EQUIPAGES
IT SOLUTIONS

Comprendre et mettre en place un PCA / PRA informatique

Méthodes, exemples et modèles pour recenser, prévoir et budgéter

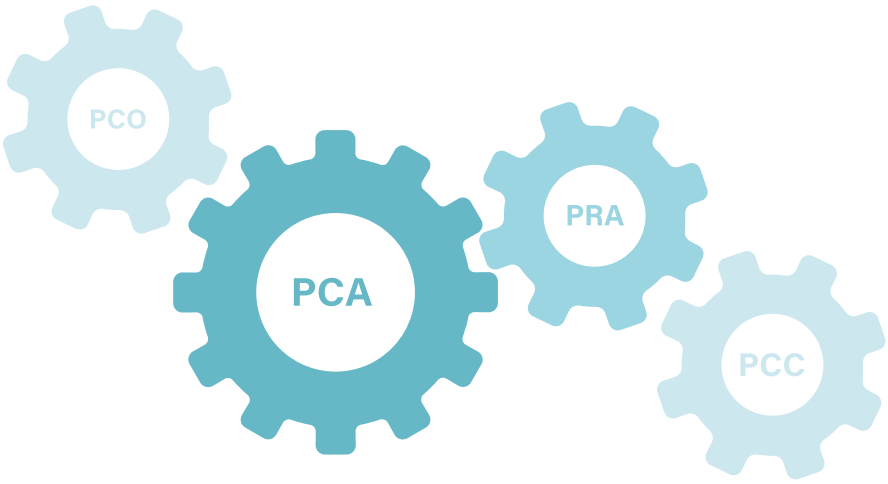
1.

Un peu de vocabulaire : Plans de reprise et continuité

Un peu de vocabulaire : Plan de Continuité d'Activité

Le PCA détaille l'ensemble des procédures destinées à assurer le maintien des activités essentielles de la société, de manière plus ou moins dégradée, en cas de crise ou de sinistre. Il se compose en réalité d'un ensemble de plans relatifs aux différents services de l'entreprise : continuité opérationnelle (CO), gestion de crise, communication de crise (CC), intervention d'urgence, reprise d'activité (RA), continuité informatique (CI)...

le PCI (**Plan de Continuité Informatique**) détaille toute les procédures mises en place afin que l'activité de l'entreprise se poursuive en cas de sinistre qui impacte les services informatiques.

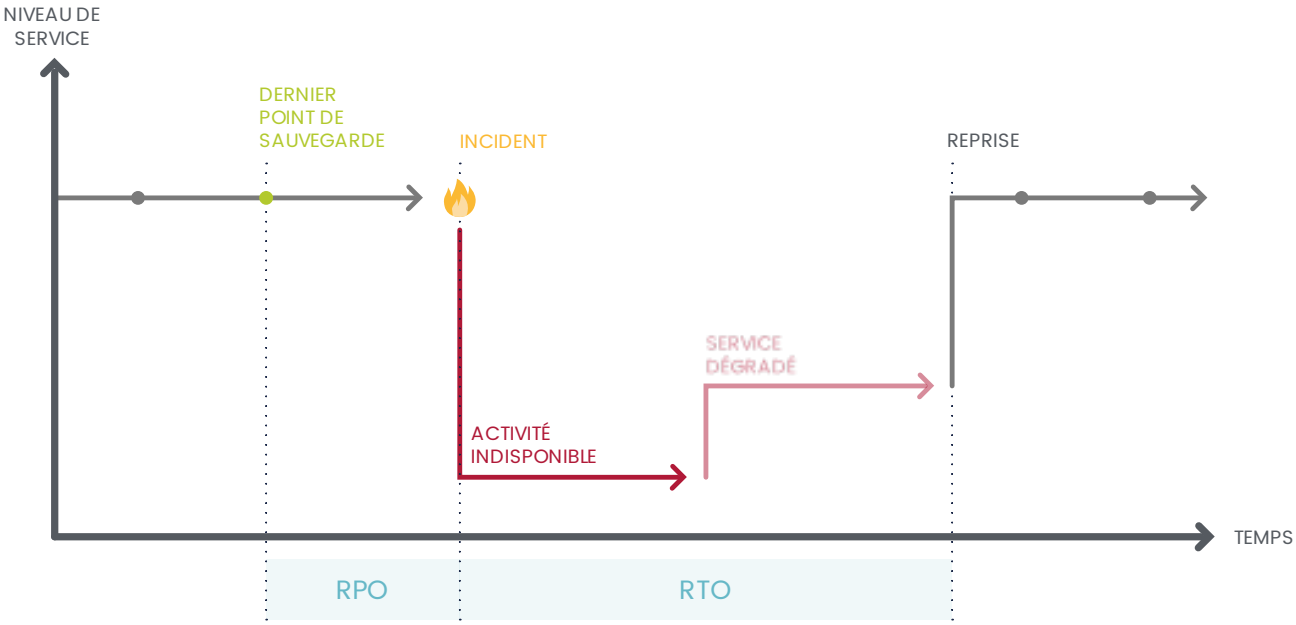


Toutes les structures n'ont pas forcément la nécessité ou les moyens de mettre en place un PCA : elles peuvent alors se tourner vers un PRA qui assurera une reprise de l'activité aussi ordonné, complète et rapide que possible.

Un peu de vocabulaire : Plan de Reprise d'Activité

Le PRA peut être mis en place dans le cadre d'un PCA, il aborde le scénario où la continuité n'a pas pu être assurée. Il détaille les procédures pour minimiser au maximum le **RTO*** et le **RPO*** : il faut reprendre l'activité au plus vite en ayant perdu le moins de données possible

Le PRI (**Plan de Reprise Informatique**) détaille ainsi les mesures pour rétablir les services informatiques en suivant les RTO et RPO préalablement définis à partir des niveaux de service minimum* et de service dégradé*.



RTO : Recovery Time Objective (Durée Maximale d'Interruption Admissible) > Temps nécessaire pour la remise en production, estimé à partir de la durée maximale pendant laquelle la société peut supporter l'absence d'activité

RPO : Recovery Point Objective (Perte de Donnée Maximale Admissible) > Intervalle de temps entre la dernière sauvegarde et le sinistre, estimé à partir de la quantité max de données que la société peut perdre

Niveau de service minimum : Niveau en dessous duquel l'activité est considérée comme indisponible
Niveau de service dégradé : niveau temporaire où l'activité est toujours disponible mais diminuée

2. Pourquoi mettre en place un PCA PRA : quelques chiffres

Le panorama des cyberattaques en 2022

En 2021, **54%** des entreprises déclarent avoir subit **au moins une attaque**.

Les attaques les plus répandues :

- **73%** Phishing
- **53%** Exploitation des failles applicatives
- **38%** Arnaque au président

Les conséquences les plus fréquentes :

- **32%** Usurpation d'identité
- **30%** Vol de données
- **23%** Ransomware

Sur 10 entreprises attaqués, **6** ont vu leur business directement impacté

- Perturbation de la production
- Compromission d'informations
- Indisponibilité du site web
- Retards de livraison

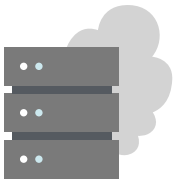
À la suite d'une attaque par ransomware, **1/3** des entreprises ont été contraintes de **suspendre temporairement ou définitivement leurs activités**

L'interruption **coûte en moyenne 27% du chiffre d'affaires**, et 60% des TPE / PME déposent le bilan dans les 18 mois.

Données issues de l'ANSSI, le Baromètre de la cybersécurité 2022 du CESIN, Etude annuelle sur les ransomwares de Cybereason

Quels risques pour les systèmes d'information ?

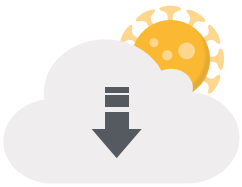
Sinistres géographiques : Incendie, inondation, tempête, séisme, coupure électrique...



