Le plan de reprise d'activité Et plan de continuité d'activité

Yann-Eric DEVARS

Table des matières

Introduction

Dans le contexte actuel, de multiples menaces se profilent et de nouvelles, souvent imprévisibles, peuvent surgir :

- Pannes techniques
- Cyberattaques
- Catastrophes naturelles
- Erreurs humaines
- Crises sanitaires ou logistiques
- Espionnage
- Atteintes à la souveraineté
- Etc. ...

Dans ce cadre, il devient incontournable pour toute organisation de s'assurer qu'elle saura maintenir ou reprendre rapidement ses activités en cas de sinistre majeur.

C'est toute l'ambition du Plan de Reprise d'Activité (PRA), une démarche qui dépasse largement la simple mise en place de sauvegardes informatiques.

Elle exige une connaissance approfondie des processus métiers, une coordination fine entre toutes les parties prenantes (IT, métiers, direction, communication) et une mise à jour permanente pour rester à la hauteur des évolutions du Système d'Information (SI) et des risques émergents.

Dans ce livre, nous allons **explorer** l'ensemble des facettes constitutives d'un PRA robuste :

- **Les fondements** (analyse de risques, définition des objectifs RTO/RPO, inventaire des applications critiques)
- **La mise en œuvre technique** (sauvegardes, réplication, redondance, tests de restauration)
- **L'organisation humaine** et la gouvernance (cellule de crise, rôles et responsabilités, plan de communication)

- **Les tests** et l'amélioration continue (exercices réguliers, audits internes ou externes, retour d'expérience)
- **Les éléments de résilience** élargis, comme la gestion des sites de repli utilisateurs ou la communication de crise
- **La transition** d'un simple PRA IT vers une démarche de **Plan de Continuité d'Activité (PCA)** intégrant la prévention, la logistique, la sécurité et la résilience globale.

Un projet d'entreprise transversal

Tout au long du livre, nous verrons en quoi le PRA est un **projet d'entreprise** à part entière.

Il ne s'agit pas d'un "simple" document rédigé au détour d'une réunion : c'est une démarche qui doit mobiliser à la fois les **équipes techniques** (pour la partie sauvegardes, réplication, infrastructures de secours) et les **équipes métiers** (pour comprendre les processus critiques, définir les modes dégradés, prioriser les actions).

La **direction** doit aussi être impliquée, car la coordination et les décisions en situation de crise requièrent souvent un support managérial et budgétaire important.

Les grandes étapes et les points clés

Nous parcourrons les **grandes étapes** d'élaboration et de maintien d'un PRA, en insistant sur certains **points essentiels** trop souvent négligés :

1. **L'inventaire exhaustif** : recenser applications, dépendances, contrats, prestataires.
2. **Moyens de communication de secours** : lignes téléphoniques d'urgence, messageries alternatives, pour ne pas être pris au dépourvu si le réseau principal est HS.

3. **Sites de repli utilisateurs** : prévoir comment les équipes continueront à travailler si les locaux ou le data center sont inaccessibles (télétravail, autre site, coworking).
4. **Tests de sauvegardes** : s'assurer régulièrement que la restauration est faisable et intégrale.
5. **Plan de crise cyber** : inclure la réaction face à une attaque (isolation, réinstallation "from scratch", communication, etc.).
6. **Formation et sensibilisation** : sans entraînement, le meilleur PRA restera lettre morte au moment critique.

Vers une démarche de continuité globale (PCA)

Au fil des chapitres, nous découvrirons également en quoi le PRA, souvent centré sur la **reprise après sinistre**, peut s'inscrire dans un **Plan de Continuité d'Activité (PCA)** plus vaste.

En intégrant les notions de prévention, de résilience, de gestion logistique, de communication de crise et de hauts niveaux de disponibilité, on dépasse la seule remise en service de l'informatique pour couvrir l'ensemble de la chaîne de valeur et des processus de l'entreprise.

Cette transition vers une **continuité globale** (qui inclut également la prise en compte des risques liés aux fournisseurs, aux ressources humaines, aux infrastructures physiques, etc.) transforme le PRA en un réel **dispositif stratégique**, permettant de réduire considérablement l'impact de toute crise, qu'elle soit technique, humaine ou naturelle.

