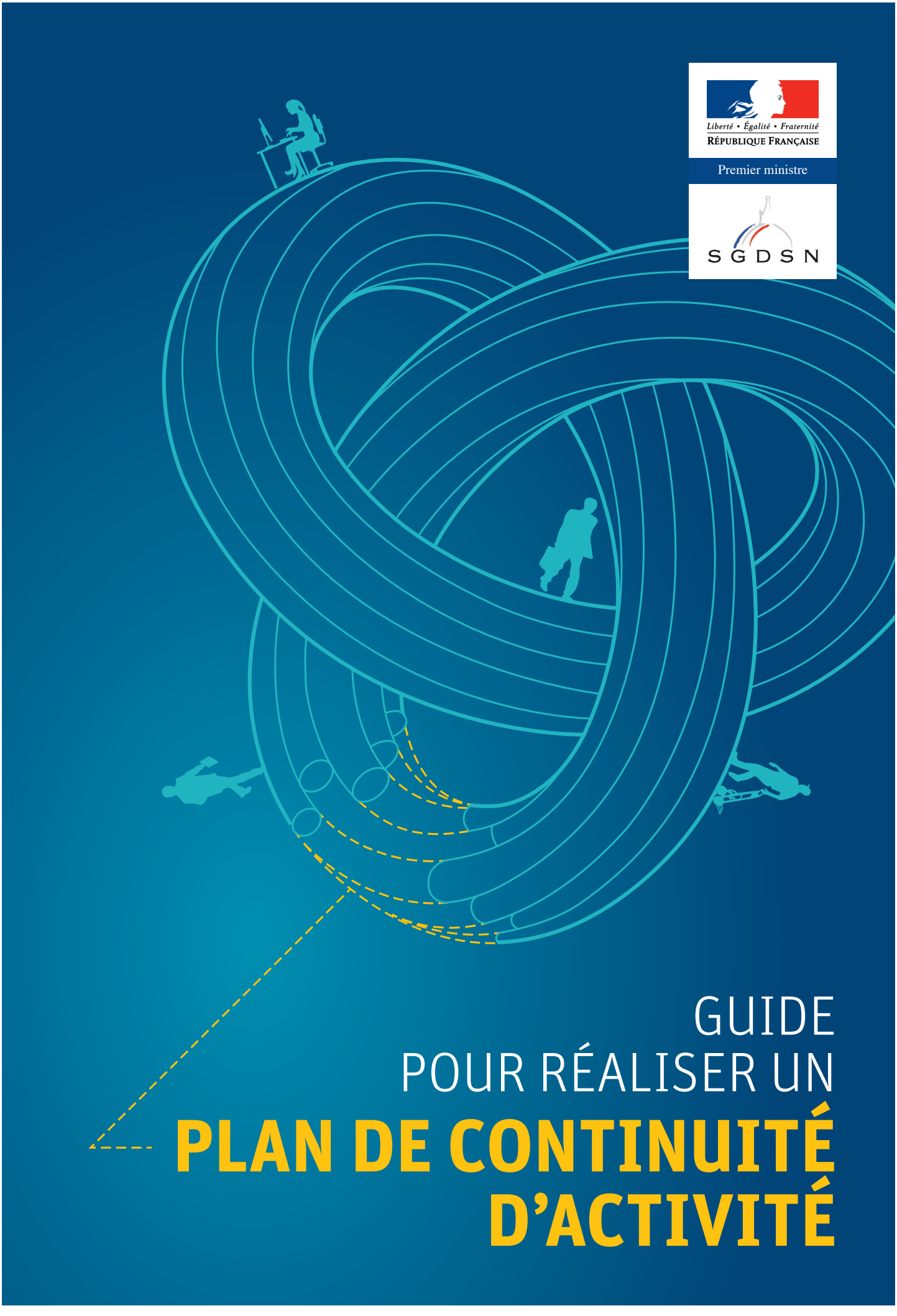
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN



# GUIDE POUR RÉALISER UN PLAN DE CONTINUITÉ D'ACTIVITÉ

Édition 2013

**CONCEPTION** / Secrétariat général de la défense et de la sécurité nationale
Remerciement à ACCESS2S - Alain Coursaget
**RÉALISATION GRAPHIQUE** / EFIL 02 47 47 03 20 / www.efil.fr

# LA DÉMARCHE PRÉSENTÉE PAR ÉTAPES

## 1 POURQUOI ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?



## 2 COMMENT ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

## 3 LES FICHES PRATIQUES

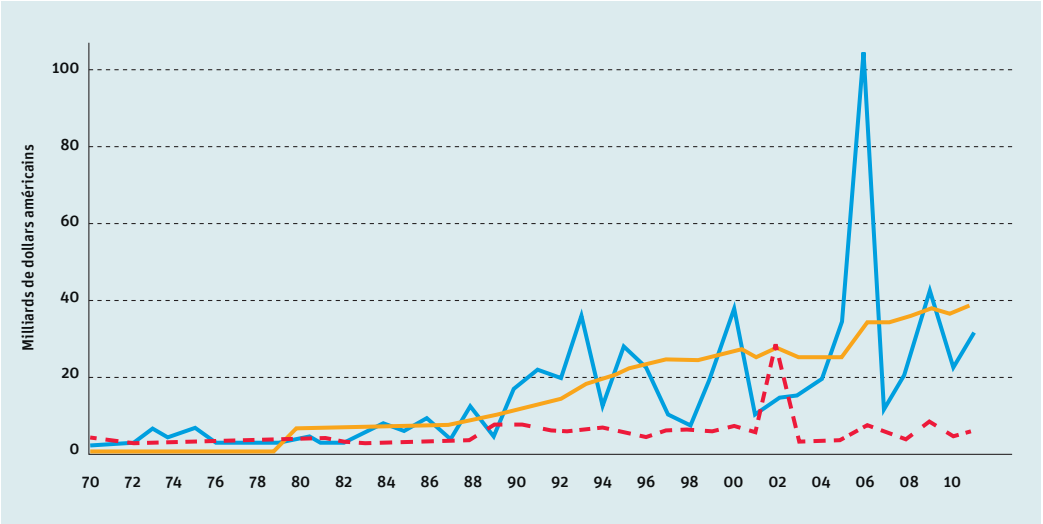


## 4 LES ANNEXES

# 1 POURQUOI ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

## 1.1 QUELQUES BONNES RAISONS D'ENTREPRENDRE UNE DÉMARCHE DE CONTINUITÉ D'ACTIVITÉ

**PRINCIPAUX CHOCS MONDIAUX**




Pertes dues aux catastrophes mondiales 1970-2010 (Source : Swiss Re, Guy Carpenter & Company LLC).

➡ La nature, la fréquence et le coût des crises ont sensiblement évolué au cours des vingt dernières années. On comprend sans doute mieux aujourd'hui à quel point sont étroitement imbriquées les différentes dimensions de ces événements qui perturbent très fortement le fonctionnement de nombreuses organisations, publiques et privées, avec des conséquences allant jusqu'à la cessation définitive d'activité. Les retours d'expérience des grandes crises récentes montrent que les organisations ayant entrepris une démarche préalable visant à garantir la continuité de leur activité sont les plus résilientes face aux événements déstabilisants.

➡ Bien qu'il soit utopique de chercher à tout prévoir et maîtriser, le responsable d'une organisation – publique ou privée – se doit de concevoir et mettre en œuvre des stratégies de protection permettant d'éviter certains événements, ou tout du moins d'en limiter

les effets directs sur les objectifs de l'organisation, et d'assurer la continuité d'activité malgré la perte de ressources critiques. Cet impératif conditionne la situation financière de l'organisation, son image dans la société et naturellement la responsabilité personnelle du dirigeant. Les établissements de crédit, les entreprises d'investissement, les établissements de santé, les opérateurs d'importance vitale doivent déjà répondre à l'obligation légale de plan de continuité d'activité.

➡ Les contraintes économiques imposent de devoir justifier les dépenses - y compris celles qui concernent les actions à entreprendre dans le domaine de la sécurité - et de pouvoir prioriser ces dépenses dans le cadre d'une stratégie globale. Il faut par conséquent disposer d'outils méthodologiques permettant d'optimiser l'efficience de ces actions, en cohérence avec les objectifs de l'organisation. Des outils existent déjà pour couvrir séparément plusieurs domaines indissociables : la gestion de risque, la gestion de crise, l'intervention, le maintien et la reprise d'activité. La démarche de continuité d'activité est le moyen d'associer de manière globale et cohérente tous ces domaines.

## 1.2 QU'EST-CE QU'UN PCA ?

La gestion de la continuité d'activité est définie[1] comme un « processus de management holistique qui identifie les menaces potentielles pour une organisation, ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation, avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs».

Un plan de continuité d'activité (PCA) a par conséquent pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une organisation la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il doit permettre à l'organisation de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image…) et de tenir ses objectifs.

Le règlement n° 97-02 du Comité de la réglementation bancaire et financière du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement donne la définition suivante : **le PCA représente l'ensemble des mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services ou d'autres tâches opérationnelles essentielles ou importantes de l'entreprise, puis la reprise planifiée des activités.**

1 / Définition de la norme ISO 22301 : 2012(F).

## 1.3 L'AMBITION DE CE GUIDE

**La démarche méthodologique permettant l'élaboration concrète d'un PCA est l'objet principal de ce guide destiné aux organismes relevant de l'État, aux collectivités territoriales ainsi qu'aux entreprises.**
Une fois élaboré, le PCA regroupe les procédures documentées qui vont servir de guide à l'organisation afin de lui permettre de répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation importante.

Le guide a également pour ambition de faciliter une telle démarche, par la délivrance de conseils méthodologiques et la diffusion de bonnes pratiques. Dans une perspective concurrentielle, il peut aussi constituer une aide à la préparation d'un éventuel projet de certification.

Présentant brièvement le rôle des services de l'État en appui des acteurs de la société civile, le document fait régulièrement référence à un vocabulaire normalisé qui contribue à faciliter le dialogue entre les organisations, notamment dans leurs relations clients/fournisseurs, afin de limiter les effets en cascade. Sa publication par le SGDSN vise ainsi à mettre en cohérence les différentes approches et documentations existantes, dans le cadre d'une démarche qui amène le secteur public et le secteur privé à renforcer la résilience nationale de manière complémentaire.

Le guide est scindé en deux parties.
La première contient les informations permettant de donner au lecteur une vision synthétique et globale de l'approche méthodologique qu'il convient de suivre afin de mener une démarche de continuité et de rétablissement d'activité en cohérence avec les normes existantes.

La seconde partie du guide est constituée de fiches pratiques qui décrivent de manière détaillée les étapes et modalités d'élaboration et de maintenance d'un plan de continuité d'activité. Ces fiches d'approfondissement visent à faciliter l'appropriation de la méthode et des bonnes pratiques en aidant leur transposition dans le contexte spécifique à chaque organisation.

Enfin, des annexes fournissent un lexique de terminologie normalisée, des références, des exemples et des fiches modèles.

# 2 COMMENT ÉLABORER UN PLAN DE CONTINUITÉ D'ACTIVITÉ ?

## 2.1 CONTENU DU PCA

**Le PCA décrit la stratégie de continuité adoptée pour faire face, par ordre de priorité, à des risques identifiés et sériés selon la gravité de leurs effets et leur plausibilité.** Il décline cette stratégie en termes de ressources et de procédures documentées qui vont servir de références pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini, lorsque celui-ci a été interrompu à la suite d'une perturbation importante.

Un PCA est nécessairement un plan évolutif car les priorités de l'organisation évoluent avec les modifications d'objectifs, d'obligations contractuelles ou réglementaires, de relations avec des partenaires externes (fournisseurs ou clients) et d'appréciation du risque. Il doit être revu régulièrement pour tenir compte de l'évolution de ces paramètres.

Toute personne en charge d'une action relevant d'un PCA doit connaître précisément son rôle et ce qu'elle doit faire concrètement en cas de sinistre. Elle doit également comprendre la finalité recherchée, afin d'inscrire son action dans la cohérence globale de l'organisation. Cet impératif est un gage de flexibilité et d'efficacité.

Il résulte des points précédents que la documentation du PCA doit faciliter **l'adhésion** des personnes concernées, **l'adaptabilité** des mesures à la situation et **l'évolutivité** du plan dans le temps, en incluant une description du contexte, des scénarios de risque retenus et de la stratégie de réponse.

**Il est par conséquent recommandé que le contenu du PCA comprenne les points suivants, qui doivent être élaborés successivement :**

➡ **Le contexte**, les objectifs et obligations de l'organisation, dont la description se prolonge logiquement par la liste des activités essentielles pour l'atteinte des objectifs et la tenue des obligations, ainsi que par la liste des processus clés, nécessaires au fonctionnement des activités essentielles.

➡ **Les risques retenus comme les plus graves** pour la continuité d'activité doivent être clairement explicités au moyen de scénarios. Comme on le verra plus loin, il est fortement recommandé de conduire une analyse complète des risques, de façon à disposer d'une grille d'évaluation et de critères objectifs pour décider des priorités. Néanmoins, en l'absence d'une démarche de gestion des risques, une approche par scénarios (par exemple une crue, une pandémie grippale, la destruction d'un site), focalisée sur les conséquences sans décrire les causes, peut suffire à élaborer une première version de PCA simplifié.

➡ **La stratégie de continuité d'activité**, établie et décrite en précisant, pour chaque activité essentielle, les niveaux de service retenus et les durées d'interruption maximales admissibles pour ces différents niveaux de service, ainsi que les ressources et procédures permettant d'atteindre les objectifs, en tenant compte des ressources critiques qui peuvent avoir été perdues, jusqu'à la reprise de la situation normale.

➡ **Le rôle des différents responsables**, les procédures de mise en œuvre du PCA et les moyens nécessaires doivent être explicités. Les dispositifs préconisés, une fois intégrés dans les moyens et procédures de l'organisation, doivent être précisés et documentés.

➡ **Le dispositif de gestion de crise**, qui permet de conduire la mise en œuvre du PCA en assurant le pilotage des actions de réponse et de gestion de l'incertitude, à travers les procédures de détection d'incident, de qualification, d'escalade, d'alerte, de mobilisation, d'activation de la cellule de crise, d'anticipation, d'intervention, de déclenchement des dispositions du PCA (solution palliative, mode secours avec fonctionnement dégradé, plan de reprise de l'activité normale) et de communication.

➡ **La maintenance opérationnelle du plan.**
Cette action essentielle consiste en premier lieu à établir des indicateurs permettant de vérifier et mesurer :
- La bonne mise en œuvre des dispositifs préconisés dans le plan.
- En amont : l'efficacité du plan au regard des objectifs de continuité.
- En aval (durant une crise) : les niveaux de service constatés sur les activités essentielles, le fonctionnement des processus spécifiques au PCA et la disponibilité des ressources de secours.

La maintenance opérationnelle consiste ensuite à mettre en place les dispositifs de mesure relatifs à des tests périodiques, à des exercices ou à un sinistre vécu. Elle se traduit enfin par l'identification des axes de progrès et le suivi des améliorations apportées au plan.

## 2.2 L'ORGANISATION REQUISE

L'élaboration d'un PCA impose au préalable une action spécifique de communication visant à sensibiliser l'organisation à la gestion du risque et à la continuité d'activité, et à préparer la conduite du changement.

**La direction doit par conséquent s'engager très fortement dans l'élaboration du PCA,** par la désignation du chef de projet et de son équipe, l'établissement d'un mandat et le pilotage de points d'avancement réguliers, permettant la validation des principaux jalons, puis l'approbation du plan et son suivi. Elle doit s'assurer en outre que l'équipe de projet pourra animer une bonne gestion de la continuité et de la reprise d'activité, à travers :

- L'analyse et l'appréciation du risque.
- La formulation de propositions de stratégie de continuité et de reprise, la capacité à vérifier la bonne prise en compte – par des responsables désignés – du besoin de disponibilité des ressources prescrites par le plan et approuvées par la direction.
- L'intégration des procédures de continuité et de reprise dans les processus de l'organisation.
- La capacité à vérifier l'efficacité et l'efficience du PCA.

Idéalement, le chef de projet est rattaché au directeur des risques[2]. Il doit connaître le métier et disposer d'une autorité reconnue. Il est parfois plus simple de former à l'analyse de risques et au PCA un expert métier que l'inverse. Il devra disposer de correspondants dans les différentes entités de l'organisation, dont les responsables auront été eux-mêmes sensibilisés à l'objectif du PCA.

2 / Par expérience il est déconseillé de choisir le responsable des affaires générales ou un responsable informatique.