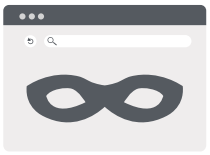
Défaillance matérielle : Arrêt d'un serveur, d'une machine de production, panne, bug...

Problèmes de réseau : Section de câbles lors de travaux, problème chez l'opérateur...

Prestataire : Arrêt de l'activité d'un prestataire dans votre chaine de production, application Cloud inaccessible...



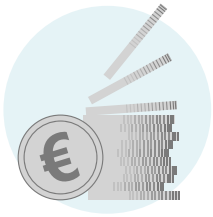
Erreur humaine : Erreur de manipulation, phishing, téléchargement dangereux par un de vos collaborateurs (virus)... 80% des attaques ont pour origine d'une erreur humaine



Menaces et malveillance : Piratage, cyberattaque, vol / dégradation d'un élément de votre infrastructure IT (ex: serveur), vol de données, espionnage industriel...

Situations exceptionnelles : Situations obligeant une modification des conditions de travail (ex: pandémie obligeant la mise en place du télétravail)...

Quelles conséquences pour les entreprises ?



Financières

Pertes dues à l'arrêt des activités et/ou inaccessibilité des services, vol financier, remplacement du matériel endommagé, sanctions financières, pénalités contractuelles, résiliations...

Juridiques

Sanctions administratives ou pénales en cas de vol / divulgation des données de vos clients, attaque en justice par les victimes de vol de données...

Sur l'image de l'entreprise

Image de marque abîmée, perte de confiance des clients et partenaires, diminution de la satisfaction client, perte de clients, perte de partenaires, méfiance des investisseurs, inaccessibilité du site web...

Interne

Difficultés à travailler et collaborer, perte d'outils de travail (documents, mails, bases de données...), moral des collaborateurs, chômage technique...

Fonctionnelles

Retard de production / des projets, indisponibilité des collaborateurs, impossibilité pour les clients d'utiliser les services de l'entreprise...

→ Peut aller jusqu'à l'arrêt définitif de l'activité

3. 15 étapes pour mettre en place un PCA PRA

Mettre en place un PCA / PRA : organiser le processus en 15 étapes

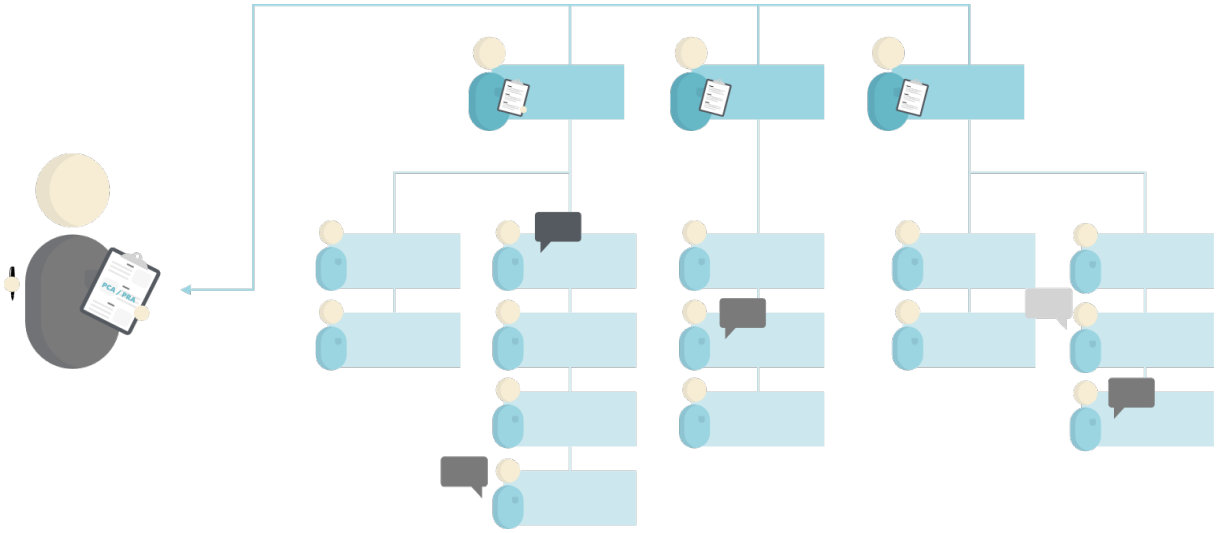
1. Engager la démarche
2. Identifier le périmètre
3. Identifier les composantes de l'infrastructure
4. Cartographier votre infrastructure
5. Identifier les processus et leurs dépendances
6. Identifier les besoins de continuité
7. Mesurer les conséquences d'une interruption
8. Identifier et évaluer les risques
9. Définir les objectifs en matière de reprise et continuité (RTO & RPO)
10. Identifier les ressources nécessaires
11. Aborder le PCA avec les partenaires et prestataires
12. Estimer le coût d'une interruption
13. Définir le budget du PCA PRA
14. S'assurer que les personnes impliquées sont formées et informées
15. Faire évoluer le plan, réaliser des exercices et des tests

FICHE 1 Engager la démarche

Impliquer la direction opérationnelle

Afin que le PCA soit réaliste et cohérent, il faut que les responsables métiers et processus soient impliqués dans la validation de chaque étape qui concerne leur domaine d'activité : description du contexte, identification des processus clés et des risques, estimation des conséquences, mesure des ressources nécessaires; établissement de la stratégie de continuité…

Sans leur participation, la récupération d'information sera plus longue, et les plans mis en place pourraient être inapplicables (manque de moyen, de ressources humaines, techniques…).



Définir le(s) responsable(s) du projet

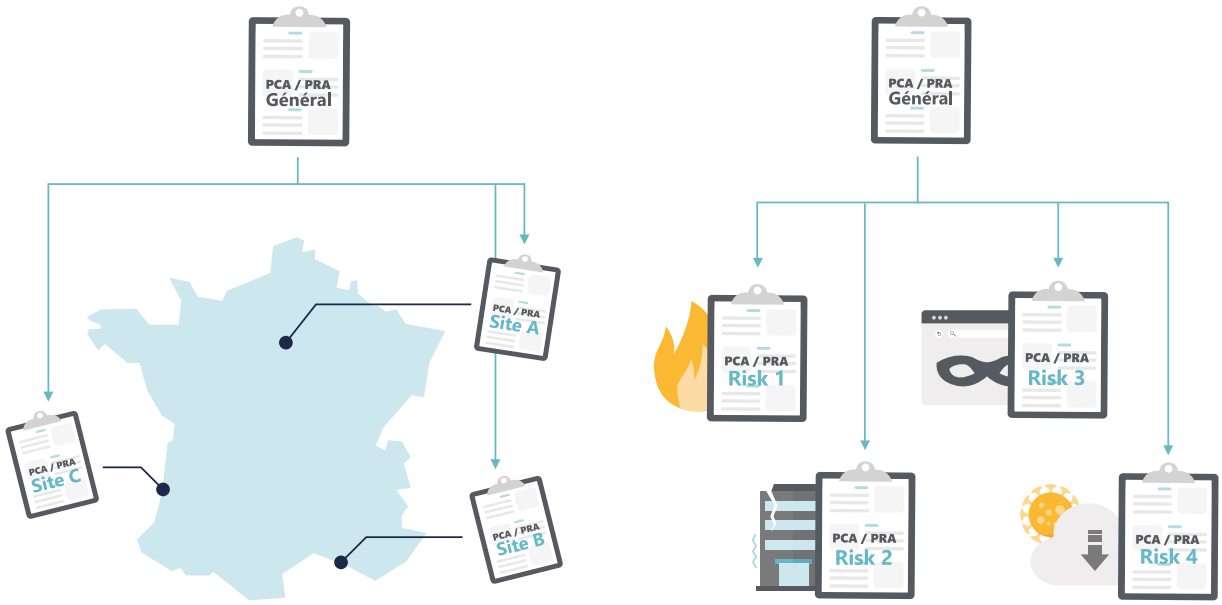
Etablir un PCA/PRA est une démarche qui demande plusieurs mois de travail et la collaboration de nombreux services. En confier le pilotage à un responsable (éventuellement accompagné d'une équipe) est indispensable pour espérer mener le projet à bien. Il faudra que ce responsable ait une connaissance des rouages de l'entreprise, une autonomie et une autorité suffisantes pour obtenir les informations nécessaires et faire accepter d'éventuels changements.