Un livre pour passer de la théorie à la pratique

Au fil des pages, nous ne nous contenterons pas de discours théoriques : chaque grande section sera illustrée par des **exemples concrets** (scénarios de tests, anecdote de sinistres réels, retours d'expérience), des **méthodes** (check-lists, grilles d'analyse, idées pour structurer la gouvernance), et des **conseils opérationnels** (comment organiser une cellule de crise ?
Comment tester efficacement ses sauvegardes ?
Quels éléments inclure dans la communication de crise ?).

L'objectif est qu'à l'issue de ce livre, vous soyez en mesure :

- De **comprendre** les enjeux et la structure d'un PRA
- De **connaître** les points clés et les bonnes pratiques pour le mettre en place et le maintenir,
- De **préparer** votre organisation, vos équipes, votre SI à faire face à des scénarios de sinistre souvent imprévisibles mais potentiellement dévastateurs
- Et, à terme, de **faire évoluer** votre PRA vers un **PCA** qui embrasse la continuité globale de l'activité, au-delà du seul volet informatique.

Bien plus qu'un manuel sur les sauvegardes et la bascule technique, ce livre vous accompagnera dans **l'aventure** d'un véritable projet d'entreprise, un gage de **résilience** et de **confiance** pour vos collaborateurs, vos partenaires et vos clients.

Au fil des chapitres, vous acquerrez ainsi une vision **complète** de la **mise en place**, du **pilotage** et de la **maintenance** d'un PRA, pour mieux dormir la nuit, en sachant que votre organisation peut rebondir, même face aux crises les plus sévères.

1. Définition du périmètre et analyse de risques

a. Identifier les processus métiers critiques

1. Contexte et objectifs

Dans toute entreprise, il existe un grand nombre de processus opérationnels, administratifs, financiers, logistiques, etc.

Tous ne possèdent pas la même importance en termes de **création de valeur**, de **service au client** ou de **pérennité**.

Quand on se lance dans la définition d'un PRA ou d'un PCA, il est essentiel d'éviter de tout traiter au même niveau de priorité, car cela diluerait l'effort et exigerait des moyens considérables (humains, techniques, budgétaires) qui ne seraient pas toujours justifiés.

L'étape d'**identification des processus métiers critiques** vise donc à focaliser l'attention sur les activités dont l'interruption affecterait gravement l'organisation.

L'impact peut être de différentes natures :

1. **Financier** : perte de revenus directs, indemnités à payer, dégradation du chiffre d'affaires.
2. **Réglementaire ou légal** : non-respect d'obligations légales, sanctions administratives, amendes.
3. **Réputation / Image** : perte de confiance des clients, partenaires, actionnaires, médias.
4. **Sécurité** : risques pour la sécurité des personnes, pour l'intégrité physique des biens, etc.

Souvent, cette étape se déroule de concert avec une **Business Impact Analysis (BIA)**, qui est l'étude méthodique permettant de quantifier et de qualifier les conséquences d'une interruption.

Concrètement, la BIA sert à répondre aux questions suivantes :

- Quels sont les processus métiers sur lesquels repose la continuité de l'entreprise ?
- Quels seraient les impacts financiers, juridiques, d'image, etc. si tel ou tel processus venait à être interrompu pendant X heures, jours ou semaines ?
- Quelles sont les priorités de reprise et de remise en route pour garantir la survie de l'entreprise et la satisfaction des obligations vis-à-vis des clients, fournisseurs, et autorités de tutelle ?

Le présent document vous guidera pas à pas pour **lister**, **classer** et **prioriser** les activités de l'entreprise, tout en articulant cette démarche avec une BIA structurée.

2. Principes clés pour l'identification des processus critiques

2.1. Processus métier : définition et périmètre

Un **processus métier** peut être défini comme un ensemble d'actions ou de tâches corrélées qui, en se succédant ou en s'enchaînant, permettent de produire un résultat contribuant directement ou indirectement à la finalité de l'entreprise.

Chaque processus a :

- Des **objectifs** : livrer un produit, fournir un service, gérer une transaction.
- Des **ressources** (matérielles, humaines, informatiques, financières).

- Des **intrants** (inputs) et des **extrants** (outputs).
- Des **indicateurs de performance** ou de succès (KPI).