# 2.3 MÉTHODOLOGIE D'ÉLABORATION DU PCA

La démarche méthodologique, présentée par étapes, consiste à :

- Avant toutes choses, bien préciser le contexte et le périmètre du PCA.
- Identifier les objectifs et obligations de l'organisation dans le périmètre retenu.
- Formuler des besoins de continuité destinés à faciliter l'atteinte des objectifs et le respect des obligations.
- Identifier, grâce à l'étude des risques, les scénarios de crise qui justifient une démarche de continuité et définir parmi eux un ordre de priorité.
- Confronter les besoins de continuité aux scénarios retenus.
- Concevoir et formaliser une stratégie de continuité (et de reprise de la situation normale) visant à répondre aux scénarios retenus. Cette stratégie doit résulter de l'optimisation entre d'une part les exigences opérationnelles et leur coût pour respecter les objectifs de continuité, et d'autre part le coût et l'acceptabilité de l'interruption de l'activité (appréciés en fonction de la probabilité de survenue des scénarios).
- Définir, dans le cadre de la stratégie, les priorités en termes de ressources et de procédures[3].
- Définir les rôles des différents responsables pour mettre en œuvre, dans les délais prescrits, les ressources et procédures.
- Concevoir et décliner les dispositifs de vérification, de contrôle et d'évolutions régulières du plan.

Ces étapes sont résumées dans les paragraphes suivants, de manière à faciliter la compréhension de la démarche méthodologique dans son ensemble. Une description à vocation pratique plus détaillée, illustrée par des schémas et comprenant des fiches de bonnes pratiques est présentée dans la deuxième partie du guide (chapitre 3).

## 2.3.1 DÉFINIR LE CONTEXTE ET LES OBJECTIFS DE L'ORGANISATION

**Cette première action est essentielle et conditionne l'efficacité d'ensemble de la démarche.** Elle vise à préciser le périmètre géographique et fonctionnel de l'organisation qui doit être pris en compte, puis à identifier tout ce qui peut orienter les choix en rapport avec la spécificité de l'organisation. Notamment, il convient de prendre en compte aussi bien le contexte externe (demande des actionnaires, des autorités chargées de la réglementation et du contrôle, contrats existants et niveaux d'exigence associés, environnement politique, social, culturel, juridique, économique et financier, dépendances, etc.), que le contexte interne (histoire et culture de l'organisation, style de gouvernance et de pilotage, politique interne de gestion des ressources humaines, informatiques, matérielles et immatérielles, stratégie et objectifs internes, organisation, processus, système d'information, flux, etc.).

Cette démarche analytique est nécessaire pour la suite, afin notamment de permettre d'apprécier le niveau de risque acceptable par l'organisation, et d'orienter en conséquence la stratégie de continuité, soit vers une approche privilégiant la continuité des activités principales, soit, au contraire, vers une approche acceptant plus facilement les pertes d'activité associées à la prise de risque.

L'analyse du contexte permet également d'identifier les activités qui sont essentielles pour l'atteinte des objectifs de l'organisation et le respect de ses obligations. Ces activités supposent l'existence de processus et de flux (matières premières, interfaces avec les systèmes d'information) dont les plus critiques doivent être utilement cartographiés et décrits. De ce travail va découler une première analyse des ressources dites « critiques » pour le bon fonctionnement de l'organisation.

3/ Concrètement cela veut dire, par exemple, qu'il faut identifier les sites de repli ou à défaut en assurer la disponibilité, les pré-équiper, et introduire les procédures adaptées au fonctionnement depuis ces sites de repli.

### 2.3.2 IDENTIFIER ET FORMALISER LES BESOINS DE CONTINUITÉ

Cette étape est la suite logique de la précédente. Il s'agit de préciser, pour chaque activité essentielle et chaque processus ou flux critique, le niveau de service minimum indispensable ainsi que la durée d'indisponibilité maximale acceptable. Des modes dégradés peuvent parfois être envisagés, rendant ainsi plus tolérable une interruption de l'activité. Cependant, le mode dégradé obéit lui aussi à des objectifs de niveau de service minimum et de durée maximale avant une reprise de l'activité normale.

Pour maintenir ou rétablir le fonctionnement des processus, il faut disposer de ressources dites « critiques » que l'on peut classer en cinq catégories : ressources humaines, infrastructures, système d'information, ressources intellectuelles, et fournisseurs externes (prestations et matières premières). Par conséquent, des objectifs relatifs au niveau des ressources critiques doivent être également définis. Pour simplifier le travail, l'analyse des besoins en ressources sera effectuée sur la base d'un nombre limité de scénarios ou situations de crise retenus comme prioritaires, à l'issue de la démarche de gestion de risque et compte tenu des besoins de continuité.

À ce stade, il est déjà possible de quantifier les conséquences d'une interruption de l'activité en termes humain (personnes blessées ou décédées consécutivement à un arrêt de service vital), ou financier (pertes de ressources non assurées, application de pénalités contractuelles, conséquences juridiques, perte de matières suite à l'indisponibilité des systèmes d'information, ou perte de marchés suite à des fuites d'information), ainsi que les conséquences sur l'environnement, sur l'image[4], sur le moral des salariés ou sur la responsabilité pénale du dirigeant.

À la fin de cette étape la direction de l'organisme devra valider la description et l'évaluation de chaque processus critique. La description du processus, sa criticité, ses objectifs de niveau de service et de délai maximal d'interruption acceptable (DMIA ou DIMA), et les conséquences d'une interruption supérieure à ce délai maximal (exprimées autant que possible en coût financier) sont détaillées dans des fiches. Si l'interruption dépasse le délai maximal acceptable, le coût augmente fortement avec la durée de l'interruption. Sans dispositif de secours il est possible de mettre en péril l'organisation. L'impact financier ou la perte d'image peuvent alors dépasser ce que l'organisation peut assumer et conduire de facto à sa disparition (comme le montrent les exemples donnés en annexe).

### 2.3.3 IDENTIFIER ET GÉRER LES RISQUES PRIORITAIRES

La démarche de gestion du risque est une démarche globale qui permet de quantifier la probabilité d'occurrence (ou plausibilité) et les impacts des risques et disposer ainsi des éléments permettant de décider des actions à entreprendre afin de limiter les effets de l'incertitude sur les objectifs et obligations de l'organisation. Elle nécessite de travailler étroitement avec les responsables des métiers et des processus de l'organisation. C'est la seule démarche qui permette d'éviter que l'émotion ou la peur ne dictent les choix car elle permet de fournir des éléments de quantification seuls à même de conduire à des décisions rationnelles.

Concrètement, il s'agit **d'identifier** les risques de toutes natures (approche « tous risques »), puis de les **analyser** (selon les critères de fréquence et de gravité) en les regroupant par scénarios significatifs, et finalement **d'évaluer** ces risques en fonction du contexte et des enjeux pour l'organisation (activités stratégiques, chaîne de valeur, conjoncture, opportunités, concurrence, capacité financière, etc.).

➡ **L'identification** des risques consiste à sérier les risques qui peuvent affecter l'atteinte

4 / Par exemple à la suite d'une perte totale de crédibilité visant aussi bien l'organisation elle-même que ses dirigeants.

des objectifs stratégiques (part de marché, nouveaux produits, équilibre financier…), opérationnels (respect des délais de fourniture, coût des prestations, qualité des produits…), de gouvernance (qualité de l'information de pilotage, cohérence des systèmes d'information décisionnels…) ou de conformité (responsabilité sociale et environnementale, respect des textes réglementaires…). Au sein de ces « rubriques », les risques peuvent être également classés selon leur origine (accidentelle, naturelle, sanitaire, technologique, ou action humaine délibérée).

➡ **L'analyse** des risques peut se faire selon différentes méthodes, par exemple en caractérisant la source du risque (la menace), les vulnérabilités (grâce auxquelles la menace peut produire des effets) et les effets (ou impacts) eux-mêmes.

➡ **L'évaluation** des risques consiste à les classer selon deux critères : la probabilité d'occurrence (ou plausibilité) et la gravité d'impact. Il résulte de ce classement une liste graduée des risques, les plus critiques étant ceux qui sont à la fois les plus fréquents et dont l'impact est le plus grave. Ces derniers peuvent faire l'objet d'une évaluation complémentaire pour prendre en compte le contexte spécifique de l'organisation avec ses valeurs. Il en résulte finalement une liste de risques classés par ordre d'importance décroissante, les premiers devant faire l'objet d'une action prioritaire : le « traitement ».

➡ **Le traitement** des risques prioritaires consiste à décider d'une action visant à éliminer le risque (par exemple en changeant l'activité ou sa localisation) ou à le limiter (par des actions de prévention et de protection physique), ou encore par une gestion financière (assurance, partage).

Quand le risque ne peut être éliminé, les actions de prévention ou de protection sont à privilégier car elles sont généralement moins coûteuses que la gestion des conséquences d'un sinistre. Les actions de **prévention** consistent par exemple à diminuer la probabilité d'occurrence (ou plausibilité) par des mesures de protection physiques ou logiques dissuasives, la sensibilisation des employés aux bons comportements, la détection rapide de signaux précurseurs pour arrêter la menace à temps, des actions de dissuasion face à des menaces de nature humaine ou encore des interventions préventives.

Les actions de **protection** visent à limiter les effets directs d'un sinistre et à circonscrire le périmètre des dégâts, par exemple en protégeant les personnes et les biens, en rendant plus résistants les points névralgiques, en développant une défense en profondeur pour ralentir la progression et en assurant une détection rapide des incidents afin de permettre une intervention rapide.

### 2.3.4 CHOISIR LES SCÉNARIOS À PRENDRE EN COMPTE

Les actions de prévention et de protection ont permis de réduire les risques, mais pas de les supprimer. Des risques résiduels demeurent, qui ont généralement une probabilité d'occurrence (ou plausibilité) faible, mais peuvent néanmoins conduire à une perte de ressources critiques susceptible d'entraîner une interruption d'activité au-delà du seuil acceptable ou une diminution du niveau de service en deçà du seuil minimum prédéfini. Ces risques sont par conséquent constitutifs de scénarios qui devront être traités dans le cadre du PCA. Le travail de gestion du risque a permis également de les caractériser en termes de vraisemblance et d'impact. Ces données vont permettre d'optimiser la stratégie du plan de continuité présentée plus loin.

### 2.3.5 FORMALISER LES MOYENS ET PROCÉDURES

Afin d'assurer la continuité d'activité (notion prise au sens large de la normalisation, recouvrant le maintien du service au-dessus du seuil minimum, le fonctionnement dégradé temporaire et les mécanismes de reprise d'activité, partielle ou totale) il est nécessaire de pallier la perte de ressources critiques en utilisant d'autres ressources. Cela n'est généralement possible que si de telles ressources ont été prévues à

l'avance. Il est donc nécessaire de limiter les pertes de façon à disposer après le sinistre d'un niveau de ressources minimum pour permettre la reprise. Par exemple il ne sera possible d'assurer la reprise d'un système d'information à un niveau acceptable que si un certain nombre de matériels et de réseaux sont disponibles après le sinistre et si les données critiques sauvegardées sont suffisamment récentes pour limiter la perte opérationnelle. C'est le concept de perte de données maximale admissible.

Il résulte de ceci que la reprise d'activité doit se préparer :
- En identifiant ou en créant des ressources redondantes non susceptibles d'être affectées par le sinistre.
- En s'ouvrant la possibilité de faire appel, dans des délais adaptés, à des ressources externes.
- En appliquant des procédures de sauvegarde des données adaptées à l'exigence en termes de perte de données maximale admissible.
- En disposant d'une organisation, d'une architecture technique et de procédures qui vont permettre le fonctionnement du centre de secours dans les délais prescrits et pour les applications prioritaires.

Il est possible par exemple de disposer de différents dispositifs de secours informatique, les données essentielles étant dupliquées par un mécanisme de reproduction synchrone, assurant de ne pas perdre des données, tandis que des applications moins critiques pourront accepter une reprise « à froid » avec les données de la veille.

La reprise d'activité doit également se préparer en disposant de procédures testées :
- Activation des ressources de secours.
- Organisation et dispositif de gestion de crise.
- Déclenchement et mise en œuvre des modes dégradés de fonctionnement.

Le PCA requiert par conséquent des moyens et des procédures qui doivent être mis en place avant la survenue d'un sinistre. Après le sinistre, la cellule de crise pourra activer certaines dispositions du PCA afin de permettre une reprise partielle puis totale de l'activité.

Les moyens et procédures à mettre en place couvrent en premier lieu les ressources critiques identifiées :

➡ **Pour les ressources humaines** il s'agit d'identifier les positions de travail clés pour la continuité des activités essentielles, les positions de travail à maintenir et les dispositions pour y arriver (suppléance du personnel, mécanismes d'astreinte, recours aux réservistes, possibilité de travail occasionnel à distance…), les dispositifs techniques nécessaires (locaux, moyens d'accès, outils de travail, moyens de télécommunication, sécurité informatique, accès à la base de connaissance…), les moyens humains (formation, sensibilisation, exercices..) et les dispositifs réglementaires (contrat de travail, convention collective, responsabilités…).

➡ **Pour les systèmes d'information et de communication**, il est souhaitable de disposer d'une architecture permettant de répondre aux exigences en termes de délais de secours et de perte de données maximale admissible, grâce à un découpage de l'architecture technique en plaques secourables homogènes, facilitant selon les critères précédents une reprise progressive par paliers, et à l'existence de centres de secours et de données sauvegardées, avec les mécanismes adéquats. Des tests réguliers sont nécessaires pour en vérifier l'efficacité. Les moyens de télécommunication sont souvent un point de vulnérabilité majeur, justifiant l'existence de dispositifs de secours (réseaux dédiés sécurisés, systèmes privés par radio, accès par satellite, etc.) qui doivent être intégrés dans les procédures en temps normal, afin de pouvoir être utilisés facilement en période de crise.

➡ **Les processus et les flux** peuvent utilement faire l'objet de redondances et de solutions de contournement, formalisées dans des plans de continuité palliatifs définis par les responsables des métiers (par exemple des procédures manuelles). Des procédures spécifiques au PCA devront par ailleurs avoir été intégrées dans les processus de l'organisation afin de pouvoir être mises en œuvre en cas d'activation du PCA.

➡ **Les ressources intellectuelles** ne sont généralement pas prises en compte en dehors des systèmes d'information et des sauvegardes associés. Néanmoins pour certaines organisations les ressources intellectuelles ou immatérielles sont si critiques que des dispositifs de protection et de reprise doivent être prévus. Des solutions de sécurisation spécifiques peuvent être nécessaires (sauvegardes, contrôle d'accès renforcé, dépôt de brevets, protection des marques, cryptage, classification au secret de défense…).

➡ **Les infrastructures** sont souvent les premières à faire l'objet de dispositifs de continuité, en raison de catastrophes vécues, comme une inondation ou un incendie. Les solutions sont souvent bien connues et maîtrisées, mais une vérification reste fortement recommandée[5].

➡ Enfin le plus complexe reste la stratégie à adopter vis-à-vis des **partenaires** (prestataires et fournisseurs externes). En effet, il est nécessaire de transposer les exigences de continuité interne vers les flux venant de l'extérieur et donc vers les fournisseurs externes. Ces exigences pouvant être quantifiées, l'enjeu est alors de les traduire en termes contractuels – accompagnés de contrôles et de dispositifs de coordination durant une crise – et/ou en mécanismes de travail en mode collaboratif avec partage des analyses et traitement du risque, dans la stratégie de continuité et d'exercices communs. Dans certains cas, il peut être nécessaire d'internaliser certaines fonctions pour en assurer la maîtrise à moindre coût[6]. Une démarche de mutualisation de certaines ressources externes peut également être envisagée, sous réserve d'appliquer des règles très strictes régissant les priorités d'accès. La problématique des interdépendances et des effets en cascade justifie des études plus approfondies. Ce sujet est analysé en détail dans la deuxième partie de ce guide.

➡ **Le rôle de l'État** doit naturellement être pris en compte dans l'analyse des solutions permettant d'assurer la continuité d'activité. L'État est fournisseur de certaines prestations et promoteur de règles de bonnes pratiques dans le cadre de la continuité de ses activités essentielles. Il est également le gardien de l'intérêt général, pour la gestion des risques et la résilience de la Nation. Ce rôle comporte pour l'État la conduite d'analyses des risques majeurs, l'élaboration et la maintenance de plans nationaux de préparation et de réponse aux crises, la réalisation d'une veille opérationnelle, la mise en œuvre de dispositifs centralisés et déconcentrés de gestion de crise pour assurer la coordination des acteurs publics et privés dans la mise en œuvre des mesures d'intervention, de protection de la population et de continuité des activités d'importance vitale pour la vie économique et sociale.

