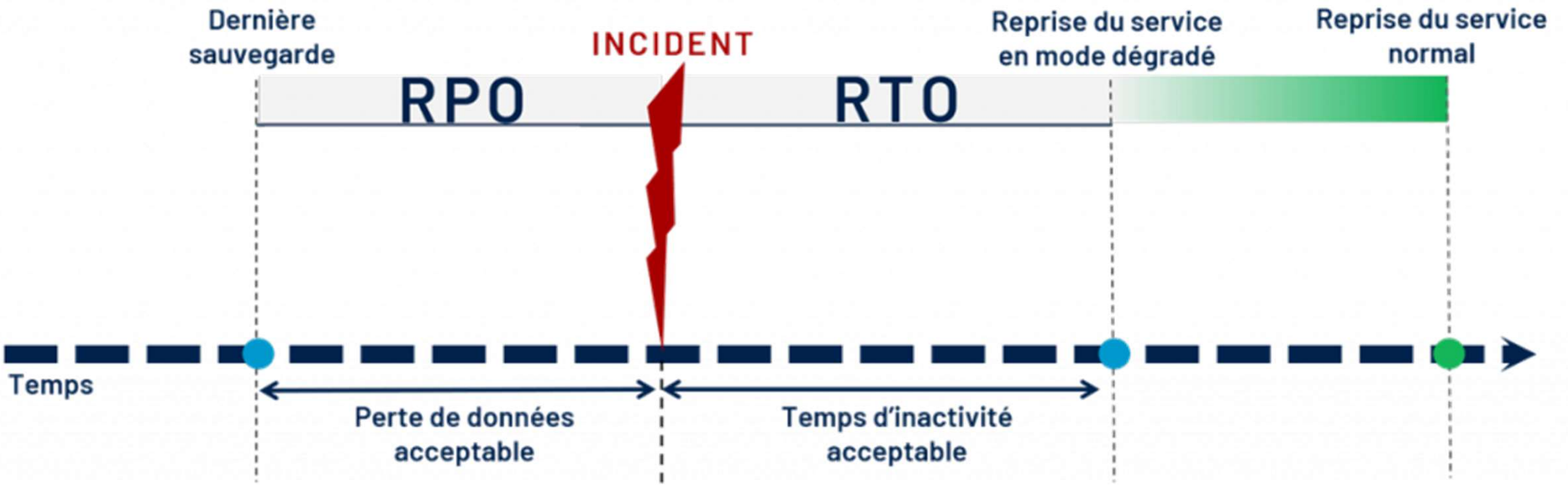
Exemples

- Mise en place d'un réseau secondaire : le réseau principal est affecté, on dérive l'activité vers un réseau secondaire
- Mise en place d'un site secondaire = site de « redondance »
  - ce site se substitue au site principal
  - ceci implique que toutes les informations soient mises à jour en simultané sur les 2 sites en permanence

PRA

Plan de Reprise des Activités

- Le PRA vise à minimiser les temps d'arrêts de l'entreprise en maintenant l'accès aux infrastructure informatiques et aux applications critiques
- Il définit aussi le rôle de chaque collaborateur dans la remise en place des services ainsi que les équipements nécessaires
- Il tient compte des ressources de l'entreprise :
  - les équipements
  - les collaborateurs
  - le budget
  - la priorité des activités à rétablir



Source : https://nuabee.fr/blog/comprendre-les-termes-rpo-et-rto

RPO

Recovery Point Objective

Le point de récupération (RPO)

- le RPO indique la quantité de données qu'une organisation accepte de perdre
- si un incident survient entre deux sauvegardes, quel historique de travail sommes nous prêts à perdre ?
- 10 minutes ? 1 heure ? 1 journée ?
- la réponse à cette question détermine la fréquence des sauvegardes à effectuer

RTO

Recovery Time Objective

L'objectif de temps de récupération (RTO)

- le RTO définit le temps d'arrêt tolérable pour une entreprise
- il dépend évidemment du secteur d'activité
- exemple :
  - quelques secondes d'interruptions peuvent représenter des pertes financières considérables pour des activités de trading
  - une base de données RH peut être indisponible pendant des heures sans nuire au fonctionnement de l'entreprise

Le RTO répond donc à la question :

- « *combien de temps peut prendre un système d'information pour être à nouveau accessible suite à interruption d'activité ?* »

PCA et PRA

Synthèse

- PCA et PRA ont des objectifs différents
- Le PCA lutte contre les arrêts opérationnels
- Le PRA prépare une remise en service la plus rapide possible après une interruption
- Toutes les entreprises, quelle que soit leur taille et leur chiffre d'affaires, sont concernées par le PCA et le PRA
- Ces deux plans assurent l'avenir de l'organisation