On retrouve généralement dans la cartographie d'une organisation divers types de processus :

- **Processus de pilotage / management** (ex. : gouvernance, stratégie, contrôle de gestion).
- **Processus opérationnels** (ex. : production, vente, logistique, approvisionnement).
- **Processus support** (ex. : informatique, ressources humaines, comptabilité, achats).

Parfois, on inclut une catégorie supplémentaire : les **processus de mesure et d'amélioration** (qualité, audit interne, R&D), selon la méthode de cartographie retenue.

2.2. Notion de criticité

La **criticité** d'un processus se détermine en fonction de l'impact potentiel qu'aurait son interruption.

Plus un processus est critique, plus il doit être protégé via des mécanismes de continuité ou de reprise.

Les critères de criticité couramment retenus incluent :

1. **Impact financier** : un processus qui génère une part significative du chiffre d'affaires, ou qui, s'il est à l'arrêt, engendre des pénalités, des pertes de revenus immédiates, ou des remboursements à effectuer.
2. **Impact réglementaire** : un processus soumis à des obligations légales strictes.

Par exemple, la production de certains documents comptables dans des délais imposés par la loi, ou la gestion de données sensibles (RGPD, données bancaires).

3. **Impact sur l'image** : un processus en contact direct avec les clients, partenaires, ou médias, dont l'arrêt prolongé mettrait en danger la confiance que l'écosystème place dans l'organisation.

4. **Impact sur la sécurité** : certains processus relèvent de la sécurité des personnes, des biens, ou de la sûreté des informations (protéger des infrastructures critiques, éviter des accidents, etc.).

Ces quatre catégories d'impact sont fréquemment utilisées dans les matrices de criticité.

D'autres organisations ajoutent des critères complémentaires comme la **complexité de reprise**, la **dépendance vis-à-vis de tiers**, ou encore l'**effet domino** sur d'autres processus.

2.3. Lien avec la BIA (Business Impact Analysis)

La BIA consiste à mesurer, de manière la plus objective possible, l'**amplitude** des conséquences d'une interruption de chaque processus.

On y retrouve souvent deux indicateurs essentiels :

- Le **RTO (Recovery Time Objective)** : temps maximal d'interruption tolérable pour le processus avant que l'impact ne devienne inacceptable.

- Le **RPO (Recovery Point Objective)** : niveau de perte de données tolérable en cas de reprise (ex. : peut-on accepter de perdre 1 heure de transaction ? 24 heures ? 0 ?).

Identifier les **processus métiers critiques** est donc un prérequis à la réalisation d'une BIA complète, qui quantifiera par la suite l'impact au fil du temps.

Toutefois, dans la pratique, l'identification et la BIA sont souvent menées conjointement, afin de **prioriser** plus rapidement et de disposer de chiffres concrets (pertes financières estimées, pénalités, retombées médiatiques, etc.).

3. Étapes détaillées pour l'identification des processus critiques

3.1. Préparation et cadrage

3.1.1. Définir l'équipe projet et les parties prenantes

La première étape consiste à constituer un **groupe de travail** représentant l'ensemble des métiers et services clés de l'entreprise.

Typiquement, on retrouve :

- Des représentants des **fonctions opérationnelles** (production, ventes, logistique, service client, etc.).
- Des représentants des **fonctions supports** (IT, comptabilité, ressources humaines, juridique).
- Un ou plusieurs membres de la **direction** (sponsor ou pilote du projet).
- Souvent, un **RSSI** (Responsable Sécurité des Systèmes d'Information) ou équivalent, qui veille à l'alignement avec les politiques de sécurité et de conformité.
- Un **coordinateur** ou **chef de projet** PRA / PCA.

Cette équipe doit être légitimée par la direction pour pouvoir recueillir les informations nécessaires dans tous les départements, et éventuellement demander la mise à disposition de données sensibles (ex. chiffres de revenus, volumes de transaction, etc.).

3.1.2. Définir les objectifs et le périmètre de l'analyse

Avant d'entrer dans le vif du sujet, il est nécessaire de bien déterminer **jusqu'où** va s'étendre l'analyse.

Parfois, on se limite à un **périmètre** : l'ensemble du siège social, un pôle d'activité précis, ou la totalité des filiales dans un pays.