### 2.3.6 DÉFINIR LA STRATÉGIE DE CONTINUITÉ

Nous avons vu précédemment que les scénarios de crise conduisant à un niveau d'activité ou à une durée d'interruption inacceptables par rapport aux seuils définis, justifient un plan de continuité. Par ailleurs, on a vu que le coût de dépassement de ces seuils peut être calculé. Il est d'autant plus élevé que l'interruption d'activité est longue. Au paragraphe précédent, les moyens à mettre en œuvre pour assurer la continuité ou la reprise d'activité ont été identifiés. Leur coût peut donc être évalué. Ce coût est d'autant plus élevé que les objectifs de délais d'interruption sont courts. Il est par conséquent aisé (au moins en théorie) de déterminer le point d'optimisation, en prenant en compte la probabilité d'occurrence du scénario de crise et l'appétence ou aversion au risque de l'organisation, pour l'activité considérée. En pratique, ces calculs financiers peuvent être parfois trop complexes. Dans ce cas l'ordre de grandeur quantitatif et qualitatif des coûts justifiant la mise en place d'une stratégie de continuité

5/ Exemple très courant du groupe électrogène ou du répartiteur de basse tension situés dans les sous-sols inondables.
6/ C'est par exemple le besoin de disposer de groupes électrogènes pour alimenter des fonctions stratégiques en cas d'absence d'électricité ou de pouvoir utiliser des moyens de télécommunication privatifs pour alerter et communiquer avec les intervenants en cas d'interruption prolongée des moyens de télécommunication publics.

peut toujours être estimé afin d'obtenir une validation en connaissance de cause par la direction.

### 2.3.7 SPÉCIFIER LES PROCÉDURES DE GESTION DE CRISE ET DE COMMUNICATION

La gestion de crise, entendue au sens large, conduit à mettre en œuvre les dispositifs et procédures nécessaires pour détecter, qualifier, alerter, anticiper, conduire les actions utiles, et décider notamment de l'activation de certains dispositifs du PCA. Dans cette perspective, les fonctions clés de la gestion de crise sont :

- La veille, qui permet de détecter des signes précurseurs et donc de préparer les responsables concernés.
- La procédure d'escalade, qui permet d'alerter les responsables du PCA et de la gestion de crise afin de qualifier l'événement assez tôt pour déclencher l'alerte de la hiérarchie, puis prendre au bon moment la décision d'activer la cellule de crise.
- Les fonctions d'aide à la décision et notamment la capacité à anticiper, analyser les différents scénarios possibles et recommander un plan d'action optimal dans le contexte incertain inhérent aux situations de crise sortant d'un cadre prédéfini.

La cellule de crise joue un rôle clé dans l'activation des dispositifs du PCA qui sont les plus adaptés à la situation. A contrario, dans le cas de situations fréquentes (par exemple en cas de fortes tempêtes dans les Antilles), des PCA peuvent être activés en mode « réflexe », sans qu'il y ait nécessairement besoin de disposer d'une cellule de crise.

### 2.3.8 RÉDIGER LE PLAN DE CONTINUITÉ ET LA DOCUMENTATION ASSOCIÉE

Au terme des travaux décrits aux paragraphes précédents et après leur validation, il est possible de rédiger le plan de continuité d'activité qui va décrire la démarche logique ayant conduit au choix de la stratégie de continuité et de la réponse aux différents scénarios de crise retenus. Cette réponse consiste à préciser les moyens et à documenter les procédures qu'il convient de mettre en œuvre en fonction des dispositifs du PCA activés par la cellule de crise.
Les responsables de ces moyens et procédures doivent être clairement identifiés ainsi que leur rôle et les actions attendues d'eux. La documentation doit être facilement accessible en cas de besoin, être aisément comprise même par des personnes récemment affectées et qui n'ont pas encore été formées. Elle doit être aussi aisément modifiable pour permettre au PCA d'évoluer. Par ailleurs, les procédures spécifiques au PCA doivent être parfaitement intégrées aux procédures normales afin d'être comprises et facilement activées en situation d'urgence.

### 2.3.9 ASSURER LA CAPACITÉ DE MISE EN ŒUVRE DU PLAN

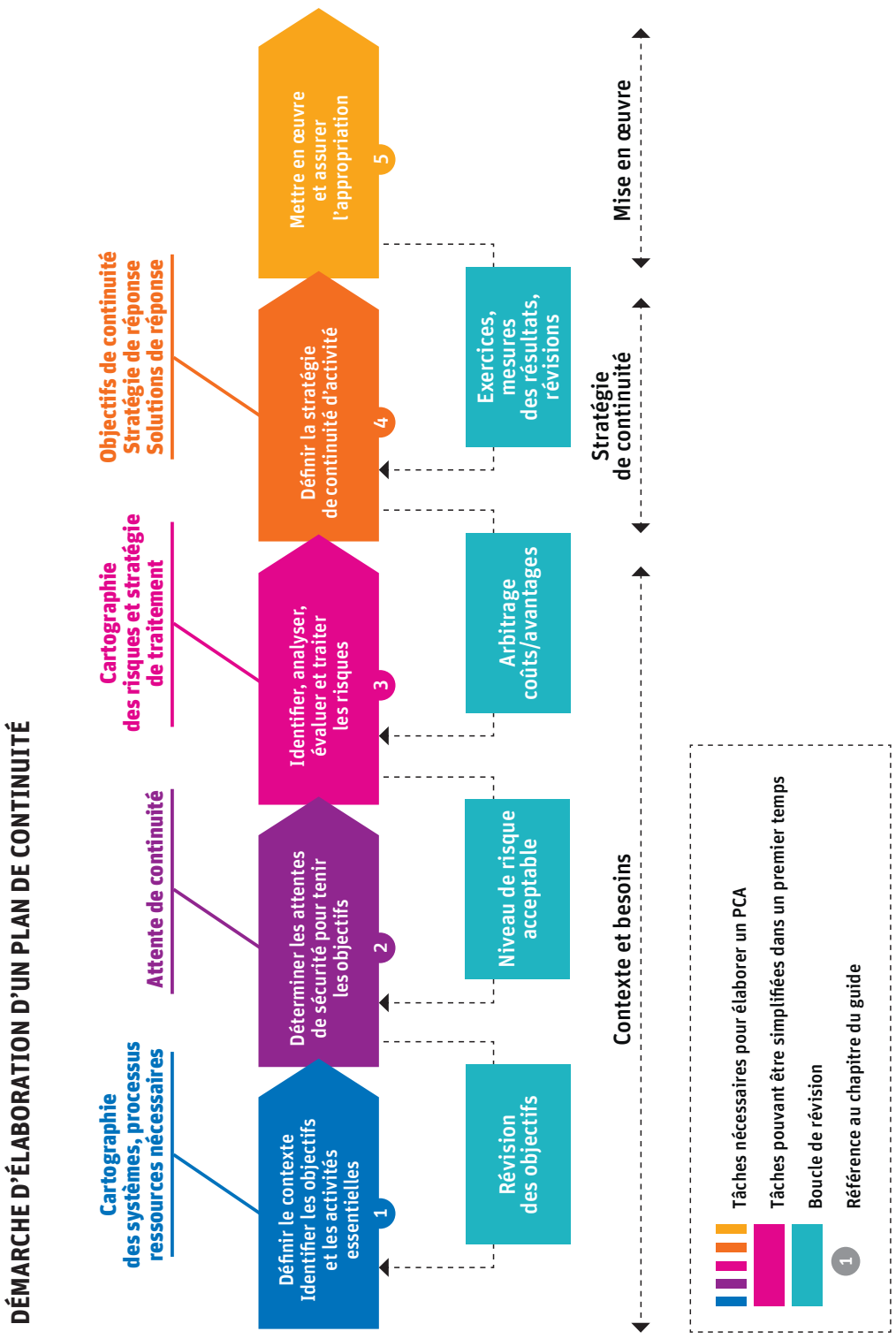
Les responsables en charge des moyens doivent vérifier la disponibilité des ressources spécifiques conditionnant l'activation du plan de continuité. À défaut, de nouvelles ressources[7] doivent être mobilisées pour assurer cette disponibilité dans les délais prescrits par le PCA. Les procédures de mise en œuvre du PCA doivent également être spécifiées, documentées et intégrées dans les processus existants[8]. Il est nécessaire de vérifier que ces ressources sont bien disponibles[9], ou le seront à une date identifiée, et que les procédures sont connues, comprises et pourront être mises en œuvre dans les délais prescrits, et selon des modalités spécifiques aux scénarios retenus. Cette tâche est beaucoup plus difficile quand on s'adresse à des prestataires externes, qui ne sont pas sous le contrôle de l'organisation. Cependant,

7 / Cela peut être par exemple un site de repli, un centre de secours informatique ou des ressources humaines qui pourront suppléer l'absence de locaux ou de personnes rendues indisponibles (maladie, absence de moyens de transport…).
8 / Cela peut inclure par exemple un dispositif simple permettant de passer une commande dans des délais plus courts qu'avec la procédure administrative habituelle, ou des procédures plus complexes destinées à déplacer un centre informatique sur un site de secours en utilisant les sauvegardes disponibles sur un troisième site.
9 / En effet, certains fournisseurs de «centre de repli» signent le même contrat avec plusieurs opérateurs, pour les mêmes ressources, mais ne peuvent les fournir qu'au « premier arrivé » lorsque l'incident survient (vérifier qu'ils ne font pas de surbooking).

les mêmes principes doivent s'appliquer, avec, selon le cas, un contrôle direct, un contrôle documentaire, une certification par un tiers et/ou la participation à des tests ou exercices communs (une fiche spécifique traite de ce sujet dans la seconde partie du guide).

### 2.3.10 FAIRE ÉVOLUER LE PLAN : EXERCICES ET RETOURS D'EXPÉRIENCE

Une fois le PCA réalisé et sa capacité à être mis en œuvre garantie, il est nécessaire d'en vérifier l'efficacité. À cet effet, différentes approches complémentaires sont recommandées. Il s'agit d'abord de faire vérifier les documents, idéalement par un tiers de confiance, puis de tester la mise en œuvre des dispositifs (par exemple le basculement de certaines fonctions sur un site de secours), de vérifier enfin, par des exercices, que les dispositifs et procédures de continuité sont connus, compris et peuvent être mis en œuvre dans les délais prescrits.


DÉMARCHE D'ÉLABORATION D'UN PLAN DE CONTINUITÉ
Définir le contexte
Identifier les objectifs
et les activités
essentielles
1
Déterminer les attentes
de sécurité pour tenir
les objectifs
2
Identifier, analyser,
évaluer et traiter
les risques
3
Définir la stratégie
de continuité d'activité
4
Mettre en œuvre
et assurer
l'appropriation
5
Cartographie
des systèmes, processus
ressources nécessaires
Attente de continuité
Cartographie
des risques et stratégie
de traitement
Objectifs de continuité
Stratégie de réponse
Solutions de réponse
Révision
des objectifs
Niveau de risque
acceptable
Arbitrage
coûts/avantages
Exercices,
mesures
des résultats,
révisions
Contexte et besoins
Stratégie
de continuité
Mise en œuvre
Tâches nécessaires pour élaborer un PCA
Tâches pouvant être simplifiées dans un premier temps
Boucle de révision
1 Référence au chapitre du guide

# LES FICHES PRATIQUES

## 3 LES FICHES PRATIQUES

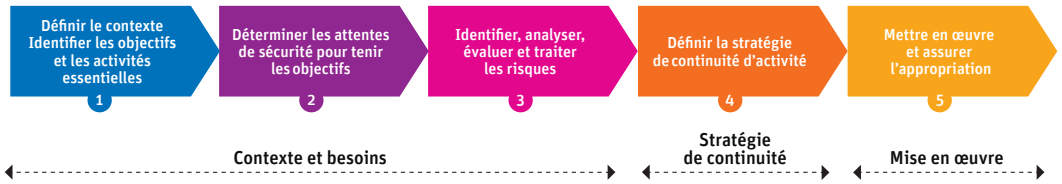


## 4 LES ANNEXES

Les fiches pratiques décrivent de manière approfondie les étapes de la démarche complète d'élaboration d'un plan de continuité d'activité. **Il est possible d'entreprendre une démarche simplifiée en se référant exclusivement aux fiches 1 à 8 et 14 à 27.**

L'ensemble de ces fiches vise à faciliter l'appropriation de la méthode et des bonnes pratiques en aidant leur transposition dans le contexte spécifique à différents types d'organisations. **Afin de mieux en situer l'objectif, les fiches ont été sériées au moyen d'un code couleur qui renvoie aux cinq étapes matérialisées par le schéma ci-dessous.**

**DÉMARCHE D'ÉLABORATION D'UN PLAN DE CONTINUITÉ**




Les titres des fiches suivantes sont de la couleur correspondant à l'étape indiquée ci-dessus

- Fiches de 1 à 5
- Fiches de 6 à 8
- Fiches de 9 à 14
- Fiches de 15 à 20
- Fiches de 21 à 27

Dans un but pédagogique, les bonnes pratiques sont identifiées grâce à un code couleur :

- Mesures recommandées
- Mesures déconseillées, ou points d'attention particuliers

# COMMENT LANCER UNE DÉMARCHE DE CONTINUITÉ D'ACTIVITÉ ?

**OBJECTIF**

La réalisation d'un plan de continuité efficace et robuste nécessite d'impliquer de nombreux responsables, de conduire des travaux transverses à l'organisation, d'assurer la cohérence des analyses et d'effectuer des arbitrages de niveau stratégique.

➡ **Condition première du succès, la direction de l'organisation doit s'impliquer fortement dans la démarche.**
Dès le lancement, il s'agira de communiquer en expliquant les finalités et de mobiliser les responsables des métiers et des processus. Par la suite et durant toute la phase d'élaboration du PCA, la direction devra valider les résultats successifs :
• Description du contexte, des objectifs et obligations de l'organisation.
• Cartographie des processus clés pour la continuité, des niveaux de service et d'interruption acceptables.
• Cartographie des risques et identification de ceux qui justifient un traitement prioritaire, compte tenu de l'attitude de l'organisation face au risque.
• Stratégie de continuité avec l'optimisation des coûts de continuité tenant compte du coût de l'interruption d'activité, du niveau de continuité souhaité et du risque résiduel.
• Moyens et procédures nécessaires à la mise en œuvre et au suivi du plan de continuité (y compris sa composante de reprise d'activité).

➡ **Les autres conditions du succès sont :**
• Un travail préalable pour formaliser les activités et processus de l'organisation avec la nomination de responsables des métiers et des processus.
• La désignation d'un chef de projet à l'autorité reconnue, et d'une équipe projet qui marqueront le lancement officiel de la démarche. Cette désignation doit s'accompagner d'un mandat précisant les objectifs, les périmètres géographique et fonctionnel, ainsi que les principaux jalons de la mission.
• Une fois la stratégie de continuité établie et validée par la direction de l'organisation, doivent être impliqués, le moment venu, les correspondants du PCA, les responsables des métiers et processus, ainsi que tous les acteurs concernés par la mise en œuvre d'actions spécifiques, afin de mettre en place les ressources et procédures nécessaires.
• L'exercice du PCA pour vérifier son réalisme et son efficacité.
• L'accompagnement à la conduite du changement dans le cadre de cette démarche.

**Il est recommandé de :**
• Confier le pilotage du projet au responsable chargé de la gestion des risques au sein de l'organisation. À défaut, le responsable en charge du métier le plus impliqué dans les activités essentielles de l'organisation, ou le responsable chargé de l'écoute des clients, peuvent être désignés.
• Donner au responsable du projet PCA l'autonomie et l'autorité, éventuellement par délégation, sur l'ensemble des responsables de l'organisation et des acteurs concernés par les effets contre lesquels on cherche à se protéger.
• Maintenir en place la structure de gestion de PCA une fois que la première version a été validée.

**Il est déconseillé de :**
• Confier le pilotage d'un projet de PCA à un responsable informatique ou au responsable des services généraux, qui n'auront pas la vision « métier » de l'organisation.