FICHE 2 Identifier le contexte

PCA unique ou sectoriel ?

Un PCA unique à tous les domaines et tous les sites géographiques de l'entreprise pourrait sembler plus simple. Mais, en raison de la complexité interne des organisations, il est en réalité recommandé d'établir un PCA général « modèle » qui contient les règles majeures et à partir duquel seront élaborés des PCA sectoriels. Il peut s'agir de PCA par site géographique, par type d'activité, par type de sinistre…

Cette méthode permet d'éviter la multiplication de scénarios propres à un seul site, et donc d'alourdir le PCA général et allonger son temps de création.



Recenser les PCA existants

Qu'il s'agisse d'initiatives personnelles, de démarches passées ou de processus existants dans certains secteurs de l'entreprise (par exemple suite à la fusion de plusieurs entités dont l'une en disposait déjà), il est possible que votre organisme recense plusieurs PCA sectoriels. Dans ce cas, il est important de tous les récupérer et de procéder à une première consolidation : vous pourrez peut-être gagner beaucoup de temps si des étapes déjà réalisées conviennent à l'ensemble de la société, et réutiliser la structure du document pour construire le votre.

FICHE 3 Recenser les composantes de l'infrastructure

Recenser les équipements informatiques

Le 1er pas pour établir un PCA complet est de savoir quels sont les éléments qui composent votre infrastructure IT et identifier :

- Caractéristiques : marque, dimensions, numéro de série…
- Sont-ils physiques ou virtuels ? Si physique, quel site / bâtiment / salle ?
- Comment sont-ils protégés (physique et/ou logiciel)
- Sont-ils hébergés par un prestataire externe ? Si oui, quels sont les coordonnées du commercial responsable de votre compte et du support ?
- Quel est votre stock : combien en utilisez-vous ? Combien en avez-vous à disposition en cas de besoin ?

Le recensement de toutes ces composantes est fastidieux, mais il participera à une meilleure gestion des stocks informatiques et permettra de faire une première évaluation de l'ensemble des mesures à créer dans le cadre du PCA/PRA.

Cette étape peut être réalisée par les responsable locaux puis mise en commun.

MODÈLE

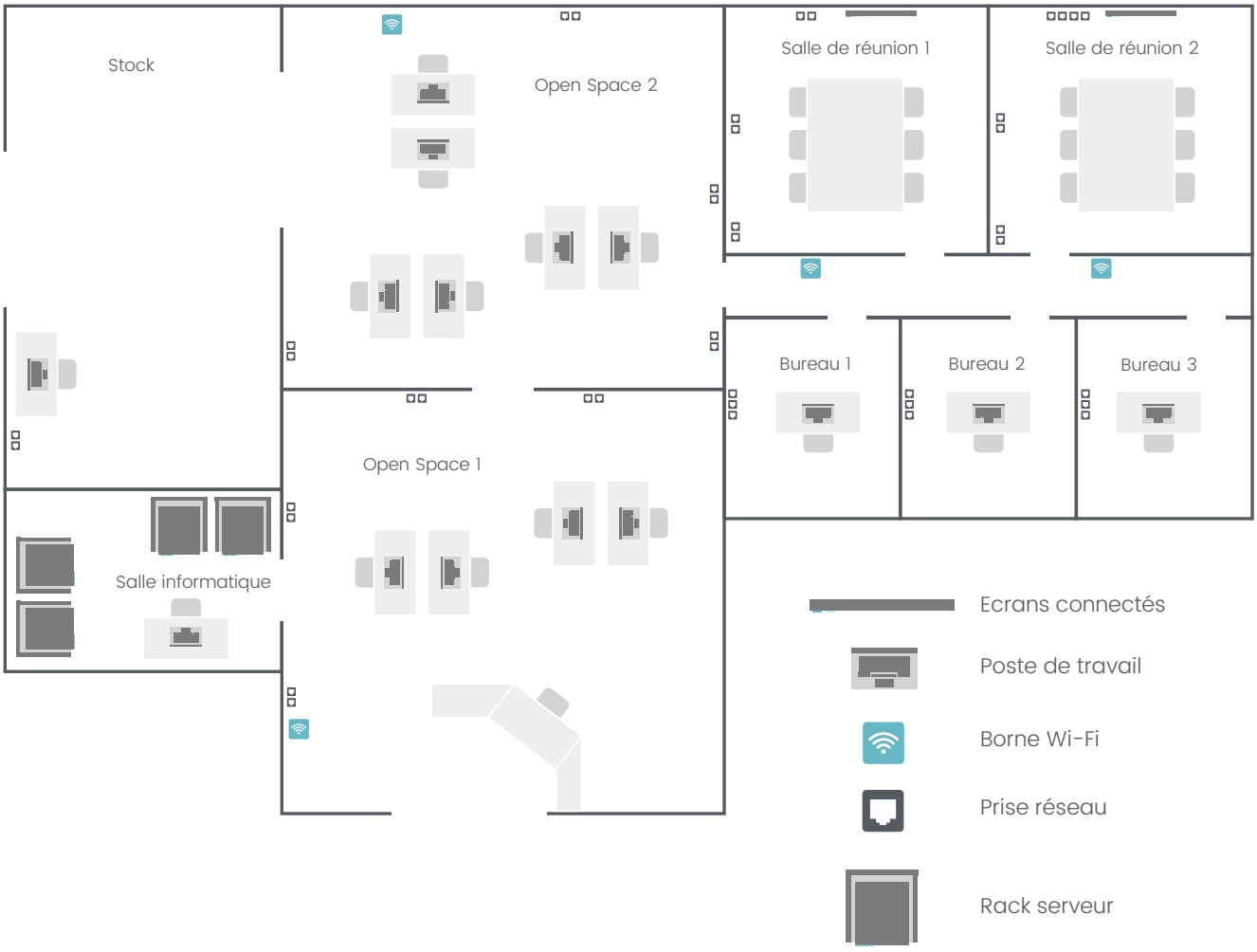
Type	Localisation	Nombre	Prestataire	Caractéristiques
Serveur, sauvegardes, téléphonie, réseau interne, site internet, applications, systèmes de surveillance et de climatisation, postes de travail…	Virtuel, Physique (préciser site et salle), hébergé chez prestataire…	Répartition par site, quantité en stock / utilisée	Nom du prestataire, contacts du commercial et numéro du support	Marque(s), dimensions, type de protections mises en place…

FICHE 4 Cartographier l'infrastructure

Cartographier les flux informatiques et les interconnexions

Etablir une carte site par site qui situe les composantes de votre infrastructure informatique, et les liens entre eux permettra de faire une 1ère évaluation des interdépendances qui existent au sein de votre réseau. Cette étape permettra également de savoir rapidement quels seraient les matériels IT touchés en cas de sinistre sur un site ou dans une salle spécifique par exemple.

MODÈLE



FICHE 5 Identifier les processus et dépendances

Identifier les processus

Une fois votre infrastructure cartographiée, il est temps de faire le point sur l'ensemble des processus de l'entreprise, afin de déterminer quels sont ceux qui peuvent être arrêtés plus ou moins longtemps (à traiter dans le PRA) et quels sont ceux qui ne peuvent être arrêtés sous aucun prétexte au risque de causer la faillite de l'entreprise (à traiter dans le PCA). Il faut donc les recenser, identifier à quelle activité ils se rapportent et qui en est responsable.

[Identifier la dépendance informatique]

Chaque processus est ensuite relié aux composantes de l'infrastructure IT qui lui permettent de fonctionner (applications, réseaux, bases de données...). Cette démarche n'est pas indispensable, mais elle facilitera l'étape 7 en créant une cartographique des dépendances à chacun de vos éléments d'infrastructure.