Dans d'autres cas, on veut cartographier l'ensemble du groupe, y compris les entités internationales.

Plus le périmètre est vaste, plus la complexité et la durée de l'exercice augmentent.

Il est donc possible de procéder **progressivement**, par lots ou par priorités géographiques et organisationnelles.

L'**objectif** principal : identifier de façon exhaustive les **processus métiers** et **évaluer leur criticité**.

Cela suppose :

- De définir une **grille de criticité** (financier, réglementaire, image, etc.) et un système de score ou de notation.
- De recueillir des informations quantitatives (chiffres d'affaires, volumes de transaction) et qualitatives (obligations légales, exigence client, etc.).
- D'arriver à une **priorisation** claire (niveau 1, 2, 3 ou haute / moyenne / faible criticité).

3.2. Recensement des processus métiers

3.2.1. Inventaire initial

La deuxième étape opérationnelle est de dresser un **inventaire** des processus métiers existants.

De nombreuses organisations ont déjà une **cartographie** plus ou moins formelle de leurs processus, parfois dans le cadre d'une démarche qualité (ISO 9001, par exemple) ou de transformation digitale.

Si ce n'est pas le cas, il peut être nécessaire de mener une série d'**ateliers** ou d'entretiens avec les équipes pour :

1. **Lister** les missions principales de chaque département (Ex. : "Le service RH gère le recrutement, la paie, la formation, la gestion des compétences, etc.").
2. **Décomposer** ces missions en sous-processus (Ex. : "Le recrutement inclut la publication d'offres, la réception de candidatures, la sélection, l'entretien, la contractualisation…").
3. **Identifier** les ressources impliquées (logiciels, bases de données, données critiques, acteurs internes ou externes).

Le niveau de détail souhaité dépend de l'envergure du PRA.

Pour certains, il suffit de rester à un niveau macro (ex. "Recrutement global").

Pour d'autres, il peut être nécessaire de descendre plus finement (ex. "Recrutement cadre dirigeant" vs "Recrutement employé" si les enjeux et les procédures diffèrent radicalement).

3.2.2. Validation transversale

Une fois l'inventaire dressé, il est pertinent de le faire **valider** par les différentes parties prenantes afin de s'assurer que **rien n'a été oublié**.

Les oublis les plus fréquents concernent :

- Les processus support, jugés parfois “moins visibles” (gestion des bâtiments, sécurité physique, archivage documentaire).
- Les processus réalisés uniquement dans certaines filiales ou unités (une usine ou un laboratoire isolé).
- Les processus externalisés chez des **prestataires** ou des **fournisseurs critiques** (transport logistique, infogérance, etc.).

Il est essentiel d’intégrer ces processus externalisés, car leur indisponibilité peut bloquer le fonctionnement global de l’entreprise (pas de livraison, pas de support IT, etc.).

Dans le cadre d’un PRA, on devra également évaluer comment ces partenaires assurent leur propre continuité.

Mais d’abord, il faut les lister comme faisant partie intégrante de la chaîne de valeur.

3.3. Définir la grille d’évaluation et les critères de criticité

3.3.1. Choisir les critères

Pour classer et prioriser, on détermine une **grille de critères** qui reflète la réalité des risques encourus.

Par exemple :

1. **Impact financier** :
    - 1 = moins de 5 000€ de pertes / jour
    - 2 = entre 5 000€ et 50 000€ de pertes / jour,
    - 3 = plus de 50 000€ de pertes / jour.
2. **Impact réglementaire** :

- 1 = risque faible (simple non-conformité interne)
- 2 = contravention modérée (remontrances, avertissements)
- 3 = risque d'amende lourde ou de suspension d'agrément.

3. **Impact sur l'image** :
   - 1 = impact interne ou restreint (incidents gérables en interne)
   - 2 = impact modéré (clients mécontents, presse spécialisée)
   - 3 = impact majeur (médias nationaux, atteinte grave à la réputation).
4. **Impact sur la sécurité / la survie de l'organisation** (optionnel selon les secteurs) :
   - 1 = problème interne qui n'affecte pas la sûreté
   - 2 = mise en danger d'une partie du personnel
   - 3 = mise en danger grave des personnes ou de l'infrastructure.