# FAIRE LE CHOIX D'UNE DÉMARCHE COMPLÈTE OU SIMPLIFIÉE

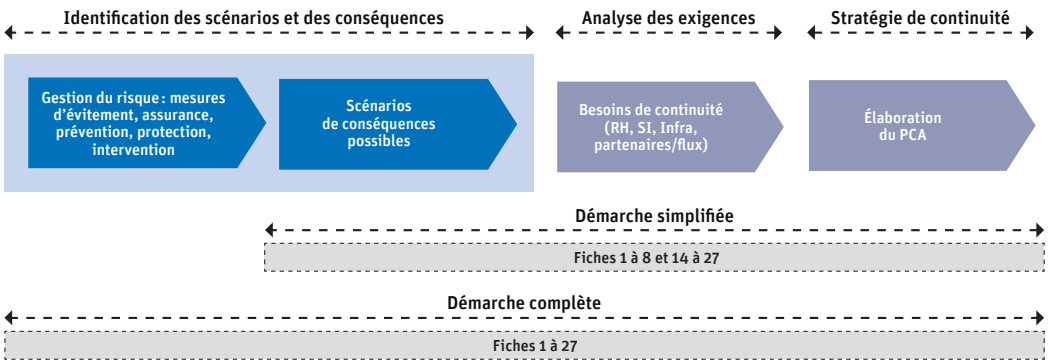
**OBJECTIF**

Le PCA s'inscrit dans une démarche globale de résilience qui intègre également la gestion du risque (notamment les plans de prévention et de protection). **Néanmoins, pour satisfaire une contrainte de temps ou lorsque la démarche de gestion du risque n'est pas encore en place, une approche simplifiée est possible.**

➡ **La démarche simplifiée** consiste, partant des effets possibles sur le fonctionnement de l'organisation et en ne s'intéressant qu'aux actions qui permettent de résister au choc, à maintenir les activités essentielles puis à assurer une reprise normale de l'activité. Cette démarche, qui ne permet pas d'apprécier globalement les priorités d'action, peut néanmoins, dans un premier temps, être dissociée de la démarche de gestion du risque, laquelle pourra être conduite ultérieurement par une approche itérative. **Dans l'urgence, un PCA spécialisé sur un scénario peut être construit de cette manière.** Cette démarche est néanmoins déconseillée car elle est source de travaux redondants, de multiplication de scénarios, et susceptible de démotiver les responsables consultés de manière répétitive.

➡ **La démarche complète** s'inscrit dans la continuité de la politique de gestion des risques de l'organisation. Cette démarche est la plus avantageuse. Elle permet de définir les scénarios significatifs (car il n'est pas possible d'être exhaustif), rationaliser les choix et mieux justifier auprès de la direction, grâce à une vue globale, les investissements nécessaires. La gestion de risque permet en outre de mieux connaître les conséquences possibles ainsi que leur probabilité d'occurrence (ou plausibilité) et donc de définir rationnellement la stratégie de continuité d'activité.

**DIFFÉRENTES APPROCHES POUR ÉLABORER UN PCA**



# DÉFINIR LE PÉRIMÈTRE DU PCA

**OBJECTIF**

Une approche méthodologique souple et quelques bonnes pratiques permettent d'entreprendre efficacement une démarche de PCA, dans un périmètre adaptable.

**Deux questions reviennent fréquemment : Pour une organisation donnée, vaut-il mieux réaliser un PCA unique ou réaliser un PCA pour chacun des établissements/sites ? Est-il pertinent d'avoir un PCA unique « tous risques » ou des PCA spécialisés par risques ?** On pourrait répondre que, par principe, le PCA unique est théoriquement préférable car il permet de mener une démarche exhaustive en évitant la redondance des démarches de recueil de données, de conception et de validation. Cependant, le paysage des organisations publiques et privées est composé de dispositifs fonctionnels et de situations d'organisation très différents. Il faut donc s'adapter au cas par cas pour définir le périmètre du/des PCA à mettre en place.

➡ **La définition du périmètre doit d'abord résulter d'une analyse du contexte ainsi que des champs géographique et organisationnel pris en compte.** Certaines parties de l'organisation peuvent être exclues, soit parce qu'elles disposent déjà d'un PCA éprouvé, soit parce qu'elles relèvent d'objectifs et d'obligations très spécifiques (par exemple pour une filiale très autonome localisée à l'étranger). Il en résulte généralement l'établissement de plusieurs PCA distincts sous la responsabilité des dirigeants des organisations respectives. Dans des grandes organisations internationales on peut trouver ainsi plusieurs dizaines, voire plusieurs centaines de PCA. Dans ces cas de figure il est conseillé de définir un modèle de PCA avec un « chapeau » unique, un format type, et de le faire décliner de manière adaptée par les dirigeants locaux.

➡ **La définition du périmètre résulte ensuite d'une analyse fonctionnelle.** L'analyse des objectifs et des obligations de l'organisation permet la description des activités essentielles ainsi que des processus et ressources qui sont critiques pour ces activités. Par suite, l'analyse du risque et des conséquences des sinistres, ainsi que l'identification des scénarios prioritaires à prendre en compte, permettent de limiter le périmètre fonctionnel aux situations les plus graves nécessitant une mobilisation de l'organisation. Ainsi, certains scénarios de crise, qui requièrent seulement l'implication d'un petit nombre de personnes (exemple d'une crise juridique simple) ne doivent pas utilement faire partie du PCA.

➡ **Un organisme qui disposerait déjà de plusieurs PCA sectoriels** (pour répondre à une pandémie, une crue, une panne informatique…) et qui serait satisfait de ces PCA, peut décider de les conserver. Dans cette perspective, il est cependant recommandé de les agréger dans un PCA global, en créant un « tronc commun » et en prenant en compte des scénarios complémentaires, identifiés en liaison étroite avec le directeur des risques. À l'occasion de cette démarche, certains PCA sectoriels peuvent être revus car le contexte et les attentes de l'organisation peuvent avoir changé[10]. Il résulte également de cette dernière recommandation que les situations de sinistres consécutives à des actes de nature terroriste (cas notamment des opérateurs d'importance vitale qui déclinent les scénarios de menace prescrits par une directive nationale de sécurité) doivent être incluses dans les scénarios du PCA. Dans ce cas de figure, les données confidentielles sont regroupées dans des annexes protégées conformément à la réglementation.

10 / Ce cas de figure peut être illustré avec l'exemple d'un PCA informatique (ou PCI) qui visait à l'origine la disponibilité informatique et que l'on fait évoluer en prenant en compte le besoin d'intégrité (risque de perte ou de modification d'information sensibles) et/ou des scénarios nouveaux. Notons à ce sujet qu'il est déconseillé de mettre en place un plan de continuité informatique (PCI) ou un plan de continuité métier (PCM), s'ils ne sont pas intégrés dans un PCA global.

# IDENTIFIER LES OBJECTIFS ET LES ACTIVITÉS ESSENTIELLES

**➡ Il faut préalablement connaître et comprendre le contexte…**
L'analyse du contexte est un préalable car c'est elle qui permet de préciser le périmètre (géographique, organisationnel et fonctionnel) qui sera couvert par le PCA, les activités et enjeux de l'organisation, ses objectifs et ses contraintes (externes et internes), les acteurs clés ainsi que les moyens techniques et humains dont elle dispose ou peut disposer. **L'analyse du contexte permet d'abord de préciser le périmètre de l'organisation pris en compte.** L'entité qui rédige le PCA peut être l'organisation complète (l'entreprise ou l'administration), une direction ou unité d'affaires, ou un centre technique. Le périmètre s'exprime en termes organisationnel, géographique ou fonctionnel. **L'analyse du contexte permet également d'apprécier les niveaux de risques acceptables pour l'organisation.**

**➡ …pour identifier les activités qui sont nécessaires à l'accomplissement des objectifs ou missions de l'organisation…**
Les activités sont généralement les grands blocs fonctionnels identifiés dans l'organigramme, matérialisés par des grandes directions, par exemple les achats, les ressources humaines, la chaîne logistique, la production, le commercial, les finances. Certaines activités peuvent être exclues, par exemple parce qu'elles sont autonomes et disposent de leur propre PCA.

**➡ … préciser les apports de ces activités pour le fonctionnement de l'organisation, les relations avec les partenaires, la performance et la création de valeur…**
Ce travail permet d'identifier les activités qui sont essentielles au fonctionnement de l'organisation pour l'atteinte de ses objectifs et le respect de ses obligations. Certaines activités qui ne sont pas dans le « cœur de métier » peuvent néanmoins être essentielles au sens où leur non-fonctionnement pourrait entraver la poursuite des objectifs ou la tenue des obligations.

**➡ …et décrire les objectifs ou enjeux principaux de chaque activité essentielle.**
Il s'agit d'objectifs qualitatifs ou quantitatifs, qui peuvent être exprimés en termes financiers, de part de marché, de niveau de service, de productivité, et concerner des aspects stratégiques ou opérationnels.
Par exemple :
- Assurer le meilleur service aux usagers ou clients.
- Contribuer à la fourniture de prestations fiables et de qualité.
- Diminuer les coûts de fonctionnement.
- Être capable d'agilité pour s'adapter aux changements.

# CARTOGRAPHIER LES PROCESSUS ET LES FLUX ET DÉFINIR LEUR CRITICITÉ

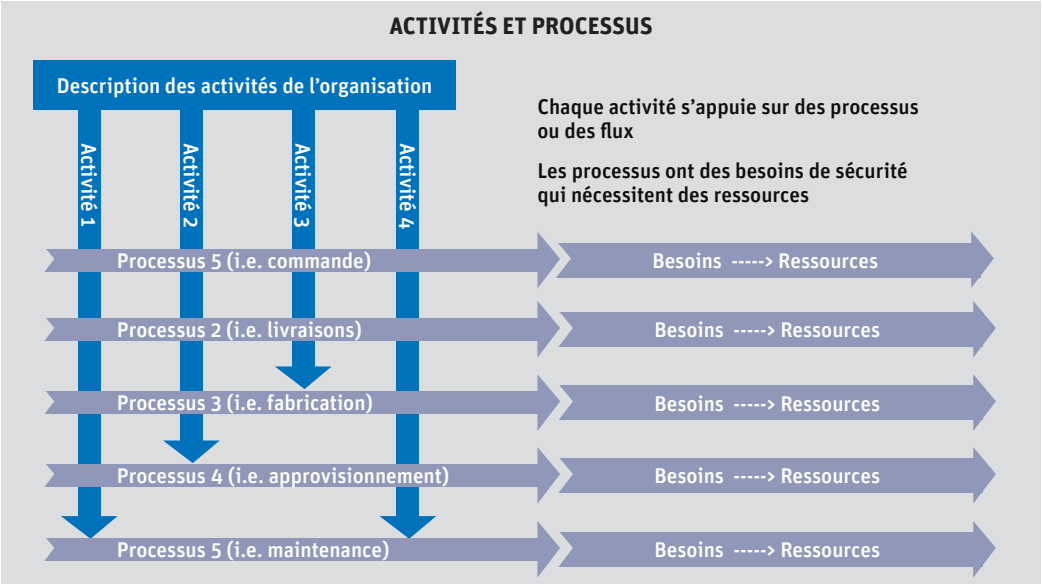
**OBJECTIF**

Chaque activité essentielle a besoin de processus et de flux pour fonctionner. Il s'agit par exemple de la paye, du système de prise de commande, du système de livraison, de la chaîne logistique, du flux de matière première, etc. La cartographie des processus, des flux et de leur criticité permet de mieux en appréhender les relations.

➔ **Les processus peuvent être propres à une activité ou être communs à plusieurs activités** et comme ils sont souvent associés à un système d'information, la cartographie des systèmes d'informations peut aider à les identifier. Les flux concernent les échanges en entrée ou sortie des systèmes d'information ; ainsi que les échanges physiques : électricité, eau, matières premières.

➔ **Les processus critiques** sont ceux qui sont essentiels pour le maintien de l'activité. Ce travail d'identification doit être réalisé à partir d'entretiens avec les responsables des métiers et des processus. L'identification des besoins et ressources nécessaires associées est présentée dans les fiches suivantes. L'analyse des processus doit comprendre l'identification des interfaces (donneurs d'ordre, prestataires). La cartographie des processus critiques doit être validée par la direction.

**Il est recommandé** de cartographier les processus de l'organisation.
**Il est très fortement recommandé** de cartographier les flux entre les systèmes d'information supportant les différents processus de l'organisation ; cette cartographie est nécessaire pour la détermination des impacts qui devront être traités par le plan de continuité informatique. Elle se décline assez naturellement à partir de la cartographie des processus.



# IDENTIFIER ET FORMALISER LES BESOINS DE CONTINUITÉ

**OBJECTIF**

Pour maintenir l'activité au niveau exigé par les objectifs et obligations identifiés, les processus doivent répondre à des objectifs de sécurité, que l'on appelle « attentes » ou « besoins » et qui doivent être identifiés.

➡ À partir des discussions avec les responsables des métiers, il est possible de dégager des attentes, qui peuvent être sériées par critères, sous la forme D.I.C.T.E.S. :

• **Disponibilité,** continuité de service, régularité, résistance aux dysfonctionnements et aux ruptures, robustesse. Ceci doit pouvoir être mesurable, par exemple en termes de fiabilité des prestations.

• **Intégrité,** c'est-à-dire que le service/produit livré est bien celui attendu, dans l'état prescrit. Si ce n'est pas le cas, le service n'est pas rendu, conduisant à un arrêt (plus ou moins long) du service.

• **Confidentialité,** protection des informations sensibles. Une perte de confidentialité peut conduire à l'arrêt de certaines activités très sensibles, voire à la faillite de certaines organisations (cf. les cas présentés en annexe).

• **Traçabilité,** visibilité, connaissance des événements. La traçabilité peut être indispensable pour permettre d'assurer des prestations (par exemple le transport de matières dangereuses).

• **Évolutivité,** capacité à s'adapter aux changements et à l'environnement et donc à assurer la robustesse. L'absence d'évolutivité peut conduire à l'arrêt dans des contextes changeants.

• **Sûreté,** capacité à limiter les effets d'actes malveillants.

➡ **Lors de cette étape, il est souhaitable de quantifier le niveau du besoin de continuité, en utilisant trois indicateurs :**

1. **Le niveau de service minimum** (une perte de service qui maintient le fonctionnement au-dessus de ce seuil affecte peu le service final. A contrario une perte de niveau de service en dessous de ce seuil est considérée comme une indisponibilité). Ce seuil peut être défini comme un pourcentage de conformité minimum ou un pourcentage de produits/services commandés livrés à la date/heure convenue. Durant la phase de reprise d'activité après un sinistre, il est possible de définir des seuils plus faibles, en mode dégradé.

2. **Le niveau d'indisponibilité minimum.** Tout arrêt de durée inférieure à ce niveau est tolérable. Pour des indisponibilités de courtes durées et relativement fréquentes l'exigence est exprimée en durée maximale d'interruption et en fréquence maximale, ce qui se combine en pourcentage de temps d'indisponibilité pendant une durée significative. Pour ce qui concerne un sinistre, rare par définition, la mesure se fait par la durée maximale d'interruption de service acceptable (DMIA).

3. **Les ressources qui restent indispensables** pour permettre la reprise d'activité. Elles peuvent s'exprimer en quantité de stock à préserver, de locaux de repli, ou de niveau de mise à jour des données sauvegardées (ce qui revient à définir la perte de données maximale admissible, depuis la dernière sauvegarde).

Page suivante ➡

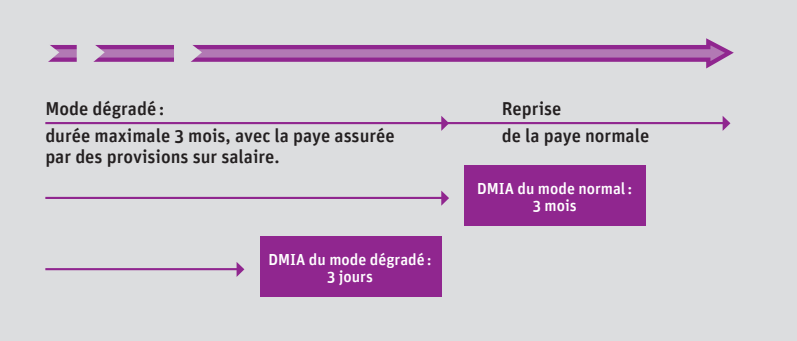
Pour illustrer la notion de DMIA, on peut citer l'exemple du processus de livraison ou de fourniture de certains produits ou services sensibles qui ne peut accepter un délai de retard (DMIA) supérieur à 12 heures (ce peut être le cas d'une livraison de médicaments), ou supérieur à 30 minutes (une intervention de service d'urgence par exemple).
Dans un autre domaine, on peut citer l'exemple d'un processus de paye qui ne peut pas accepter un retard (DMIA) supérieur à trois jours, en mode dégradé (avec un versement de provisions sur salaires). Cette possibilité de pouvoir fonctionner en mode dégradé permet une interruption maximale (DMIA) du fonctionnement normal de plusieurs mois. Une autre formulation consiste à dire que la durée maximale de fonctionnement en mode dégradé est de plusieurs mois :

➡ **Le mode dégradé** est souvent présenté comme un palliatif sans qu'il y ait une analyse précise de son contenu. Cependant, pour tout mode dégradé il convient de :

- Définir les circonstances de sa mise en place.
- Intégrer les aspects réglementaires spécifiques au mode dégradé (et notamment les modifications envisageables des textes réglementaires dans des circonstances exceptionnelles).
- Définir des procédures spécifiques et des mesures d'ordre juridique.
- Pouvoir transférer le personnel sur des postes nouveaux.
- Faire éventuellement appel à l'intérim.
- Respecter les textes réglementaires spécifiques (comme dans le domaine du transport de voyageurs ferroviaire ou aérien, avec des dispositifs permettant d'adapter les moyens de transport aux ressources humaines disponibles, dans le cadre d'un dialogue social).
- Disposer de solutions de dernier secours, connues et rapidement mises en œuvre[11].