MODÈLE

Processus	Activités concernées	Respon-sable(s)	Applications utilisées	Composantes IT concernées
Prise de commande, livraison, facturation, salaires, maintenance, emailing, stockage...	RH, Commercial, Comptabilité, Finance, Logistique, Production, Communication	En charge des décisions sur ce processus	Office O365, ERP, CRM, logiciel de paie, logiciel de facturation, messagerie...	Site internet, téléphonie, réseau, base de données...

Une bonne méthode pour recenser tous les processus de l'entreprise est de suivre le parcours client : ainsi, vous identifiez tous les processus par lequel il passe, et pouvez y relier tout ceux qui sont nécessaires en interne pour rendre ce parcours fonctionnel.

FICHE 6 Identifier les besoins de continuité (1/2)

Calculer la criticité des processus

Dans cette étape, il est indispensable d'impliquer les responsables des processus : c'est eux qui seront le plus à même de déterminer les niveaux de service minimum, de service dégradé et d'indisponibilité maximum de chaque processus, au-delà desquels leur activité, voire même l'entreprise, sera mise en danger.

Pour évaluer l'importance du processus pour l'activité de l'entreprise, vous pouvez vous concentrer sur la manière dont le processus impacte :

- Sa disponibilité (continuité de l'activité)
- Son intégrité (respect de qualité du produit/service fourni au client)
- Sa confidentialité (protection des données sensibles impliquées)
- Sa traçabilité (suivi des événements et déplacements)
- Sa sécurité (limitation des actes malveillants)

Certaines activités seront en effet arrêtées dès que l'un de ces critères n'est plus respecté. Il faut donc réfléchir à la manière dont le processus impacte un ou plusieurs de ces critères et l'importance de ces derniers pour l'activité. A partir de cette réflexion, vous noterez le processus sur une échelle de 1 à 5 :

1 Superflu (dégrade l'expérience utilisateur et/ou client mais n'entrave pas l'activité)

2 Non critique (l'arrêt dégrade l'activité mais ne la met pas en danger)

3 Important (l'arrêt dégrade l'activité et sa prolongation la met en péril)

4 Critique (l'arrêt met l'activité en péril)

5 Indispensable (l'arrêt met l'entreprise en péril)

FICHE 6 Identifier les besoins de continuité (2/2)

Evaluer le niveau de service min et d'indisponibilité max

Une fois la criticité du processus établie, il faut déterminer :

- Combien de temps l'activité de l'entreprise peut continuer en cas d'arrêt du processus (indisponibilité maximum)
- À partir de quel niveau de service le processus est considéré comme indisponible car il impacte trop la qualité de l'activité (niveau de service minimum)
- Lorsqu'un processus demeure fonctionnel (niveau de service > niveau minimum) mais n'est pas 100% opérationnel, l'activité est réduite à un niveau de service dégradé. Cette situation n'est pas durable, mais permet de maintenir l'activité jusqu'à retour à la normale

EXEMPLE

A cause de défaillances techniques, un fournisseur de produit frais pour restaurant ne dispose plus que de 2 camions au lieu des 4 habituels. Avec 2 camions, il peut tout de même assurer 200 livraisons par jour, c'est plus que les 100 minimum qu'il lui faut pour que sa journée soit rentable (*niveau de service minimum = 100 livraisons / jours*). Grâce à une réorganisation des trajets, une réduction des commandes et la mise au chômage technique de 2 chauffeurs, la société peut assurer le maintien de son activité en *service dégradé*. Mais si la situation dure plus de 3 mois, elle risque d'aggraver la fatigue des effectifs, l'usure des camions restants, de perdre des parts de marché, périmer une partie de son stock et sa trésorerie ne pourra plus compenser le nombre de commande réduit : c'est *l'indisponibilité maximum* de ses camions.

MODÈLE

Processus	Tolérance fonction dégradée					Tolérance arrêt complet				
	1min	1h	24h	7j	30j	1min	1h	24h	7j	30j
	Oui / non	Oui / non	Oui / non	Oui / non	Oui / non	Oui / non	Oui / non	Oui / non	Oui / non	Oui / non

FICHE 7 Mesurer les conséquences

Définir l'impact de chaque incident

Grâce à l'étape 5, nous pouvons savoir de quels éléments de l'infrastructure IT est dépendant chaque processus. Il faut désormais estimer quel impact aura l'indisponibilité de chaque élément IT sur le bon fonctionnement du processus.

EXEMPLE

Prenons par exemple une société de vente de vêtements en ligne :

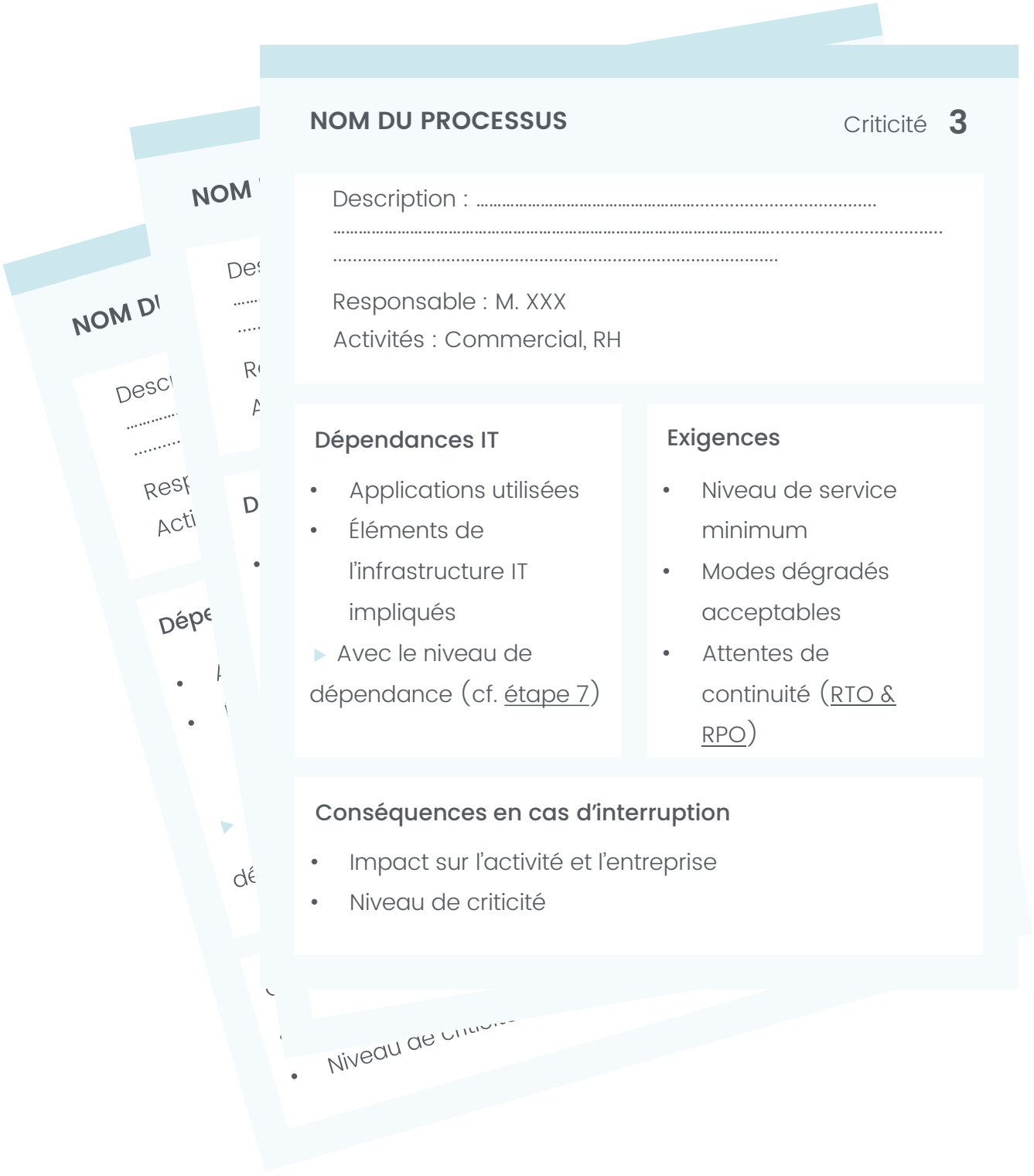
- Une indisponibilité du site web entravera les processus de communication, de prise de commande, de paiement et de fidélisation
- Une panne du système de téléphonie va dégrader la communication interne, les échanges avec les partenaires et interrompre le processus de SAV
- Une indisponibilité du système de facturation va interrompre le processus de paiement des fournisseurs, ce qui va dégrader les livraisons ou encore la gestion du stock