On peut aussi intégrer d'autres éléments, comme **l'effort** ou la **complexité de remise en route**, si on veut une vue plus large.

Toutefois, il est souvent préférable de se limiter à un **faible nombre de critères** (3 à 5) pour conserver la lisibilité et éviter les surcharges d'évaluation.

3.3.2. Pondération et score

Une fois les critères définis, l'entreprise peut décider de **pondérer** certains critères davantage que d'autres (ex. : si le risque légal est un enjeu primordial, on peut lui donner un coefficient plus élevé).

Cela se formalise par l'attribution de coefficients, par exemple :

- Impact financier : coefficient 2
- Impact réglementaire : coefficient 3
- Impact image : coefficient 2
- Impact sécurité : coefficient 1

Ainsi, un processus ayant un fort impact réglementaire obtiendra un score global supérieur à un processus ayant un fort impact financier mais un impact réglementaire faible.

Le système de pondération doit être validé par la direction générale, afin de refléter les **priorités stratégiques** de l'entreprise.

On peut utiliser une **matrice** ou un **tableur** pour agréger les notations de chaque critère.

Par exemple :

Processus	**Impact Financier (max 3)**	**Impact Règle (max 3)**	**Impact Image (max 3)**	**Pondération F=2, R=3, I=2**	**Score total**
Processus A	3	2	2	(3x2) + (2x3) + (2x2) = 6+6+4 = 16	16
Processus B	1	3	3	(1x2) + (3x3) + (3x2) = 2+9+6 = 17	17

Processus	Impact Financier (max 3)	Impact Règle (max 3)	Impact Image (max 3)	Pondération F=2, R=3, I=2	Score total
Processus C	2	2	1	(2x2) + (2x3) + (1x2) = 4+6+2 = 12	12

Le score total permet alors de **classer** rapidement les processus.

3.4. Récolter les informations et réaliser les évaluations

3.4.1. Entretiens et ateliers métiers

Pour chaque processus identifié, il convient de remplir la grille de notation.

Cela se fait en général par :

- Des **entretiens** individuels avec les responsables de processus ou les opérationnels clés
- Des **ateliers** collectifs où l'on discute de l'impact probable en cas d'arrêt.

Il est important de bien **objectiver** l'évaluation, en se basant sur des données tangibles (ex. volumes de ventes journalières, coût d'un retard d'approvisionnement, montant d'amende possible).

La tendance naturelle de chaque département est parfois de **sur octroyer** de l'importance à ses propres processus.

L'animateur du PRA doit donc **challenger** les réponses avec diplomatie, et éventuellement recouper les données auprès d'autres services (comptabilité, direction financière, direction juridique).

3.4.2. Synthèse des résultats

À l'issue de ces ateliers, on dispose d'un **tableur** (ou d'un outil dédié) où figurent tous les processus, notés selon les critères retenus.

On effectue ensuite le **calcul du score** global et on obtient un classement du plus critique au moins critique.

Ce classement constitue une **base de discussion** pour la phase de validation.

3.5. Validation et arbitrage

3.5.1. Comité de validation

Les résultats de l'analyse sont présentés à un **comité** (souvent le comité de pilotage du PRA, ou un comité de direction élargi) pour arbitrer sur la **hiérarchisation**.

Il peut arriver que la direction décide de **modifier le classement** en tenant compte de facteurs stratégiques qui n'apparaissaient pas clairement dans la grille (ex. un projet d'acquisition, un contrat majeur à venir, une dépendance à un partenaire sensible).

Les enjeux politiques et budgétaires entrent également en ligne de compte.

3.5.2. Catégoriser les processus critiques

Au final, il est courant de regrouper les processus en **3 niveaux** de criticité, par exemple :

- **Critique (Niveau 1)** : arrêt supérieur à X heures ou jours provoquant un impact majeur.

Le PRA doit couvrir la reprise ou la continuité en priorité absolue.

- **Important (Niveau 2)** : interruption plus longue tolérable, mais qui reste à encadrer dans un dispositif de reprise moins exigeant.
- **Secondaire (Niveau 3)** : peut être interrompu plusieurs jours sans impact insurmontable.

  La priorité de reprise est faible.