**Il est recommandé** de faire valider le niveau dégradé, qu'il est prévu de maintenir en période de crise, par les représentants des clients.
La description de chaque niveau dégradé doit nécessairement expliciter :

- Le délai avec lequel il est mis en place.
- La durée pendant laquelle on peut s'en accommoder avant un retour à un fonctionnement nominal (ou moins dégradé, si plusieurs niveaux sont définis avant un retour à la normale).
- Les modalités acceptables de fonctionnement en mode dégradé.




11 / Il peut être suggéré de mettre en place des serveurs informatiques accessibles sur Internet (via des liens sécurisés et protégés) afin de permettre le fonctionnement des principaux métiers en mode dégradé. En effet le support papier n'est généralement pas suffisant pour permettre un fonctionnement satisfaisant en mode dégradé.

# IDENTIFIER LES BESOINS DE CONTINUITÉ
## POUR LES RESSOURCES CRITIQUES

**OBJECTIF**

Pour répondre aux attentes de sécurité des processus et flux critiques qui viennent d'être définis, il est nécessaire de formaliser des objectifs de disponibilité pour les moyens.

➡ **Ces moyens, appelés « ressources critiques », peuvent être différenciés en cinq catégories :**

- **Infrastructures** (bâtiments, locaux, moyens de transport…).
- **Systèmes d'information** (systèmes informatiques, serveurs, moyens de télécommunication, réseau local, messagerie, accès Internet…).
- **Ressources humaines** (équipes disponibles, renforts, personnes clefs, qualifications, compétences, motivation…).
- **Ressources intellectuelles** et immatérielles (données internes, informations stratégiques[12], informations à protéger…).
- **Prestations externes** (eau, énergie, sous-traitants…) ou produits critiques (matières premières rares).

**Il est recommandé :**

- D'intégrer dans le PCA de l'organisation le niveau dégradé des prestations que les fournisseurs ont prévu de maintenir en période de crise.
- D'intégrer dans les systèmes critiques de l'organisation son système téléphonique, ses serveurs de fichiers et son système de messagerie.

➡ **Pour l'identification des ressources critiques immatérielles** il peut être utile de se référer aux 10 actifs immatériels identifiés par l'Observatoire de l'immatériel (www.observatoire-immateriel.com) : Les biens immatériels (intellectuels) peuvent ne pas être inclus. Certaines organisations considèrent en effet qu'ils relèvent de struc-


12 / Exemples : plan stratégique, études de concurrence, fichiers clients et prospects, liste des fournisseurs, contrats, données comptables, paie, dossiers du personnel, organigramme détaillé de l'entreprise, brevets, plans, procédés de fabrication, codes sources…

Page suivante

tures spécifiques et que le PCA doit se limiter aux risques opérationnels (conséquences de perte de ressource matérielle critique sur l'activité). Néanmoins leur inclusion dans la démarche de PCA reste généralement souhaitable, notamment dans les environnements concurrentiels.

➡ **La formulation des attentes de continuité permet de préciser le périmètre du PCA :**

• Le PCA doit prendre en compte les pertes des ressources critiques qui génèrent la rupture de processus critiques et par voie de conséquence la perte d'activités essentielles. Néanmoins une approche par trop complexe n'est pas recommandée. Par exemple la perte de conformité juridique est généralement traitée seulement par le service juridique et ne justifie donc pas le déclenchement du PCA.

• Il est conseillé de prendre en compte a minima la perte des ressources dites « dures » : infrastructures, personnel, systèmes d'information, prestations externes et matières premières.

• La prise en compte des ressources immatérielles est recommandée. Ce choix peut dépendre des objectifs de l'organisation et de son contexte.

• Le choix du périmètre final du PCA relève de la direction générale.

➡ **La formulation des attentes permet aussi de calculer les coûts de PCA :**

Les attentes de continuité se traduisent par des exigences de continuité sur les ressources critiques, qui génèrent des coûts de maintien (duplication, redondance, site de secours, astreintes, matériel de protection individuel, etc.).

Ces coûts sont analysés au cours de l'étape 4, relative à l'équilibre entre le coût de maintien de ressources critiques et le coût d'arrêt de l'activité, qui permettra de définir la stratégie de continuité.

# MESURER LES CONSÉQUENCES D'UNE INTERRUPTION DE SERVICE

**OBJECTIF**

Les conséquences d'une perte d'activité ont un coût et il existe un seuil d'interruption tolérable au regard des objectifs et enjeux de l'activité. Ces données sont mesurables.

➡ **Une indisponibilité est mesurable en termes de coûts :**

- Humain (protection des travailleurs…).
- Part de marché (perte de chiffre d'affaires, perte de clients…).
- Conséquences des engagements commerciaux et contractuels (pénalités, résiliations…).
- Conséquences juridiques (coût résultant du respect des obligations légales et réglementaires, sanctions possibles, responsabilité pénale du dirigeant…).
- Impacts opérationnels (coûts de réparation…).
- Conséquences sociales (chômage technique, impact sur les partenaires…).
- Conséquences psychologiques (démotivation, perte de moral…).
- Conséquence sur l'environnement (pollution…).
- Conséquences sur des partenaires situés en aval, voire au niveau du fonctionnement de la société.
- Perte de valeur, d'image ou de réputation, et donc perte de confiance ou de marché, voire perte de l'activité.

**EXEMPLE DE MESURE DES CONSÉQUENCES DE L'INTERRUPTION DE SERVICE ET DONC DE LA CRITICITÉ DE CHAQUE PROCESSUS**

| Activité | Processus | Humain | Financier | Contractuel | Environnement | Juridique et réglementaire | Opérationnel | Social | Perte d'image |
|---|---|---|---|---|---|---|---|---|---|
| Commercial | Prise de commande | 1 | 4 | 2 | 1 | 1 | 3 | 1 | 3 |
| Commercial | Relation client | 1 | 3 | 3 | 1 | 1 | 3 | 2 | 3 |
| Commercial | Niveau de service | 2 | 3 | 4 | 2 | 3 | 2 | 2 | 3 |
| Commercial | Livraison | 2 | 2 | 4 | 1 | 1 | 4 | 2 | 3 |
| Achat | Approvisionnement | 1 | 3 | 2 | 2 | 3 | 3 | 2 | 3 |
| Production | Fabrication | 4 | 3 | 4 | 3 | 2 | 3 | 3 | 2 |
| Logistique | Stockage | 1 | 4 | 2 | 2 | 1 | 3 | 2 | 1 |
| Ressources humaines | Paye | 1 | 3 | é | 1 | 3 | 1 | 4 | 2 |
| Finances | Facturation | 1 | 4 | 2 | 1 | 1 | 1 | 1 | 2 |

**1** = très faible - **2** = faible - **3** = fort - **4** = très fort

Page suivante ➡

➡ **L'analyse des conséquences d'une interruption d'activité permet de valider la durée maximale acceptable (DMIA).** Ces conséquences sont pour beaucoup d'entre elles chiffrables et permettent ainsi de déterminer un coût (qui augmente quand la durée de l'interruption augmente). Certaines sont en revanche difficilement chiffrables et relèvent davantage d'une appréciation qualitative (cf. la perte d'image, la perte de valeur, la perte de confiance). La définition de l'échelle de mesure, qui doit être la même pour tous les processus et acceptée par les responsables des métiers et ceux des processus, est un point important.

Cette analyse des conséquences de l'interruption d'activité permet ainsi de préciser le périmètre (fonctionnel et temporel) des processus critiques, dont le bon fonctionnement doit être privilégié. Il peut s'agir par exemple d'une période critique dans l'année ou le mois, ou d'une partie du processus. En effet une activité peut n'être essentielle que certains jours de l'année ou lors de circonstances bien spécifiques.

**Plus il est possible de réduire le périmètre à prendre en compte, plus les travaux ultérieurs seront facilités.**

**À ce stade il est possible d'établir une fiche par processus faisant apparaître :**

- **le nom du processus**
- **le nom du responsable**
- **la description du processus (avec les enjeux et contraintes)**
- **les interfaces et flux externes**
- **les activités métier rattachées**
- **le niveau de service minimum (et modes dégradés acceptables)**
- **les attentes en matière de continuité (DMIA, PRMA)**
- **l'appréciation de la criticité du processus**
- **les conséquences (et les coûts) d'une interruption d'activité**
- **les ressources critiques associées**
- **les interdépendances critiques (en amont, en aval, avec des partenaires)**

# LA DÉMARCHE DE GESTION DU RISQUE POUR LES ACTIVITÉS ESSENTIELLES

**OBJECTIF**

Assurer l'atteinte des objectifs de l'organisation en minimisant le risque de catastrophe.

➡ **La gestion de risque a pour objectif de limiter les effets de l'incertitude sur l'atteinte des objectifs de l'organisation.** C'est un travail d'anticipation qui consiste à identifier les risques potentiels, à en évaluer les effets possibles et la probabilité d'occurrence, de manière à pouvoir définir l'ordre de priorité des actions à conduire pour limiter l'impact et la vraisemblance des risques identifiés comme majeurs. Cette démarche permet de rationaliser les choix et d'optimiser la protection grâce à laquelle l'organisation va pouvoir atteindre ses objectifs dans le respect des ressources qu'elle est prête à dégager.

**La gestion du risque comprend 4 étapes :**

1. **Identifier** les risques de toutes natures (dans une approche « tous risques »).
2. **Analyser** les risques (selon les critères de fréquence et de gravité) en les regroupant par scénarios significatifs.
3. **Évaluer** ces risques en fonction du contexte et des enjeux de l'organisation (activités, chaîne de valeur, conjoncture, opportunités, concurrence, moyens financiers, grands choix stratégiques…).
4. **Traiter** ces risques pour en limiter la probabilité d'occurrence et les impacts.

La démarche, décrite de manière approfondie dans les fiches suivantes, amène à effectuer une **cartographie des risques,** contribuant à donner une vision globale, puis à faciliter une décision quant à la stratégie de gestion de ces risques. L'adoption de processus cohérents et « tous risques » dans un cadre organisationnel complet peut contribuer à garantir que le risque est géré de façon efficace, performante et cohérente au sein d'une organisation, qu'elle soit publique ou privée. *Cependant, afin de mettre en place rapidement un plan de continuité, il est possible de se limiter à une analyse des effets des principaux scénarios de crises, quelles qu'en soient les causes, sans chercher à limiter ou prévenir les sources de risque. Il suffit alors d'aller directement à la fiche relative aux scénarios à prendre en compte dans le PCA.*

**Il est recommandé :**

- De connaître les risques et de mener une analyse de risque qui tienne compte des probabilités d'occurrence des événements craints, de leurs impacts sur le fonctionnement des activités de l'organisation, sur sa capacité à satisfaire ses clients et identifier les catastrophes contre lesquelles il est prioritaire de se protéger.
- De prendre en compte les aléas et les menaces de nature humaine, dans une démarche « tous risques ».
- D'identifier explicitement les incidents contre lesquels l'analyse de risque conclut à leur acceptation et donc à l'absence de besoin de développer des mesures particulières de protection.
- De rédiger autant de composantes du PCA global que de scénarios d'incidents contre lesquels il a été jugé utile de se prémunir.
- De formaliser et d'enregistrer les hypothèses faites et les conséquences imaginées lors de la définition des scénarios d'incident.
- D'identifier les partenaires et organismes extérieurs à l'organisation qui pourraient être également impliqués dans la gestion du sinistre ou de ses conséquences.
- De reprendre régulièrement l'analyse de risque effectuée pour en vérifier la pertinence.

# IDENTIFIER LES RISQUES

**OBJECTIF**

Les risques doivent être identifiés à différents niveaux de l'organisation (groupe, division, département, unité d'affaires) puis en fonction des objectifs qui peuvent être affectés par le risque (stratégique, opérationnel, gouvernance et conformité).

➡ Dans cette étape d'identification des risques, et pour un niveau d'organisation donné, **l'approche par les objectifs qui peuvent être affectés permet d'aider à répertorier les risques dont certains peuvent être ni perçus ni reconnus :**

- **Risques de nature stratégique** (p.ex. indisponibilité des matières premières rares ou de ressources critiques, inaccessibilité de certains pays, perte d'image ou de notoriété, sécurité économique, hausse importante du coût du carburant, rupture majeure d'énergie, insuffisance de trésorerie, cession d'activité d'un client ou d'un fournisseur essentiel…).
- **Risques opérationnels** (p.ex. inaccessibilité d'une infrastructure par suite de catastrophe naturelle, technologique, d'acte de terrorisme, de conflit social ou de coupure/indisponibilité de voies de communication, ou indisponibilité du système d'information par suite d'intrusion à travers les réseaux à des fins malveillantes, ou encore indisponibilité du personnel consécutive à une pandémie…).
- **Risques liés à la gouvernance et à la communication de l'information** (p.ex. manque d'information, de coordination, de cohérence, d'anticipation, hétérogénéité des systèmes d'information décisionnels, fonction de pilotage déficiente, absence de décision…).
- **Risques de conformité et juridiques** (p.ex. non-respect des règles prudentielles, de sécurité sanitaire, de protection des travailleurs ou de l'environnement…).

Le pilotage fin de ces travaux est indispensable pour assurer une cohérence, car la tendance d'un responsable est souvent de sous-estimer les risques (parce qu'un risque donné ne s'est jamais produit ou bien parce que l'on souhaite inconsciemment cacher certains risques) ou au contraire de les surestimer (par exemple pour justifier une hausse du budget).

**Il est recommandé** d'étudier les risques économiques qui pèsent sur l'organisation par suite d'actions malveillantes : vols d'informations, de savoir-faire et de secrets de fabrication, contrefaçons et atteintes à la propriété intellectuelle, pertes de données après un sinistre ou une erreur de manipulation, intrusions dans le système informatique, mises hors service des ressources informatiques, débauchage de salariés, risque financier par prise de capitaux extérieurs, mises en cause au plan légal et actions de justice, atteintes à l'image de marque et à la réputation, etc. Ces actions touchent aux objectifs stratégiques ou opérationnels.

Il est nécessaire de définir les limites des risques pris en compte (les scénarios retenus sont ceux qui restent dans le champ du vraisemblable, sinon la liste serait beaucoup trop longue et risquerait de nuire à la crédibilité du travail. Cependant, il peut être utile de prendre en compte des scénarios très peu vraisemblables (très faible probabilité, mais conséquences très graves) pour tester la capacité de l'organisation à réagir dans ces circonstances extrêmes et vérifier la capacité des PCA à répondre à de tels sinistres, sauf à vouloir les traiter par une approche exclusivement assurantielle.

Page suivante

L'approche « tous risques » permettant d'optimiser le dispositif de sécurité de l'organisation repose sur la prise en compte d'un ensemble des risques, tels que ceux présentés dans la liste indicative ci-dessous, qui permet de les sérier selon quatre grands types :

### 1. RISQUES STRATÉGIQUES

- Concurrence.
- Risque clients.
- Risque fournisseurs.
- Indisponibilité des matières premières rares.
- Risques pays.
- Perte d'image ou de notoriété.
- Risques économiques.
- Hausse importante du coût de l'énergie.
- Déséquilibre du bilan.
- Risques de liquidité.

### 2. RISQUES OPÉRATIONNELS

➡ **Risques naturels, sanitaires et environnementaux :**

- Risques sanitaires.
- Risques pandémiques.
- Risques vétérinaires.
- Perturbations météorologiques graves (tempêtes, cyclones, tornades, orages violents).
- Risques d'inondation.
- Autres aléas naturels (séismes, tsunamis).
- Températures extrêmes (sécheresse, neige…).
- Incendies.