MODÈLE

	Processus 1	Processus 2	Processus 3	Processus 4
Panne élément 1	HS	HS	Dégradé	Fonctionnel
Panne élément 2	HS	HS	HS	Dégradé
Indisponibilité app 1	Dégradé	HS	Fonctionnel	Dégradé
Indisponibilité app 2	Fonctionnel	Fonctionnel	Dégradé	HS

ANNEXE Fiche de processus

A partir d'ici, il est possible de constituer des fiches récapitulatives concernant chaque processus, les exigences de continuités et ses dépendances aux éléments de l'infrastructure IT



FICHE 8 Mesurer les conséquences (1/4)

RISQUE = MENACE x VULNÉRABILITÉ x IMPACT x PROBABILITÉ

Répertorier les menaces et votre vulnérabilité à ces dernières

Maintenant que nous connaissons l'impact d'un incident IT sur l'activité de l'entreprise, il faut évaluer quels sont les risques que cet incident se produise, c'est-à-dire quelle est la vulnérabilité de l'entreprise face aux menaces qui pourraient causer cet incident.

Vous devez donc mener une analyse des menaces qui peuvent peser sur votre / vos site(s) et votre infrastructure (cf. page Risques) :

- **Géographique** : Êtes vous en zone à risque (le gouvernement détaille et cartographie l'ensemble des risques naturels qui peuvent survenir sur le territoire sur www.georisques.gouv.fr) ?
- **Réseau** : Travaillez-vous avec plusieurs opérateurs réseau ? Ont-ils des procédures de secours en cas d'interruption ? Une Garantie de Temps de Rétablissement dans votre contrat ?
- **Matériel** : Quels sont vos contrats de support et/ou d'infogérance ? Vos équipes IT ont-elles une bonne expertise sur les éléments de votre infrastructure ? Votre infrastructure est-elle dans une salle sécurisée ?
- **Humain** : Les collaborateurs sont-ils sensibilisés et formés aux cyber-risques ?
- **Malveillance** : Disposez-vous des logiciels adaptés pour faire face aux cybermenaces (virus, ransomware,...) ? Tous vos logiciels sont-ils à jour ? (test de cybersécurité et outils d'autodiagnostic mis à disposition par www.cybermalveillance.gouv.fr)

FICHE 8 Mesurer les conséquences (2/4)

RISQUE = MENACE x VULNÉRABILITÉ x IMPACT x PROBABILITÉ

Déterminer l'impact de chaque menace

Chaque menace peut impacter votre informatique de manière plus ou moins grave. Il vous faudra donc déterminer quel serait l'impact global d'une menace en évaluant quelles en seraient les conséquences sur les éléments de votre infrastructure. En fonction de la gravité de l'impact, du nombre d'éléments impacté et de la criticité desdits éléments, vous pourrez attribuer une note à chaque menace :

1 Insignifiant (Peu d'impact sur des éléments peu critiques)

2 Mineur (Impacts sur plusieurs éléments peu critiques)

3 Modéré (Impacts sur plusieurs éléments modérément critiques)

4 Majeur (impacts sur beaucoup d'éléments et/ou quelques éléments critiques)

5 Catastrophique (fort impact sur des éléments critiques)

MODÈLE

	Impact				
Menace	Élément 1	Élément 2	Élément 3	...	Moyenne
Incendie salle machine, inondation des locaux, opérateur down, câbles réseau sectionnés, vol...	Note 1 à 5				Moyenne en fonction des note et criticité des éléments

FICHE 8 Mesurer les conséquences (3/4)

RISQUE = MENACE x VULNÉRABILITÉ x IMPACT x PROBABILITÉ

Déterminer la probabilité d'occurrence

Les menaces n'ont pas toutes la même probabilité d'occurrence de part leur nature, mais également en fonction de la situation géographique : un des site peut être inondable et pas les autres par exemple.

Il vous faudra donc déterminer quelle est la probabilité d'occurrence de la menace, site par site, en évaluant les chances qu'elle se produise sur 5 ans.

1 Très faible (< 0,05% : la menace a peu de chance de se produire)

Ex : inondation, risque sismique, attentat, circonstances exceptionnelles

2 Faible (> 0,05% : la menace peut occasionnellement se produire)

Ex: section de câble lors de travaux, départ de feu, cambriolage, crise sociale…

3 Moyenne (> 0,5% : la menace se produira vraisemblablement)

Ex: Tempête, fuite canalisations, arrêt serveurs…

4 Forte (> 5% : la menace à de forte chance de se produire)

Ex: Coupure électrique, cyberattaque, températures extrêmes, indisponibilité d'une application…

5 Très forte (> 50% : la menace est quasi certaine)

Ex: bug matériel, erreur humaine, problème opérateur, problème prestataire…

FICHE 8 Mesurer les conséquences (4/4)

RISQUE = MENACE x VULNÉRABILITÉ x IMPACT x PROBABILITÉ

Hiérarchiser les risques

Une fois la probabilité et l'impact calculés, vous pouvez finalement croiser ces données pour déterminer le niveau de risque encouru. C'est ce niveau qui permettra de savoir sur quelles menaces votre PCA/PRA doit se concentrer, et dans quel ordre vous devrez élaborer et mettre en place les mesures de continuité et reprise.

1 à 4 faible (Impact et probabilité faible)

5 à 6 moyen (Impact fort mais faible probabilité ou inversement)

7 à 8 élevé (Impact et probabilité moyens à forts)

9 à 10 extrême (Impact et probabilité élevé)

Niveau de risque		IMPACTS				
		5 - Catastrophique	4 - Majeur	3 - Modéré	2 - Mineur	1 - Insignifiant
PROBABILITÉ	5 - Très forte	10	9	8	7	6
	4 - Forte	9	8	7	6	5
	3 - Moyenne	8	7	6	5	4
	2 - Faible	7	6	5	4	3
	1 - Très faible	6	5	4	3	2

ANNEXE Récapitulatif d'avancement

Cette annexe conclut la partie « audit » de votre infrastructure IT, de votre activité et des risques que vous encourez. Avant de passer à la suite, assurez-vous de n'avoir manqué aucune étape afin que la suite du travail soit pertinente.