Cette catégorisation rend l'analyse plus **lisible** et facilite la préparation de la suite (BIA détaillée, définition des RTO/RPO, allocation de ressources techniques de secours, etc.).

4. Couplage avec la BIA (Business Impact Analysis)

Bien que l'on présente souvent l'"identification des processus critiques" comme une étape préalable à la BIA, dans la réalité, ces deux exercices s'imbriquent et se **nourrissent mutuellement**.

Voici comment :

1. **Pré-BIA** : on dresse une première liste de processus, on fait une évaluation approximative de leur impact, on obtient un classement provisoire.
2. **BIA détaillée** : pour les processus jugés "critiques" ou "importants", on mène une analyse plus poussée (chiffrage des pertes financières par heure/jour, estimation de la perte de clients potentielle, évaluation du délai légal maximum, etc.).
3. **Finalisation** : on consolide la classification en fonction des résultats chiffrés de la BIA.

   On peut alors affiner ou réviser la hiérarchie.

La BIA va généralement produire plusieurs livrables :

- Une **courbe d'impact dans le temps** : qui montre l'évolution des pertes ou de l'impact en fonction de la durée de l'interruption (p. ex. : "20k€ de perte après 24h, 100k€ après 72h, 500k€ après 5 jours").
- Les **RTO** (Recovery Time Objectives) et **RPO** (Recovery Point Objectives) cibles : c'est-à-dire le temps maximal d'arrêt toléré et la quantité de données (ou transactions) que l'on peut se permettre de perdre.
- Un **plan de priorisation** : quels processus/doit-on relancer en premier, en second, etc., lors d'un incident majeur.

Ainsi, la démarche BIA est très complémentaire et renforce la robustesse du classement des processus critiques.

5. Cas particuliers et pièges à éviter

5.1. Surévaluation systématique

Comme évoqué, chaque service ou département peut être tenté de "gonfler" l'importance de son activité pour obtenir plus de garanties, de budgets, ou de ressources dédiées dans le cadre du PRA.

Pour éviter cela :

- S'appuyer sur des **données financières** et des **exemples concrets** (p. ex. : "tel jour, quand on a eu une panne de 2 heures, on a perdu X milliers d'euros de ventes").
- Impliquer la **direction** pour trancher les débats trop subjectifs.

5.2. Sous-estimation des processus support

Les processus support (IT, RH, maintenance, etc.) peuvent être mal évalués si l'on ne se rend pas compte de leur **effet domino**.

Par exemple :

- L'indisponibilité du service paie peut entraîner un conflit social si les salaires ne sont pas versés.
- L'arrêt de la fonction achat peut bloquer les matières premières nécessaires à la production.
- La coupure du réseau informatique impacte l'ensemble des activités.

Il est donc primordial de **cartographier** convenablement ces processus pour leur attribuer un **niveau de criticité** adapté.

5.3. Oubli des dépendances externes

Les fournisseurs, sous-traitants et partenaires peuvent être autant de maillons faibles.

Si un transporteur critique tombe en panne, si un hébergeur cloud subit un incident, le processus métier peut cesser de fonctionner même si tout va bien en interne. Il faut donc :

- Lister les **prestataires essentiels**.
- Vérifier leurs engagements contractuels (SLA).
- Évaluer leur plan de continuité propre.

5.4. Manque de validation sur le terrain

Une erreur fréquente est de faire cette analyse "en chambre" ou en comité restreint.

On obtient alors un résultat trop théorique, déconnecté des réalités du terrain.

Il est indispensable de **valider** l'identification des processus métiers critiques en allant questionner les **collaborateurs opérationnels**, ceux qui réalisent concrètement les tâches, pour vérifier la faisabilité, l'utilité, et la pertinence de l'évaluation réalisée.

6. Documentation et formalisation des résultats

Une fois la démarche achevée, il est essentiel de produire un **document** (ou un ensemble de documents) clair et pérenne, par exemple :

1. **Cartographie des processus** : présentation visuelle (diagrammes, tableaux) illustrant la structure globale de l'entreprise, les liens entre processus, et leur importance relative.
2. **Liste des processus et note de criticité** : un listage exhaustif ou un tableur, avec pour chaque processus :
    - Nom et description
    - Responsable / propriétaire
    - Critères de criticité (financier, réglementaire, image…)
    - Niveau de criticité final (ex. : 1, 2 ou 3)
    - RTO/RPO (si déjà défini ou estimé).
3. **Document de synthèse** destiné à la direction : résumant l'essentiel (top 5 ou 10 processus les plus critiques, budget nécessaire, risques majeurs).