➡ **Risques technologiques ou accidentels : risques d'accidents majeurs (transports, informatiques, énergie, distribution de l'eau…) :**

- Risques technologiques.
- Risques liés aux substances nucléaires, radiologiques, biologiques ou chimiques.
- Risques d'explosion.
- Accident industriel.
- Risques de vieillissement des installations et infrastructures.
- Risques accidentels de pollution.
- Indisponibilité d'alimentation en énergie.
- Indisponibilité d'alimentation en eau.
- Indisponibilité de téléphonie.
- Indisponibilité d'Internet.
- Défaillance d'un processus.
- Défaillance d'un système interne.

➡ **Risques provoqués :**

- Malveillance.
- Intrusion.
- Actions de destruction et de sabotage.
- Menace par explosion et engin explosif improvisé.
- Menaces informatiques.
- Vol d'informations sensibles.
- Contrefaçons.
- Menaces nucléaires, radiologiques, biologiques et chimiques.

### 3. RISQUES DE GOUVERNANCE

- Absence de tableau de bord pertinent.
- Fonction de pilotage déficiente.
- Absence de coordination.
- Manque d'anticipation.
- Hétérogénéité des systèmes d'informations décisionnels.

### 3. RISQUES DE CONFORMITÉ

- Responsabilité civile et pénale.
- Règles sanitaires des produits alimentaires
- Protection des travailleurs.
- Protection de l'environnement.
- Prise en compte des risques des sous-traitants, y compris à l'étranger.
- Filière d'approvisionnement.
- Enjeux de développement durable.
- Obligations d'informations sociales et environnementales (loi Grenelle II).

# ANALYSER ET CARACTÉRISER LES RISQUES

**OBJECTIF**

Caractériser les risques par leurs composantes.

➡ **Un risque peut être caractérisé par trois composantes :**

- **La menace** (qu'elle soit d'origine humaine ou résulte d'un aléa) ou le scénario matérialisant la source de risque.
- **La/les vulnérabilités** que la menace/scénario peut exploiter pour avoir des impacts.
- **Les impacts,** classés selon le niveau de gravité et le type (humain, financier, environnemental, relations avec les partenaires, juridique, valeur, image) et appréciés en fonction des objectifs de l'organisation.

Le produit des deux premières composantes permet d'exprimer la probabilité (ou plausibilité) d'un événement, source de risque pour l'organisation.

➡ **Il ne reste plus alors que deux composantes : la probabilité d'occurrence (1) et l'impact (2).**

**1. On analyse la probabilité d'occurrence** d'une source de risque en utilisant des seuils tels que ceux exprimés dans le tableau « probabilité d'occurrence » page suivante.
Il est conseillé de prendre une échelle avec des niveaux dans un rapport de 10 (comme illustré dans le tableau page suivante).
La probabilité est facilement mesurable quand il s'agit de sinistres statistiquement connus (risques naturels notamment). Quand il s'agit d'un risque provenant d'une action humaine, avec des modes opératoires nouveaux, il est possible de calculer la probabilité (ou vraisemblance) par la combinaison de trois éléments qui

**ANALYSE DE RISQUE**

RISQUE = MENACE X VULNÉRABILITÉ X IMPACT

RISQUE = PROBABILITÉ X IMPACT

La vulnérabilité représente les facteurs intrinsèques ou faiblesse d'un système qui le rendent sensible ou fragile devant un ou plusieurs types de menaces ;
quand la menace se concrétise par un événement explicite, la vulnérabilité contribue à augmenter la gravité des impacts.

Exemples de vulnérabilités :

- Protection insuffisante des points d'importance vitale.
- Non mise à jour des logiciels.
- Sécurité insuffisante d'un site chimique.
- Existence de portes dérobées.
- Absence de détection de la menace par explosifs (IED).
- Localisation de répartiteur basse tension dans les sous-sols inondables.
- Protection insuffisante des données sensibles.
- Co-localisation du site de secours.
- Personnel mal formé.
- Fournisseur unique de prestations essentielles, etc.

Page suivante

caractérisent la menace : la motivation, le savoir-faire, la disponibilité des moyens, et de deux éléments qui caractérisent la vulnérabilité : failles et portes dérobées, fragilité de la cible (qu'il s'agisse d'infrastructures, de processus, de systèmes d'information, d'êtres humains ou de prestataires externes).
Les risques, naturels et technologiques, sont caractérisés par un aléa, défini comme un événement potentiellement dangereux et un impact défini préalablement.

**2. L'analyse des impacts** doit se faire en fonction de critères homogènes au sein de l'organisation, par exemple en s'inspirant du tableau « analyse des impacts » ci-dessous.
Pour cette mesure d'impact il est également conseillé de prendre des niveaux dans un rapport de 10.
La durée de l'interruption d'activité est un élément important des impacts. À titre d'exemple, le rétablissement des sites informatiques inondés peut prendre deux à six semaines, parfois plusieurs mois : il faut pomper l'eau, sécher, contrôler les câblages et matériels, rééquiper, requalifier, etc.
Il est nécessaire de prendre en compte les conséquences venant des fournisseurs considérés au sens très large. À titre d'exemple, un site localisé en zone non inondable peut être fortement touché par les effets d'une inondation : d'abord par des coupures d'électricité compensées par la mise en fonctionnement de groupes électrogènes, puis par la pénurie de fuel causée par l'impossibilité de livraison, et finalement par l'absence de personnel par suite de l'arrêt des moyens de transport.

Il est recommandé de :
- Regrouper les risques identifiés en quelques scénarios dimensionnant, pour donner plus de réalité et également pour prendre en compte simultanément plusieurs risques concomitants avec effets aggravants (par exemple l'indisponibilité des moyens de communication durant une catastrophe naturelle).
- Bien prendre en compte les interdépendances et effets en cascade.

Ce travail est fait avec le responsable identifié pour chaque risque et ayant autorité pour gérer ce risque. L'annexe 4 donne un exemple de fiche d'analyse d'un type de risque pour un scénario de grand froid.

| Probabilité d'occurrence ou vraisemblance | Niveau | Description | Mesure de la probabilité sur 5 années |
|---|---|---|---|
| Très forte | 5 | Probabilité presque certaine | > 50% (1 chance sur 2) |
| Forte | 4 | Probabilité forte ou attaque très probable (devrait survenir à court terme) | > 5 % (> 1 chance sur 20) |
| Moyenne | 3 | Probabilité plausible ou attaque plausible (pourrait arriver) | > 0.5 % (> 1 chance sur 200) |
| Faible | 2 | Peut intervenir occasionnellement | > 0.05 % (> 1 chance sur 2000) |
| Très faible | 1 | Probabilité très faible ou attaque improbable. Peut intervenir dans des circonstances exceptionnelles | < 0.05 % (> 1 chance sur 20 000) |

| | Niveau moyen de l'impact | Types d'impact | Sous critères | Valeur de l'impact par sous critères et commentaires éventuels |
|---|---|---|---|---|
| Mineur | 2 | Humain | 1.1 Nombre de morts<br>1.2 Nombre de blessés | 1<br>2 |
| | | Social | 2.1 Nombre de personnes<br>2.2 Effet psychologique | 2<br>2 |
| | | Financier | 3.1 Coût global | 2 |
| | | Contractuel | 4.1 Incidences sur les engagements | 2 |
| | | Opérationnel | 5.1 Effets directs<br>5.2 Déficience des sous-traitants | 3<br>3 |
| | | Environnement | 6.1 Impact environnemental | 1 |
| | | Image | 7.1 Impact sur la réputation | 1 |
| | | Juridique | 8.1 Responsabilité civile ou pénale<br>8.2 Obligations réglementaires | 1<br>2 |

# ÉVALUER LES RISQUES

**OBJECTIF**

Hiérarchiser et apprécier les risques.

➔ **Suite à l'analyse des risques, l'évaluation consiste d'abord à hiérarchiser les risques, en utilisant les critères de probabilité et d'impact définis précédemment.** Une matrice du type de celle ci-dessous peut être utilisée à cet effet.
L'évaluation consiste ensuite à apprécier les risques par rapport au contexte de l'organisation, pour définir ceux qui sont acceptables et ceux qui nécessitent un traitement.

Il faut notamment apprécier les risques auxquels l'organisation sait résister, les avantages que certaines activités peuvent retirer de cette prise de risque et au contraire les inconvénients que d'autres parties de l'organisme devront subir si les risques devaient se concrétiser. Il faut également que les décisions respectent les obligations réglementaires ainsi que les autres exigences auxquelles l'organisation est soumise.

Dans une approche plus rigoureuse et afin de pouvoir additionner certains risques, il est préconisé de garder les niveaux de mesure dans un rapport de 10 plutôt que de les remplacer par la seule référence au niveau proposée pour l'exemple page suivante.
La matrice d'évaluation prend alors la forme du tableau page suivante « Gestion du risque d'évaluation - autre version ».
Ce schéma peut encore être critiqué, parce qu'il donne le même poids à un risque de très faible probabilité et de très fort impact qu'à un risque de très forte probabilité et de très faible impact. On peut considérer en effet qu'un incident fréquent est bien connu, et les mesures de réponses sont assimilées en mode réflexe. A contrario, un risque extrêmement rare est souvent négligé et les instruments de réponse peu développés. De plus, quand l'impact est très élevé les conséquences ressenties sont amplifiées par les effets sur les partenaires, l'impact sur la vie sociale, les phénomènes aggravants de la médiatisation et *in fine* les conséquences sur l'image, la survie de l'organisation et la société en général. Pour ces raisons il peut être préférable de donner plus de poids à l'échelle des impacts. Il en résulte la matrice page suivante « Gestion du risque d'évaluation - autre version pondérée ». Malgré son apparente complexité, elle peut s'avérer plus opérationnelle.

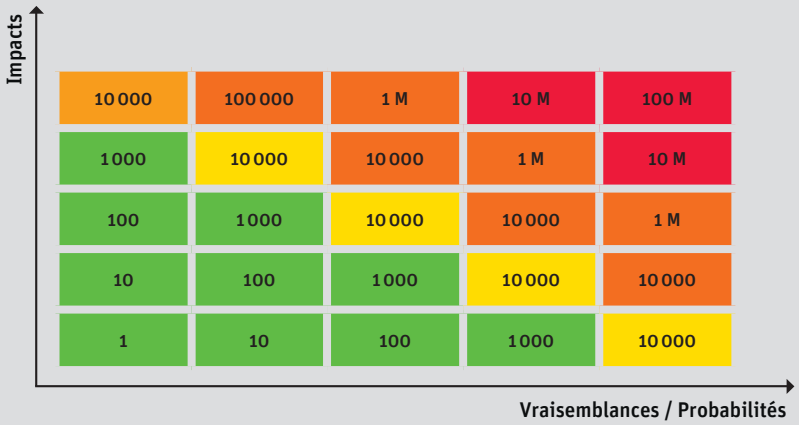
| | Impacts | | | | |
|---|---|---|---|---|---|
| **Probabilité** | Catastrophique 5 | Majeur 4 | Modéré 3 | Mineur 2 | Insignifiant 1 |
| Très forte 5 | 10 | 9 | 8 | 7 | 6 |
| Forte 4 | 9 | 8 | 7 | 6 | 5 |
| Moyenne 3 | 8 | 7 | 6 | 5 | 4 |
| Faible 2 | 7 | 6 | 5 | 4 | 3 |
| Très faible 1 | 6 | 5 | 4 | 3 | 2 |

Niveau de risque encouru

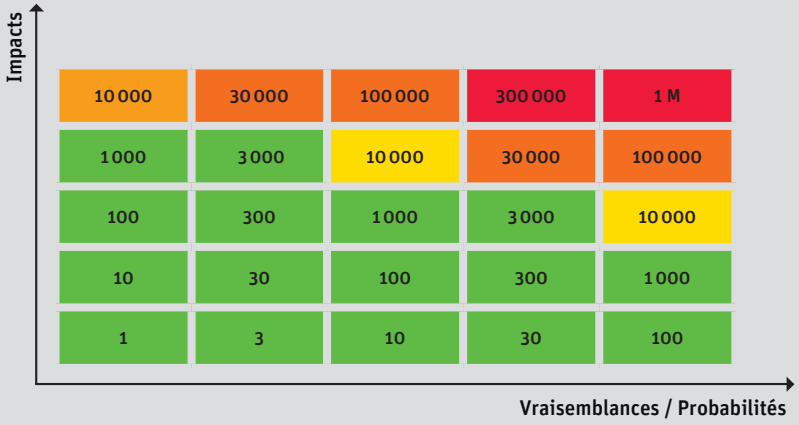
| | | | |
|---|---|---|---|
| 9 ≤ Risque extrême ≤ 10 | 7 ≤ Risque élevé ≤ 8 | 5 ≤ Risque moyen ≤ 6 | 1 ≤ Risque faible ≤ 4 |

Page suivante ➡

**GESTION DU RISQUE D'ÉVALUATION**
(AUTRE VERSION)




**GESTION DU RISQUE D'ÉVALUATION**
(AUTRE VERSION PONDÉRÉE)



# TRAITER, TRANSFÉRER, ÉVITER OU ACCEPTER LES RISQUES IDENTIFIÉS

**OBJECTIF**

Définir les manières de prendre en compte les risques.

➡ **En cohérence avec la norme ISO 31000, le traitement du risque peut inclure les actions de types suivants :**

- **Un refus du risque** en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque.
- **La prise ou l'augmentation d'un risque** afin de saisir une opportunité.
- **L'élimination de la source de risque,** par exemple en relocalisant des bureaux pour les éloigner d'un zone inondable.
- **Une diminution de la probabilité d'occurrence** ou de la vraisemblance, par des actions de prévention, de protection et de détection[13] (mesures de protection physique ou logique, sensibilisation et mesures comportementales, détection rapide de signaux précurseurs, contrôle interne, actions de dissuasion face à des menaces humaines, intervention préventive…).
- **Une modification des conséquences,** par des mesures de protection et de limitation des impacts directs (durcissement des points névralgiques, protection du personnel, détection rapide d'un incident anormal, capacités et procédures d'intervention et de gestion de crise…).
- **Un partage du risque** avec une ou plusieurs autres parties (incluant des contrats d'assurance du risque).
- **Un maintien du risque** fondé sur un choix argumenté.

➡ **S'agissant des risques assumés,** l'organisation doit chercher à tout faire pour en limiter l'occurrence et les impacts (actions de type 4 et 5), afin d'arriver à **un risque résiduel acceptable.** Les solutions retenues nécessiteront des ressources et auront un coût, qui devra être validé par la direction.

➡ **La sensibilisation des « responsables de risques »** au sein de l'organisation est nécessaire à l'adoption d'une démarche homogène et cohérente visant à déterminer et proposer les niveaux de risques acceptables. Une validation de la direction reste indispensable. Elle permettra de déterminer les risques nécessitant un traitement et l'ordre de priorité dans la mise en œuvre des traitements.

**La direction centrale du renseignement intérieur (DCRI), la direction de la protection du secret de défense (DPSD) et la gendarmerie nationale peuvent aider à protéger les organisations :** Ces trois services de l'État sont fortement impliqués dans la prévention des ingérences contre les institutions et les entreprises qui constituent le tissu économique national. À ce titre, ils disposent d'une expertise dans le domaine de la protection physique et économique des entreprises.

**L'agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de sécurité des systèmes d'information.** A ce titre, elle met à disposition gratuitement sur son site (http://ssi.gouv.fr) un certain nombre de guides et de recommandations.

13 / Exemple des mesures du plan Vigipirate, qui visent à limiter le risque d'événement de nature terroriste.

# QUELS SCÉNARIOS DE RISQUES PRENDRE EN COMPTE ?

**OBJECTIF**

Retenir des scénarios en fonction des conséquences appréciées au regard des objectifs et obligations de l'organisation.

➡ **La démarche simplifiée ne s'intéressera qu'aux effets sur la disponibilité**, en prenant en compte suffisamment de scénarios pour couvrir la plupart des conséquences sur les ressources critiques :

- Infrastructures (bâtiments, locaux, moyens de transport…).
- Systèmes d'information (systèmes informatiques, serveurs, données internes, moyens de télécommunication, réseau local, messagerie, accès Internet…).
- Ressources humaines (équipes disponibles, renforts, personnes clefs, qualifications, compétences, motivation…).
- Ressources intellectuelles ou immatérielles (données internes, informations à protéger…)
- Prestations externes (eau, énergie, sous-traitants…) ou produits critiques (matières premières rares).