Lancement

- ☐ Vous avez défini un responsable du projet PCA/PRA (Fiche 1)
- ☐ Vous avez informé l'ensemble des directeurs du lancement du processus (Fiche 1)
- ☐ Vous avez recensé et consolidé les éventuels PCA existants (Fiche 2)

Contexte interne

- ☐ Vous avez réalisé une cartographie de votre infrastructure IT (Fiche 3 et Fiche 4)
- ☐ Vous avez recensé les principaux processus de votre activité (Fiche 5)
  - ☐ Vous avez identifié leur dépendance à votre infrastructure IT (Fiche 5)
  - ☐ Vous avez évalué leur criticité (Fiche 6.1)
  - ☐ Vous avez évalué leur besoin de continuité (Fiche 6.2)
- ☐ Vous avez estimé l'impact d'une panne IT sur vos processus pour chaque élément de votre infrastructure (Fiche 7)

Risques

- ☐ Vous avez identifié l'ensemble des menaces qui peuvent affecter votre infrastructure IT (Fiche 8.1)
  - ☐ Vous avez déterminé les conséquences de chacune de ces menaces sur votre infrastructure (Fiche 8.2)
  - ☐ Vous avez estimé la probabilité d'occurrence de chacune de ces menaces (Fiche 8.3)
- ☐ Vous avez hiérarchisé les menaces en fonction de leur risque (Fiche 8.4)

FICHE 9 Formuler les objectifs de continuité et reprise

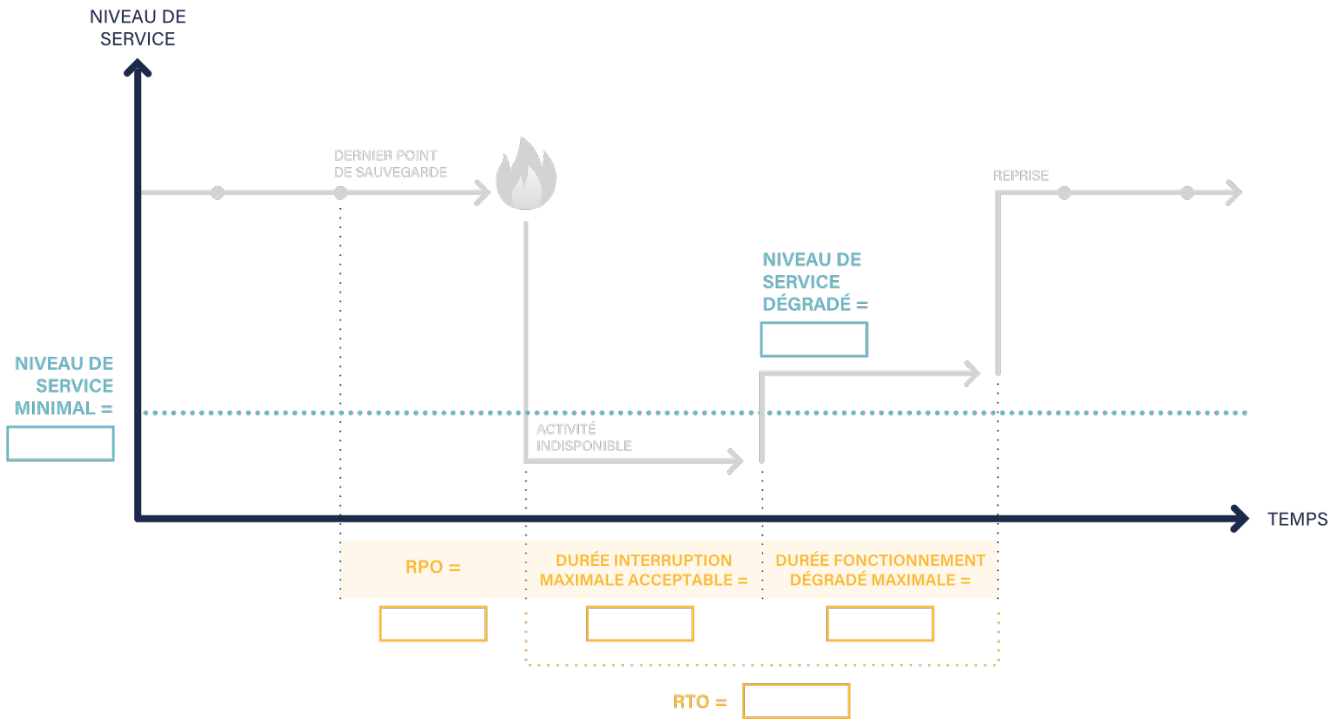
Déroulement du PCA/PRA par élément d'infrastructure

Cette étape se construit à partir des études de l'étape 6.2 et de l'étape 7. Il est désormais temps de réaliser, pour chaque élément de votre infrastructure IT, un schéma de déroulement d'un sinistre en définissant définitivement :

- La fréquence de sauvegarde à partir de la quantité maximale de donnée qu'il est acceptable de perdre (RTO)
- La durée d'interruption maximale acceptable (RPO)
- Le niveau de service minimal
- Le ou les niveaux de service dégradé et leur durée maximale acceptable

Il peut être utile pour les risques à haute probabilité et/ou très critiques de créer un schéma très détaillé avec plusieurs pallier de service dégradé qui correspondent à la remise en marche progressive de chaque éléments IT impacté.

MODÈLE



FICHE 10 Évaluer les ressources nécessaires (1/2)

Choisir les solutions nécessaires à la continuité / reprise

Maintenant que vous avez défini les RTO et RPO, il va falloir identifier les ressources nécessaires pour assurer le respect de ces derniers. Cette étape a pour objectifs de recenser les possibles anticipations et réponses aux risques précédemment identifiés, sans pour le moment se préoccuper de leur coût d'implémentation.

EXEMPLE

Sauvegardes

Utiliser la stratégie 3-2-1, mettre en place un système de sauvegarde sur disque et/ou virtualisé, en local et/ou chez un prestataire (choisir en fonction de flexibilité, la rapidité de relance, ancienneté max des sauvegardes)...

Réseaux et communication

Avoir un moyen de communication non dépendant d'internet en plus des moyens de communication habituels, avoir plusieurs opérateurs, opter pour le SD-WAN...

Redondance

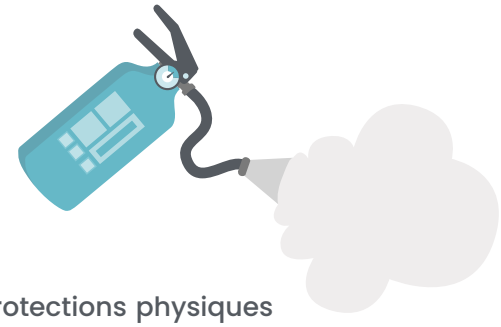
Système de duplication avec site(s) de secours géographiquement éloigné(s), externalisation des sites de secours, Système de réplication synchrone...

Protections logicielles

Bloquer certains sites, équiper l'infrastructure des protections adaptées (anti-virus, antimalware...), utiliser une technologie logicielle de bascule automatisée...

FICHE 10 Évaluer les ressources nécessaires (2/2)

EXEMPLE (suite)



Télétravail

Sélectionner du matériel qui puisse facilement être utilisé en télétravail (ex: ordinateur portable avec station d'accueil), redirection d'appels (VoIP), accès aux données à distance (VPN)...

Protections physiques

Emplacement sécurisé (éviter les sous-sols inondables, porte anti-feu) et sécurisation des accès (porte à code, barreaux aux fenêtres), détecteurs de fumée, extincteurs, disposer d'un générateur...

Stock matériel

Disponibilité de matériel de secours en cas de défaillance, disponibilité de matériel en cas de situation exceptionnelle (ex: boitiers Wi-Fi en cas de télétravail), contrat de remplacement matériel en temps limité chez le prestataire...

Prestataires

Délégation d'une partie de l'infrastructure à des partenaires choisis selon les critères de sécurité et conformité préétablis : niveau de service, engagement de qualité et disponibilité, existence de PCA audité, indemnisation en cas de sinistre...

Equipe IT

Choisir un responsable suppléant, maintenir les certifications des équipes à jour, formations régulières...

FICHE 11 Aborder le PCA PRA avec les tiers

Qui sont les tiers ?

Les tiers regroupent tous les organisations externes dont les services interviennent dans le fonctionnement de votre entreprise. Il peut s'agir :

- De prestataire d'infogérance
- De sous-traitant informatiques
- De prestataire de services (électricité, télécom…)
- De gestionnaires d'activités externes (applications)

Certains partenaires peuvent être critiques pour votre activité (impliqué dans des activités ou processus essentiels), c'est pourquoi il est important de les choisir en fonction de vos exigences de sécurité et les inclure dans votre PCA/PRA. Vous réduisez ainsi le risque que votre entreprise soit la victime collatérale en cas d'incident chez un partenaire.