Cette **documentation** doit être facilement accessible et mise à jour au fur et à mesure que l'entreprise évolue.

Les processus ne sont pas figés, de nouveaux produits peuvent apparaître, des anciens disparaître, les priorités stratégiques peuvent changer.

Il est donc important de prévoir un **mécanisme de mise à jour** (généralement annuel ou bi-annuel), assorti de revues ad hoc lors de changements majeurs (acquisition, fusion, lancement d'une nouvelle offre, etc.).

7. Prochaines étapes après l'identification des processus critiques

L'identification et la classification ne sont qu'un **prélude** au déploiement d'un PRA / PCA complet.

Une fois le panorama des processus critiques établi :

1. **Réaliser la BIA approfondie** (si ce n'est pas déjà fait en parallèle) pour chaque processus de niveau 1 et 2, afin de chiffrer précisément les coûts d'interruption.
2. Définir les **stratégies de continuité ou de reprise** : haute disponibilité, redondances, plan de sauvegarde et restauration, sites de secours, etc.
3. Rédiger un **Plan de Reprise d'Activité** ou un **Plan de Continuité** adapté, précisant les procédures de crise, les ressources techniques, humaines, et logistiques nécessaires.
4. **Tester** régulièrement le plan : exercices de simulation, tests de restauration, etc.
5. **Maintenir** et **faire évoluer** le PRA / PCA en continu, via une gouvernance structurée et des audits internes/externes.

8. Exemple illustratif

Pour rendre plus concret le processus, imaginons une PME fictive spécialisée dans la logistique e-commerce.

Elle a plusieurs grands processus :

- **Prise de commande** : reçoit les commandes clients via une interface web, traite les paiements.
- **Préparation de commande** : picking, emballage, étiquetage.
- **Expédition** : gestion des transporteurs, suivi des colis.
- **Service client** : gestion des réclamations, retours, demandes d'information.
- **Ressources humaines** : paie, gestion du personnel.
- **Comptabilité / facturation** : envoi des factures, gestion des règlements.
- **Informatique** : maintenance des serveurs, réseaux et applications.

En menant l'analyse, on constate :

- La **prise de commande** et **l'expédition** sont extrêmement critiques : si elles s'arrêtent, l'entreprise ne peut plus fonctionner, le CA chute immédiatement.

  Les retards de livraison provoquent la colère des clients et la perte de contrats.
- Le **service client** est jugé "important" (critique niveau 2) : il peut être stoppé quelques heures, mais pas trop longtemps, sinon l'image de la société se dégrade.

- La **comptabilité** est de niveau 2 ou 3, car un arrêt de quelques jours est gérable en mode dégradé (facturation manuelle, ou en différé), même si ce n'est pas idéal.
- La **paie** (RH) est essentielle à la satisfaction du personnel, mais un décalage de quelques jours est parfois envisageable.

  Cela reste toutefois un processus ayant un fort enjeu social et réglementaire.
- L'**informatique** est à la fois un processus support, mais crucial, car si l'infrastructure IT est à l'arrêt, tous les autres processus sont bloqués.

  Il sera donc classé au plus haut degré de criticité (niveau 1).

Au terme de cette évaluation, l'entreprise sait qu'elle doit en priorité protéger ses systèmes de prise de commande et de suivi des expéditions, ainsi que la base de données logistique.

Les ressources (budgets, plans de secours, personnel formé) seront prioritairement affectées pour assurer la reprise rapide de ces processus.

9. Conclusion et synthèse

Identifier les processus métiers critiques est la fondation sur laquelle repose tout **Plan de Reprise** ou **Plan de Continuité d'Activité**.

Cette démarche :

1. **Dresse la cartographie** des processus clés de l'organisation.
2. **Hiérarchise** leur importance et leur sensibilité (financière, réglementaire, réputationnelle, etc.).