**… tout en précisant l'étendue du sinistre :** organisation entière ou zone géographique et activités touchées.

Les effets sur les ressources critiques ont des conséquences sur les processus critiques et donc sur le niveau de service ou l'interruption d'activités essentielles. Chaque interruption de processus critique et donc d'activité essentielle a des conséquences mesurables en terme de coûts. Grâce au tableau suivant on dispose de scénarios d'indisponibilité et l'on peut calculer les conséquences des interruptions ou indisponibilités des ressources critiques, permettant de trancher sur l'opportunité de développer des PCA (cette question est traitée de manière approfondie, avec la prise en compte du coût du PCA).

**EXEMPLE DE TABLEAU DE SCÉNARIO DE RISQUES**
(AVEC UNE QUANTIFICATION DES EFFETS SUR LES RESSOURCES CRITIQUES)

| | local | route | moyen de transport | système d'information | ressource humaine | ressource intellectuelle | fournisseur et sous-traitance | produit critique |
|---|---|---|---|---|---|---|---|---|
| Catastrophe naturelle : inondation | 4 | 4 | 4 | 3 | 3 | 2 | 1 | 2 |
| Catastrophe naturelle : tempête | 2 | 4 | 4 | 3 | 2 | 2 | 1 | 2 |
| Grave accident | 4 | 1 | 1 | 4 | 4 | 2 | 3 | 1 |
| Crise sanitaire | 1 | 1 | 3 | 2 | 4 | 2 | 3 | 1 |
| Attentat terroriste | 4 | 1 | 1 | 1 | 4 | 3 | 2 | 2 |
| Crise sociale | 1 | 1 | 4 | 1 | 4 | 2 | 3 | 3 |
| Arrêt électricité | 3 | 3 | 3 | 4 | 2 | 1 | 3 | 3 |
| Arrêt Telecom ou Internet | 3 | 2 | 2 | 4 | 2 | 3 | 3 | 2 |

**1** = très faible - **2** = faible - **3** = fort - **4** = très fort

Page suivante

**➡ Conséquences pour le périmètre du PCA :**
- Le PCA doit prendre en compte les scénarios qui conduisent à des situations inacceptables ; néanmoins certains scénarios peuvent être traités par la direction concernée sans faire appel au PCA (par exemple la direction juridique).
- Le périmètre du PCA peut être variable selon la taille, la nature ou la complexité de l'organisation.
- Le PCA doit comprendre au minimum les risques opérationnels, pour lesquels l'interruption d'activité résulte de la perte de ressources critiques.
- Il est recommandé de faire valider le périmètre du PCA par la direction générale.

L'analyse des conséquences de pertes de ressources critiques sur la continuité d'activité et de l'acceptabilité de ces interruptions d'activité ou dégradations de niveau de service, conduit à intégrer a priori dans le PCA une liste de scénarios.
Cependant, la gestion du risque apporte deux éléments complémentaires :
- La mesure de la probabilité d'occurrence.
- L'appréciation du risque résiduel après les mesures de traitement.

La liste évoquée précédemment peut donc être réduite,
- Soit parce que l'analyse de la probabilité d'occurrence ou les mesures de prévention rendent cette probabilité trop faible pour justifier une action de continuité ou parce que d'autres réponses sont plus pertinentes (par exemple une police d'assurance).
- Soit parce que l'organisation est prête à assumer et accepter un risque et les conséquences associées, sans action complémentaire.
- Soit parce que les mesures de protection prises rendent les conséquences acceptables.

**Pour chaque scénario finalement retenu dans le PCA, il est recommandé d'indiquer :**
- S'il y a des mesures particulières de prévention ou protection.
- Les impacts principaux sur l'organisation et ses capacités (chiffrés).
- Les indices permettant d'identifier le début de la crise.
- Les critères permettant de mesurer l'ampleur du sinistre.

# DÉFINIR LES OBJECTIFS DE CONTINUITÉ EN MODE DÉGRADÉ ET POUR LA REPRISE D'ACTIVITÉ

**OBJECTIF**

Passer de la définition des besoins de continuité à celle des d'objectifs de continuité.

**À ce stade, il s'agit de fixer des objectifs de continuité à atteindre compte tenu des besoins dans l'absolu et des scénarios de sinistre retenus.** Ces objectifs portent sur les activités et par suite sur les processus et sur les ressources critiques. L'atteinte de ces objectifs requerra des moyens spécifiques et des coûts associés, qui pourront conduire à revoir lesdits objectifs (voir la fiche 19 sur le bilan coût/avantage du PCA). À la suite de cette confrontation entre le coût de l'interruption d'activité et le coût du PCA proposé, et compte tenu de la probabilité d'occurrence, la stratégie de continuité pourra être finalisée.

➡ **Les objectifs de continuité (en matière de disponibilité) :** Nous n'évoquons pas ici les objectifs à fixer en matière de prévention et protection (qui font l'objet du traitement des risques) mais les objectifs à fixer en matière de continuité d'activités. Ces derniers sont formalisés par des indicateurs qui quantifient d'une part (1) **l'exigence concernant les systèmes en place** (pour rendre possible la continuité d'activité) et d'autre part (2) **l'exigence concernant les modalités de la réponse mise en œuvre** à la suite d'un sinistre (pour assurer une continuité d'activité conforme aux objectifs de l'organisation) :

1. **Perte maximale susceptible de résulter des impacts directs du sinistre** et qu'il ne faut pas dépasser pour rendre possible la continuité d'activité, par exemple :
- Perte de Ressources Maximale Admissible (PRMA) pour permettre une reprise,
- Perte de Données Maximale Admissible (PDMA), dans le domaine informatique, qui implique de définir les modalités de sauvegarde, duplication, reprise des données et redémarrage (il peut n'y avoir aucune perte en cas de réplication synchrone ou des pertes partielles en cas de redémarrage progressif selon un ordre de priorité prédéfini).

**Ces indicateurs doivent permettre de quantifier le niveau minimum qui doit subsister juste après le sinistre pour permettre la mise en œuvre des solutions de continuité.**

2. **Exigences de délais pour la reprise d'activité** (par la mise en œuvre planifiée d'une solution palliative, puis d'une solution de secours en mode dégradé et enfin la reprise des conditions normales) qui s'imposent aux solutions à mettre en œuvre :
- Durée Maximale d'Interruption Acceptable (DMIA), avant de disposer d'une solution de contournement palliative (qui mobilise des processus spécifiques et fait généralement appel à des procédures manuelles). Le dépassement de cette durée maximale d'interruption, pouvant résulter de la non-fourniture d'un produit ou d'un service ou de la non-réalisation d'une activité, aurait des conséquences défavorables qui seraient inacceptables pour la tenue des objectifs ou des obligations de l'organisation. Afin de tenir cet objectif de DMIA il est nécessaire de préciser la ressource critique/non critique concernée, les indicateurs précis, le niveau de service attendu (fonctionnement en mode dégradé), les conséquences indirectes…
- Durée Maximale de Reprise technique Prévue (DMRP) – avant de fonctionner selon le mode de secours ou le mode nominal prévu (et donc reprise partielle ou totale des moyens techniques et informatiques). La décision de

Page suivante

déclencher le mode secours est souvent une décision qui ne peut plus être annulée (on ne peut plus faire « machine arrière »).

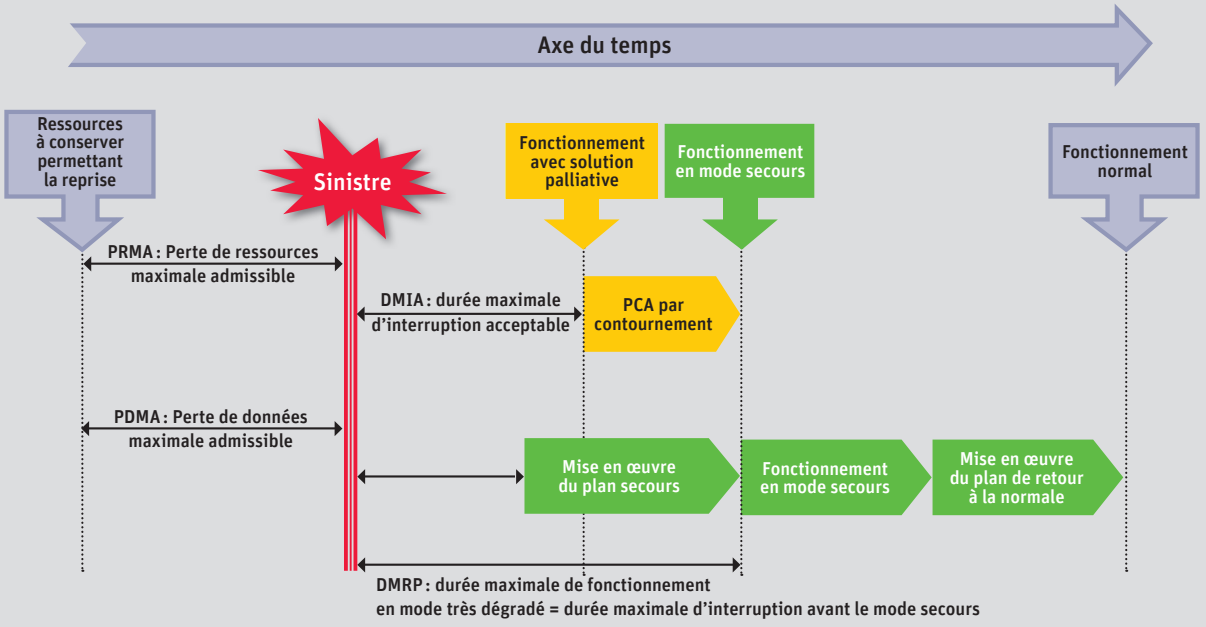
Le retour à la normale peut se faire par paliers successifs, chaque étape étant alors associée à un objectif de durée maximale. Ce continuum est représenté dans le diagramme ci-dessous.

Quand il y a plusieurs DMIA, la plus contraignante est la DMIA la plus faible, mais les autres valeurs de DMIA, les durées maximales de fonctionnement en mode dégradé et les valeurs de DMRP ont également des conséquences importantes sur les ressources techniques et procédures à mettre en œuvre, qui devront être valorisées.

➔ **La définition des objectifs de sécurité** (en matière d'intégrité, de confidentialité, de traçabilité, d'évolutivité et de sûreté) permet de préciser les objectifs de continuité.
Dans cette perspective on peut identifier :

- **Une perte de qualité**, voire un vol ou une détérioration volontaire des ressources, du produit ou du service fourni, qui peuvent se traduire par l'arrêt de la prestation correspondante. Il est par conséquent nécessaire de déterminer le niveau de seuil d'acceptabilité[14] du produit/service final. L'effet étant voisin de l'indisponibilité d'un produit/service, il peut être traité par une démarche voisine, nécessitant la mise en place rapide d'un plan de continuité adapté.

**FIXATION DES OBJECTIFS POUR ASSURER LA CONTINUITÉ D'ACTIVITÉ**




PDMA mesure le temps maximum acceptable durant lequel les données sont perdues, car elles ne peuvent pas être reconstituées ; il est nécessaire de recourir aux dernières données sauvegardées.

DMIA mesure la durée d'interruption de fonctionnement du processus au-delà duquel les conséquences deviennent intolérables.

DMRP (délai maximum de reprise technique prévu) mesure la durée d'interruption de fonctionnement des parties techniques du processus avant la reprise en mode secours. Cela correspond à la durée maximale de fonctionnement acceptable en mode très dégradé.

14 / Il existe des techniques pour définir ce seuil et assurer son maintien en situation normale (cf. Six sigma).

Page suivante

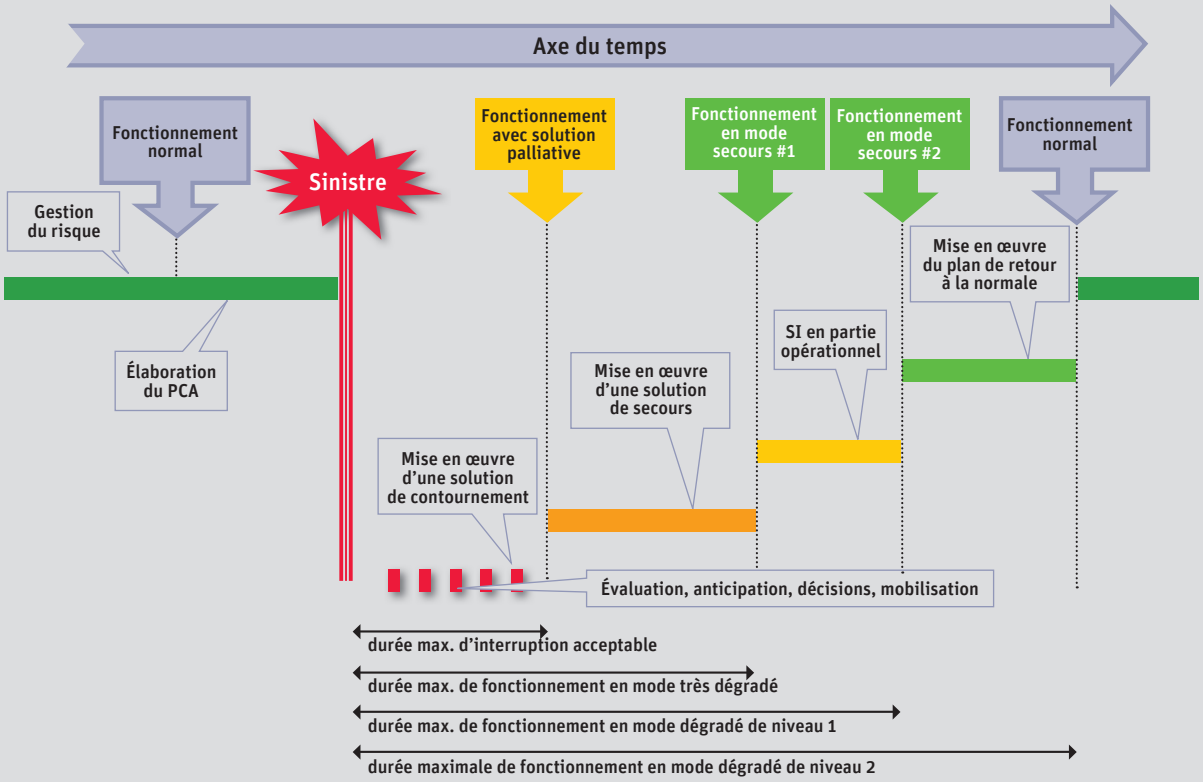
• **Une perte d'intégrité** amène dans un premier temps à localiser les produits/services défectueux, assurer leur cloisonnement s'il y a un risque de propagation, les récupérer, puis les substituer par des produits intègres. Ces tâches nécessitent une très grande réactivité quand il s'agit de produits périssables qui sont passés dans la chaîne de distribution et qui ont une durée de vie courte. L'indisponibilité du produit/service concerné peut être plus ou moins longue.

• **Une perte de confidentialité,** qui couvre un champ très large et doit faire l'objet d'une étude spécifique. Elle peut résulter d'intrusions dans les systèmes d'information avec des conséquences très graves, comme la remise en cause ou l'arrêt de certaines activités.

• **Une perte de traçabilité** peut également, dans des situations extrêmes où le produit/service fourni est d'une grande valeur ou dangereux, conduire à l'arrêt de la prestation et donc à l'indisponibilité.

• **Une perte de sûreté,** conduisant à une action malveillante ou de nature terroriste se traduit généralement par une perte de disponibilité.

**DÉROULEMENT DU PCA**




Exemple d'un arrêt de l'activité suite à un sinistre, d'une reprise en mode dégradé, d'abord par une solution de contournement, puis par un fonctionnement en mode secours, avec deux paliers successifs, avant le retour à la normale.

# DÉFINIR LES EXIGENCES SUR LES RESSOURCES NÉCESSAIRES AU PCA

**OBJECTIF**

Approfondir les modalités de mise en œuvre des réponses proposées pour répondre aux objectifs de continuité, et à leurs implications (contraintes/exigences) sur les ressources internes et externes de l'organisation et les procédures.

**Cet objectif concerne :**
- Les systèmes d'information et de communication.
- Les processus et l'organisation.
- Les ressources intellectuelles.
- Les infrastructures.
- Les prestataires externes.
- Les relations avec les partenaires.
- Les relations avec l'État.

➡ **Exigences pour les ressources humaines**

Ces exigences portent **d'une part** sur les ressources nécessaires pour préparer la mise en œuvre du PCA :
- Désigner le directeur des risques, les responsables des risques, le responsable PCA et les correspondants PCA.
- Identifier les positions de travail critiques pour la continuité des activités essentielles.
- Évaluer le nombre nécessaire de ressources humaines et en particulier des postes critiques à maintenir (décisionnel et opérationnel).