Impliquer les tiers dans le PCA

Dans la partie audit, vous avez identifié et évalué les risques provenant de vos partenaires. Cela suppose un travail commun avec ces derniers, afin de connaitre les dispositifs prévus par le partenaire à inclure dans le contrat :

- Durée maximale d'interruption d'activité garantie
- Dispositifs mis en place pour assurer un service minimum
- Modalités de fonctionnement en service dégradé

MÉTHODE

	Presta A	Presta B	Presta C
Contacts commerciaux			
Contacts supports			
Modalités de continuités incluses dans le contrat			
Le partage de responsabilité décrit dans le contrat			
Les modalités de leur PCA			

+ Définir les exigences de sécurité pour les prochains contrats

FICHE 12 Estimer le coût d'une interruption

Estimer le coût d'une interruption

Estimer le coût des interruptions d'activité potentielles peut être un argument de poids dans les négociations autour du budget PCA/PRA. Vous pouvez donc calculer une estimation des coûts des risques auxquels l'entreprise devra faire face dans les 5 ans à venir, et comparer cette estimation au coût du PCA/PRA précédemment calculé.

MÉTHODE

Pour chaque menace identifiée, estimez rapidement le temps d'interruption qu'elle pourrait causer sans PCA/PRA, puis calculez :

COÛT D'INTERRUPTION DE LA MENACE EN CAS D'OCCURRENCE =

Perte de CA	= (CA hebdomadaire / 35) x Nombre d'heures d'interruption x % de disponibilité
+ **Perte productivité**	= Salaire horaire moyen x Nombre d'employés x Nombre d'heures d'interruption. Pour plus de précision, le calcul peut être fait par service, car certains seront plus impactés que d'autre par l'arrêt de l'activité
+ **Coûts restauration**	Coût éventuels de remplacement de matériel ou d'intervention d'un technicien si non couvert par le contrat prestataire et/ou les assurances...
+ **Frais indirects**	Coût éventuels pour informer les clients du sinistre et de ses conséquences pour eux, déclaration légale...
+ **Impacts sur l'image**	Perte de clients / contrats. Dépend de l'importance de l'interruption et des services touchés, de la criticité de vos services pour vos clients, de la fréquence des interruptions...

COÛT ESTIMATIF DE LA MENACE SUR 5 ANS =

Coût d'interruption ✖ **Probabilité d'occurrence** sur 5 ans (voir fiche 8.3)

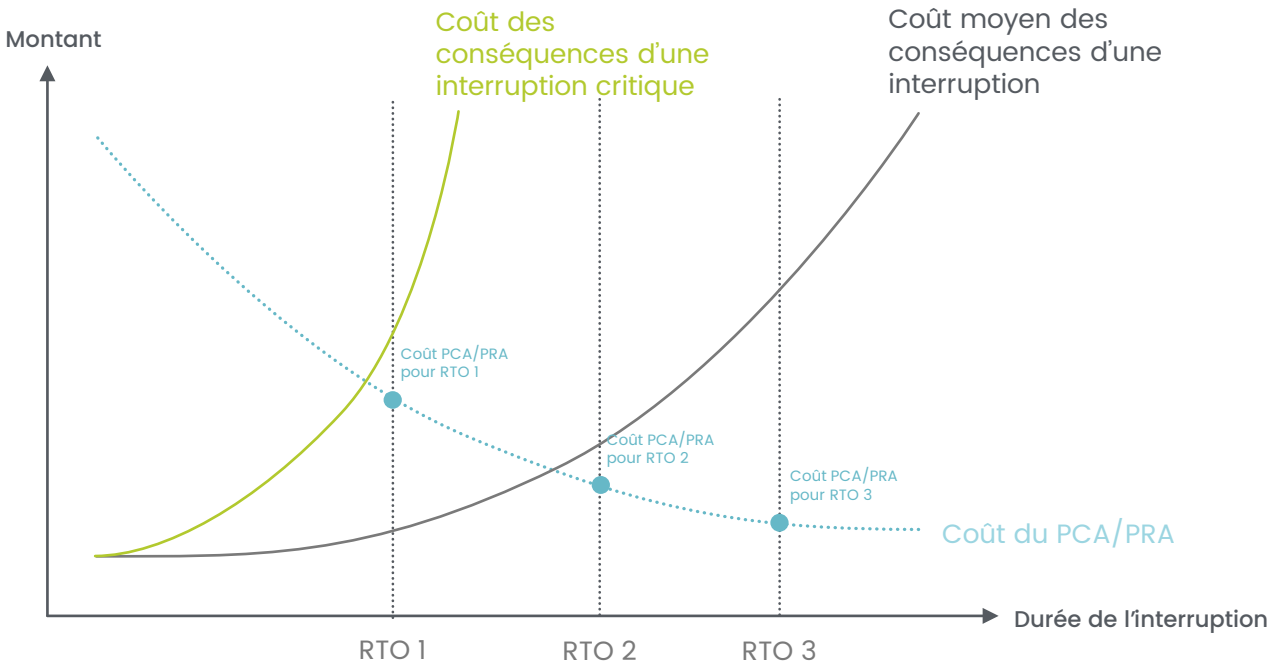
COÛT ESTIMATIF DES RISQUES SUR 5 ANS =

Additionner le coût estimatif sur 5 ans de chaque menace

FICHE 13 Définir le budget du PCA PRA (1/2)

Quel niveau d'exigence ?

La définition du budget est bien évidemment cruciale, et décisionnelle. Il faut savoir trouver l'équilibre entre les risques possibles, les avantages des réponses identifiées et leur coût. Le coût de la réponse doit être inférieur au coût des conséquences de la ou des menaces dont elle est la riposte. C'est votre niveau d'exigence face à la criticité estimée de vos éléments d'infrastructure qui déterminera majoritairement le budget : plus votre exigence est élevée, plus les coûts le seront également.



On peut voir sur le schéma ci-dessus que les exigences de rapidité de reprise vont avoir un impact sur le coût du PCA/PRA. Plus l'interruption dure, plus le coût à payer pour l'entreprise sera élevé. Il serait donc tentant d'établir un plan avec des délais de remise en fonctionnement très courts. Mais un RTO court implique des investissements importants : votre plan vous coûtera donc plus cher. Déterminer les investissements à faire pour votre PCA PRA sont donc une question d'équilibre et d'exigence. Idéalement, le coût du PCA PRA doit être inférieur au coût moyen des conséquences des interruptions (ici, coût pour RTO 2). Mais si votre niveau d'exigence est plus élevé, et que vous ne pouvez tolérer une interruption critique, il faudra opter pour un RTO plus court, et donc un budget plus élevé (ici, coût pour RTO 1)

FICHE 13 Définir le budget du PCA PRA (2/2)

Estimer le coût du PCA/PRA

Dans la partie précédente, vous avez calculé le risque de menace en estimant sa probabilité sur 5 ans (Fiche 8.3). Nous allons réutiliser cette durée pour estimer le coût de notre PCA/PRA, afin de pouvoir ensuite le comparer au coûts risqués d'interruptions.

MÉTHODE

Coûts fixes

	☐		Achat matériels / logiciels
+	☐	X 5	Frais annuels de licences
+	☐	X 5	Frais annuels de stockage Cloud
+	☐		Installation / déploiement
+	☐	(X 5)	Autres

Coûts variables

	☐	X 5	Coût annuel support / gestion
+	☐	X 5	Salaire annuel salarié(s) supplémentaire(s)
+	☐	X 5	Coût annuel formation employés
+	☐	(X 5)	Autres

= ☐ **COÛT ESTIMATIF DU PCA/PRA SUR 5 ANS**

Vous avez précédemment calculé le coût estimatif des risques sur 5 ans, vous pouvez le comparer au coût estimatif du PCA PRA sur 5 ans, et rééquilibrer vos investissements prévus en conséquence.

ANNEXE Fiche de menace

A partir d'ici, il est possible de constituer des fiches récapitulatives concernant chaque menace, ses conséquences directes, les procédures à suivre pour y faire face et les personnes à contacter.