3. **Prépare la voie** à une analyse plus détaillée des impacts (BIA) et à la définition d'objectifs de reprise (RTO, RPO).
4. **Guide la priorisation** dans la mise en place des solutions techniques et organisationnelles de secours.
5. Permet de **focaliser les moyens** (humains, financiers, technologiques) sur les activités dont la survie est réellement cruciale pour l'entreprise.

Le succès de cette étape tient à une **implication forte** de la direction, à la **collaboration** de tous les métiers, à la **cohérence** entre l'évaluation théorique et la réalité du terrain, ainsi qu'à la **transparence** des données (chiffre d'affaires, coûts, risques légaux).

Le résultat final doit être un **référentiel** clair de processus critiques, régulièrement **mis à jour** et validé, pour que, le jour où un incident majeur survient, l'entreprise sache **précisément** vers quoi concentrer ses efforts de reprise et de continuité.

Cette identification constitue la **pierre angulaire** d'un dispositif de résilience.

Sans une bonne connaissance de ses priorités, l'entreprise risque de s'éparpiller, de gaspiller des ressources et, en situation de crise, de **perdre un temps précieux** à tenter de redémarrer ce qui n'est pas essentiel.

À l'inverse, en ayant une **vision claire** de ses processus critiques, elle peut réagir rapidement, mobiliser les ressources adéquates et **limiter les dommages** (financiers, juridiques, médiatiques).

Ainsi, la première brique posée (l'identification des processus critiques) va donner du sens et de l'efficacité à l'ensemble du projet PRA/PCA, qui vise in fine à assurer la continuité du service rendu aux clients et la survie de l'entreprise, même dans les situations les plus difficiles.

b. Analyser les risques et menaces

1. Contexte et enjeux

Dans la démarche globale d'élaboration d'un Plan de Reprise d'Activité (PRA) ou d'un Plan de Continuité d'Activité (PCA), on cherche à protéger l'entreprise contre les **interruptions majeures** susceptibles de mettre en péril sa pérennité, ses finances, son image ou encore sa conformité réglementaire.

Pour ce faire, il est indispensable de disposer d'une **vision claire** des différents types de risques qui pourraient provoquer :

- Un **arrêt total** ou **partiel** des opérations,
- Une **indisponibilité** de systèmes informatiques,
- Une **mise en danger** de la sécurité physique des locaux,
- Une **rupture** dans la chaîne logistique ou la fourniture de services.

L'analyse des risques et menaces consiste à **déterminer** les scénarios dans lesquels un sinistre se produirait (panne, cyberattaque, incendie, etc.), puis à **estimer** pour chacun la **probabilité** de survenue et l'**impact** potentiel sur l'entreprise.

Cette étape nourrit plusieurs objectifs :

1. **Hiérarchiser** les scénarios de sinistre par ordre de priorité, afin de ne pas tout traiter au même niveau.
2. **Dimensionner** les politiques de gestion et de prévention (sécurité informatique, dispositifs anti-incendie, redondances, etc.) en fonction de la criticité.
3. **Préparer** les procédures de reprise pour les situations les plus probables et/ou les plus dangereuses.

4. **Sensibiliser** les équipes dirigeantes et opérationnelles à la réalité des menaces et à la nécessité de mesures adaptées.

La réalisation d'une telle analyse peut relever de différentes méthodologies de gestion des risques, parmi lesquelles on peut citer l'approche ISO 31000, l'EBIOS (pour la sécurité informatique, en France), ou encore des standards propres à certains secteurs (ex. : NIST pour la cybersécurité aux États-Unis).

L'important est d'avoir une **démarche structurée** pour :

- Recenser les menaces,
- Les décrire,
- Les évaluer (probabilité, impact),
- Les cartographier pour en extraire une **priorisation**.

2. Principes généraux de l'analyse des risques

2.1. Terminologie

- **Menace** : événement redouté susceptible de survenir (ex. : incendie, panne réseau, intrusion, etc.).
- **Vulnérabilité** : faiblesse ou lacune dans les dispositifs de protection ou les processus, qui peut être exploitée par une menace ou amplifier ses conséquences.
- **Probabilité (ou vraisemblance)** : chance que l'événement se produise dans un laps de temps donné (par an, par semestre, etc.).
- **Impact (ou gravité)** : conséquences néfastes de l'événement s'il survient (pouvant être financières, réglementaires, réputationnelles, etc.).