FICHE 14 Impliquer et informer les collaborateurs (1/2)

Impliquer les responsables

Les responsables de chaque service doivent être impliqués du lancement à l'implémentation du PCA/PRA. Le responsable du projet PCA/PRA pourra leur remettre un cahier des charges qui résume leur participation dans la mise en œuvre du nouveau plan (délais de mise en œuvre, embauche, aspects juridiques). Ces derniers devront alors lui faire un retour sur les modalités de mises en œuvre (délais, besoins financiers…) pour consolidation et décisions. Cette dernière étape vous permettra également d'identifier des coûts cachés que vous n'aviez pas anticipé.

Une fois le budget validé et les changements actés, ils devront :

- Adapter les procédures du PCA/PRA à leurs processus
- Informer leurs équipes
- Créer des « fiches d'action » à destination de leur équipe pour formaliser simplement le PCA/PRA et les actions à faire en cas d'incident*
- Remonter régulièrement les problèmes identifiés suite aux changements

*Le PCA/PRA est souvent un document long et complexe, ce qui fait que peu de gens sont réellement au courant des procédures et les appliquent en cas d'incident. Ces fiches permettront à tous d'avoir un document avec des actions simples et claires auxquelles se référer. Ainsi, même si les responsables sont absents / injoignables, les principales procédures seront actionnées, ce qui minimisera les dommages.

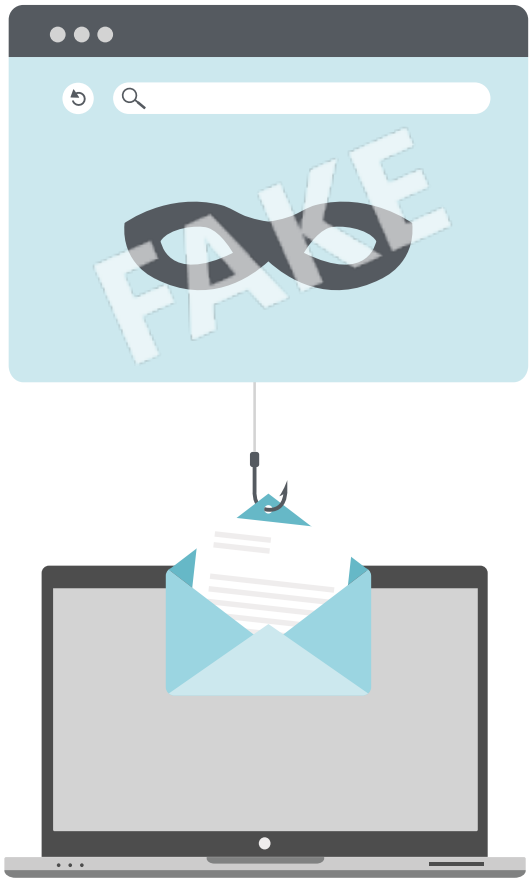
FICHE 14 Impliquer et informer les collaborateurs (2/2)

Impliquer les collaborateurs

Vos collaborateurs auront également un rôle à jouer dans la bonne implémentation du PCA/PRA. Il pourrait être intéressant de faire passer un questionnaire pour identifier les process IT actuels qui ne sont pas respectés, et pourquoi. Car vous pourrez mettre en place un grand nombre de mesures et de processus pour protéger votre infrastructure, s'ils sont trop contraignants pour vos collaborateurs, ces derniers trouveront un moyen de les contourner. Il faut donc s'assurer que vos changements s'intègrent facilement dans la routine des employés : informez-les des changements, sensibilisez-les aux bonnes pratiques (Kit de sensibilisation de www.cybermalveillance.gouv.fr) formez-les aux nouveaux outils et recueillez régulièrement des retours d'utilisation.

Formation et test

Il faudra bien évidemment former l'équipe IT à l'utilisation des nouveaux éléments de l'infrastructure, et éventuellement l'ensemble des collaborateurs (si vous choisissez par exemple de changer une application pour des raisons contractuelles). Au-delà des formations, qui doivent être renouvelées régulièrement, il peut être intéressant de « tester » vos collaborateurs avec par exemple l'envoi un faux email de phishing destiné à évaluer le respect des bonnes pratiques de cybersécurité



FICHE 15 Faire évoluer le plan

Tirer des leçons des incidents

La vie de l'entreprise étant ce qu'elle est, même préparés, certains scénarios ne se dérouleront pas comme prévu : notez les problèmes qui ont entravé le bon déroulé du PCA/PRA et faites évoluer ce dernier en conséquence.

Il est également probable que vous vous retrouviez face à des menaces imprévues : une fois la situation réglée, analysez l'origine de l'incident, les conséquences et les moyens utilisés pour y faire face, et intégrez-les à votre PCA/PRA. Vous aurez éventuellement à faire des modifications sur votre infrastructure pour vous adapter à l'évolution perpétuelle des cybermenaces.

Faire évoluer le plan avec l'infrastructure et la société

Votre entreprise également va évoluer : rachats, fusions, nouveaux sites, nouveaux employés, nouvelles activités, nouvelles technologies… Veillez à réévaluer votre PCA/PRA de temps en temps pour réadapter et/ou redimensionner les réponses définies à l'époque.

Pour s'assurer de la pertinence de votre PCA/PRA, il faudra bien évidemment faire des tests lors de la mise en place pour en vérifier le bon fonctionnement ; mais également des exercices, simulés ou réels, pour tester certains éléments au moins une fois par an. Veuillez également à ce que les dispositifs de secours mis en place soient bien entretenus (ex : extincteurs).

A propos d'Equipages

Equipages est un Intégrateur système réseau et sécurité, qui accompagne ses clients sur l'ensemble de leur infrastructure informatique.

Créé il y a 15 ans, Equipages est né de la conviction que la confiance d'un client se gagne par l'honnêteté et la qualité de son travail. Une expertise technique reconnue et certifiée, que nous mettons en œuvre pour analyser les besoins et environnements de nos clients afin de concevoir des solutions sur mesure.

Nous pouvons mettre à votre disposition notre expertise technique pour vous construire avec vous votre PCA/PRA, vous aider à faire les bons choix de solutions et à les mettre en place.

Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE

EXPERT CYBER LABEL SÉCURITÉ NUMÉRIQUE Cybermalveillance.gouv.fr RÉPUBLIQUE FRANÇAISE

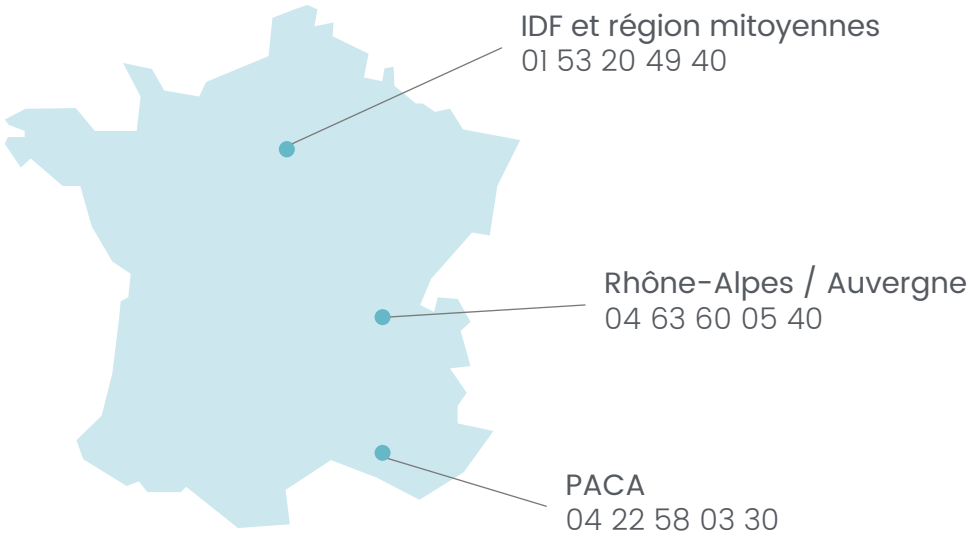
arcep

Retrouvez-nous en ligne

www.equipages.fr

Ou échangez avec nous juste là

commercial@equipages.fr



EQUIPAGES
IT SOLUTIONS