Et **d'autre part** sur les dispositifs à préparer pour permettre la continuité des postes critiques :
- Maintenir techniquement les positions de travail critiques :
  - mécanisme d'astreinte,
  - travail à distance, télétravail[15],
  - accès (physique et logique) aux données des dossiers,
  - droits de lecture des espaces de stockage et de la messagerie,
  - création de nouveaux comptes,
  - travail depuis un site de repli,
  - disposer de capacité à modifier les annuaires et assurer leur diffusion,
  - capacité à conserver les mêmes numéros de téléphone, par redirection automatique,
  - polyvalence du personnel,
  - prévoir les mesures d'adaptation de l'organisation,
  - aménager le temps de travail, sociétés d'intérimaires,
  - protection des travailleurs concernés,
  - modalités de transport domicile-travail, covoiturage,
  - disponibilité de l'outil de travail (notamment des terminaux et moyens informatiques), des moyens de communication,
  - prise en compte de la sécurité informatique (sur les réseaux, sur le poste des agents),
  - prise en compte des mécanismes de sauvegarde des données durant le fonctionnement sur site de repli,
  - modalités de prise en charge des coûts de communication et de la responsabilité civile,
- Prévoir les incidences pour la convention collective, contrat de travail[16], règlement intérieur, responsabilité civile, rémunération, contrôle.
- Assurer une formation préalable, une sensibilisation au travail occasionnel à distance et la responsabilisation des personnes concernées.

**Pour la suppléance du personnel :**

Il est recommandé, pour tout poste sensible, de disposer du nom du titulaire et d'un suppléant. Prévoir un mécanisme de mise à jour des annuaires en cas de fonctionnement en mode dégradé.

15 / Circulaire de la direction générale du travail (DGT) 2007/18 du 18 décembre 2007.
16 / Même si l'article L. 1222-11 du code du travail précise qu'en cas de circonstances exceptionnelles le télétravail est considéré comme un aménagement du poste de travail.

Page suivante

• Il peut être utilement mis à la disposition du personnel un site web permettant de signaler depuis le domicile toute absence au travail. Le message est ensuite relayé au responsable concerné. En cas de sinistre, un tel outil permet de gérer les absences en nombre.
• La formation du personnel (et notamment des suppléants) doit apporter la capacité à assurer des positions de travail différentes.
• Il est recommandé d'avoir une gestion des connaissances dans l'organisation qui facilitera la rédaction du PCA et l'accès aux informations utiles par des personnes différentes et depuis des lieux différents des modalités habituelles.

### ➡ Exigences pour les systèmes d'information et de communication

Cette partie est parfois appelée plan de continuité informatique (PCI) par opposition au plan de continuité « métier » (PCM).
Les objectifs de DMIA, DMRP et PDMA ont des conséquences très directes sur les solutions techniques à prévoir :
• Découper le système d'information en plaques secourables homogènes.
• Réaliser une architecture du système d'information permettant de répondre aux exigences définies en termes de délai de secours et de perte de données maximale admissible :
- niveau de redondance et d'éloignement des centres de secours,
- système à haute disponibilité pour une partie des applications les plus critiques (réplication synchrone),
- système permettant une reprise à chaud, avec un redémarrage progressif des applications, par ordre de priorité,
- système permettant une reprise à froid, à partir de la dernière sauvegarde, avec gestion fine de la phase de recouvrement.

• Contractualiser les prestations externes en matière d'exigences de continuité d'activité, formaliser la maintenance avec des engagements de résultats.
• Disposer de moyens de télécommunication sécurisés de secours (par exemple accès par satellite, moyens radio privés, systèmes d'alerte robustes). Pour ce qui concerne l'État, des réseaux spécifiques hautement robustes de phonie et de transmission de données sont mis en œuvre. Ces réseaux, totalement indépendants des réseaux publics contribuent à la résilience en cas de catastrophe. L'adoption de tels dispositifs doit être envisagée par les organisations qui dépendent fortement des moyens de télécommunication pour assurer la gestion de crise et la mise en œuvre de leur PCA.

**Externalisation des sites de secours :**
• Solution attractive du point de vue financier (coût d'acquisition remplacé par un coût annuel du contrat).
• Vérifier cependant le niveau de service et les modalités de continuité, l'existence de séances d'entraînement, l'évolutivité au cours du temps, le risque que plusieurs clients du même site de secours fassent valoir leur droit au même moment, la protection des données pendant ou après l'utilisation du site de secours, etc.

**Les sauvegardes :**
• La procédure de récupération des sauvegardes doit être assez flexible pour pouvoir aussi bien relancer rapidement les systèmes critiques de l'organisation que relancer, même avec des délais accrus, l'ensemble du système.
• La procédure de récupération des sauvegardes doit être testée sur l'ensemble des serveurs et systèmes utilisés par une activité de l'organisation et vérifiée par les responsables « métier ».
• Il est également recommandé de disposer de vielles sauvegardes (6 mois à 1 an) pour améliorer la robustesse des procédures de sauvegarde.

**Les moyens de télécommunication :**
• Il est recommandé de vérifier les possibles vulnérabilités de l'opérateur (connaissance de l'architecture logique et physique, des dispositifs de sécurité et de continuité d'activité…).
• La multiplication d'opérateurs n'est pas forcément un gage de moindre vulnérabilité (une panne simultanée peut résulter du partage d'infrastructures entre opérateurs différents, de l'usage du même matériel ou d'un même fournisseur de logiciel).
• Il est recommandé de disposer de moyens de télécommunication indépendants d'Internet et des opérateurs publics (par satellite, par radio, par messagerie unilatérale « paging »,

Page suivante

par téléphonie fixe traditionnelle, en utilisant lorsque cela est possible des moyens sécurisés gouvernementaux) ainsi que de terminaux pouvant fonctionner sans alimentation électrique externe à l'organisation (courant secouru avec générateur interne, fonctionnement sur batterie).
Il convient d'utiliser ces moyens de télécommunication régulièrement en situation normale, pour pouvoir les utiliser aisément en situation exceptionnelle.

La fiche N°17 décrit plus en détail les mécanismes de relations avec les partenaires (prestataires, fournisseurs, sous traitants). Il est conseillé de se reporter à cette fiche pour plus d'informations concernant les bonnes pratiques avec les partenaires.

**➡ Exigences pour les processus et l'organisation**
L'objectif final étant de maintenir des applications « métier » critiques, les processus critiques correspondants doivent avoir été identifiés, avec les solutions permettant d'assurer leur continuité et respecter l'objectif de DMIA :
• Identifier les solutions de contournement par d'autres processus (par exemple ne faisant pas appel aux systèmes d'information) afin de tenir l'objectif de durée maximale d'interruption acceptable, avant de disposer d'une solution de contournement (DMIA). Cette solution palliative précède le fonctionnement en mode secours.
• Néanmoins il est de plus en plus difficile de fonctionner sans la ressource informatique (les données ne sont généralement plus disponibles sous forme papier). Il faut donc organiser la disponibilité de l'accès à un site distant disposant des informations « métier » essentielles, pour faciliter la continuité d'activité.
• Les priorités de reprise des processus doivent être définies, ainsi que les conditions qui permettent la reprise dans l'ordre prédéfini.

Par ailleurs, l'organisation doit disposer de la capacité à revoir et adapter les processus en fonction de l'évolution de la situation.
Enfin les processus spécifiques de mise en œuvre du PCA devront être définis et intégrés dans les processus de l'organisation.

**➡ Exigences pour les ressources intellectuelles**
Il s'agit d'exigences relatives au maintien de la disponibilité des ressources intellectuelles tenant compte de scénarios d'attaques économiques notamment par intrusion dans les systèmes d'information (pour plus de précisions à ce sujet, il est recommandé de consulter le Guide de l'intelligence économique dont les références figurent en annexe).

**➡ Exigences pour les infrastructures**
Il s'agit des mesures qui permettent aux sites critiques de fonctionner en mode dégradé, ainsi que les solutions permettant de basculer rapidement l'activité concernée vers des sites de replis :
• Installer les équipements techniques des sites critiques dans des zones mieux protégées (éviter les sous-sols inondables pour les équipements informatiques, les groupes électrogènes ou les répartiteurs à basse tension).
• Assurer une redondance de sites critiques, notamment des équipements informatiques, par des procédures de duplication adaptées aux objectifs de continuité, et une distance physique évitant de subir les mêmes dommages.
• Assurer le dimensionnement du site de secours en fonction des activités jugées critiques qui pourront y être localisées.
• Identifier des solutions de replis (capacité d'accueil, compatibilité technique, facilité d'accès, matériel de travail, ressources informatiques, dispositif d'activation, etc.).
• Pré-équiper les solutions de replis avec des dispositifs d'activation permettant le fonctionnement des activités relocalisées dans les délais prescris : délai maximal de reprise prévu pour fonctionner en mode secours (DMRP).

**➡ Exigences pour les prestataires externes et les partenaires**
Compte tenu de son importance, ce sujet est détaillé dans la fiche suivante.

**➡ Exigences pour le fonctionnement en mode dégradé**
Se reporter à la fiche N°15.

# DÉFINIR LES EXIGENCES VIS-À-VIS DES « PARTENAIRES »

**OBJECTIF**

Les « partenaires » recouvrent de nombreux types de structures en relation avec l'organisation. La compréhension de leurs fonctionnements est essentielle à la gestion de risque et à la continuité d'activité de l'organisation.

➡ **Le terme « partenaires » recouvre dans un premier temps tous les organismes externes qui apportent des services** dont dépend le bon fonctionnement de l'organisation. Ce sont notamment :

- **Les sous-traitants** qui effectuent des prestations de support à la demande, pour le compte du maître d'ouvrage (par exemple des tâches de maintenance, de formation, d'hébergement, de surveillance ou de travaux, pouvant aller jusqu'à la réalisation de tâches touchant directement le cœur de métier de l'organisation, avec des responsabilités pouvant aller jusqu'à la délégation de maîtrise d'ouvrage).
- Les prestataires de services externes (eau, énergie, télécom, fluides industriels) dont la fourniture est essentielle au bon fonctionnement de l'organisation.
- **Les fournisseurs** de matière première, en amont d'une chaîne logistique qui regroupe l'ensemble des flux de matières, d'informations et de ressources qui sont activés pour répondre à une demande de client.
- **Les gestionnaires** d'activités externes nécessaires au bon fonctionnement de l'environnement de l'organisation (par exemple la fourniture de transport collectif pour le personnel et le transport de marchandises, de colis et de courrier).

**Ces partenaires peuvent être qualifiés de critiques s'ils sont indispensables pour assurer la sécurité des activités essentielles de l'organisation et des processus critiques qui les sous-tendent.** La criticité est d'autant plus forte que les moyens de substitution sont difficiles à trouver, notamment dans les cas suivants :

- Importance du poids du partenaire dans la valeur ajoutée de l'organisation.
- Rareté de la matière première fournie.
- Unicité du fournisseur dans un domaine d'activité.
- Absence d'autres fournisseurs ayant la même qualité de service.
- Fonctionnement sans stock.

Dans de telles situations, la coopération s'impose et peut se matérialiser dans les termes du contrat qui lie le partenaire à l'organisation cliente. En effet, dans son analyse de risque l'organisation doit prendre en compte les risques provenant de ses partenaires, les évaluer et s'assurer que des solutions de traitement ont été définies. Cela suppose que l'organisation dispose d'une connaissance suffisante des risques (occurrence et impacts) de ses partenaires et des solutions mises en œuvre pour les limiter. Dans le prolongement de ce travail et pour ce qui concerne la continuité d'activité, l'organisation doit connaître les dispositifs prévus par son partenaire, la durée maximale d'interruption d'activité acceptable qui lui est garantie, les dispositifs permettant de fournir un service minimum et les modalités de ce fonctionnement en mode dégradé, ainsi que l'organisation et les procédures de gestion de crise.

Les termes du contrat vont donc au-delà de la simple formulation d'objectifs avec pénalités, car ils doivent permettre à l'organisation d'intégrer les risques et les mesures de sécurité et de continuité d'activité de son (ses) partenaire(s).

Pour les organisations qui assurent des prestations de prises de commande et livraison et qui contrôlent tout ou partie

Page suivante

d'une chaîne logistique il est recommandé de prendre connaissance de la spécification ISO/PAS/28001 qui définit les principes de gestion de la sûreté de la chaîne logistique. Cette spécification insiste sur la clarification entre les éléments que l'organisation contrôle et ceux qui sont sous le pilotage d'un partenaire. Il est alors recommandé de demander un audit ou une validation de la conformité du partenaire à cette spécification.

➡ **Plus généralement, plusieurs approches peuvent être utilisées par l'organisation vis-à-vis d'un partenaire :**

- Demander au partenaire une déclaration de conformité à des normes de gestion du risque et de continuité d'activité et l'autorisation de procéder à des revues[17] des processus et des installations, pour vérifier la validité des déclarations, ceci avec une fréquence déterminée en fonction du niveau de risque.
- Demander un certificat ou une validation officielle de conformité par rapport aux normes de gestion du risque et de continuité d'activité.
- Demander une confirmation de conformité avec des normes de gestion du risque et de continuité d'activité, assortie d'une vérification de cette conformité par une tierce partie de confiance.
- Ou instaurer une démarche coopérative, par l'élaboration commune de la stratégie de PCA et des dispositifs et procédures associés, et la recherche en commun d'améliorations continues.

Ces approches peuvent cependant susciter des réserves concernant l'accès à des informations sensibles, notamment dans un environnement concurrentiel ou quand les informations sont classifiées. L'organisation peut alors s'abstenir de demander ces informations à son partenaire, si celui-ci est certifié par un organisme tiers de confiance, accrédité par un organisme compétant, ou validé par un dispositif gouvernemental[18]. Ces procédures peuvent en outre générer un net avantage commercial pour les entreprises concernées.

Il est par conséquent recommandé que l'organisation associe ses partenaires à l'élaboration de son PCA, en couvrant notamment les domaines suivants :

- Formation commune.
- Partage d'expertise.
- Études de vulnérabilités.
- Analyses de risques.
- Formalisation des engagements de continuité (DMIA).
- Dispositifs de continuité.
- Mutualisation de moyens.
- Travail sur les processus transverses.
- Fonctionnement en mode dégradé.
- Conduite commune de projet.
- Exercices communs.

**La démarche habituelle pour limiter le risque fournisseur consiste à multiplier les fournisseurs, mais cette démarche se heurte à deux difficultés :**

- Elle génère un surcoût, par une perte d'économie d'échelle.
- Les fournisseurs différents peuvent présenter les mêmes risques.

**Il est par conséquent souhaitable de :**

- Dresser la liste des principaux contrats détaillant ce qui est garanti en cas de sinistre.
- Sensibiliser les fournisseurs au besoin de conduire une analyse de risque et de disposer d'un plan de continuité d'activité.
- Demander une certification de conformité à la norme ISO 22301.
- Conduire une analyse de risques en liaison avec les fournisseurs, et en déduire le niveau d'exigence de continuité à demander aux fournisseurs, qui soit compatible avec les objectifs de continuité de l'organisation.

17 / Ceci peut être facilité par l'accès aux systèmes d'informations : traçabilité des incidents, gestion événementielle, tableau de bord sur Internet, outils de suivis des actions.
18 / Par exemple, en application des conventions internationales douanières, le statut d'opérateur économique agréé (OEA), qui permet de distinguer les opérateurs communautaires les plus fiables, dans une logique de labellisation qualité (règlement n°1875/2006 du 18 décembre 2006).

Page suivante ➡

• Contractualiser le niveau du service demandé comprenant des engagements de qualité de service, de disponibilité, de Garantie de Temps de Rétablissement (GTR) ou durée maximale d'interruption acceptable (DMIA).
• Contractualiser éventuellement l'existence de moyens d'intervention ou de secours permettant de pouvoir fonctionner en mode dégradé ou limitant l'interruption d'activité à un seuil prédéfini (par exemple fourniture de groupe électrogène avec un droit prioritaire).
• Disposer d'une capacité d'appréciation de l'analyse de risque, des vulnérabilités et du plan de continuité d'activité du fournisseur.
• Avoir accès aux résultats des audits de la gestion des risques et du PCA du fournisseur.
• Préciser les responsabilités.
• Étudier les implications des cas de force majeure.
• Envisager la possibilité d'internaliser certaines fonctions.
• Définir des processus administratifs d'acquisition exceptionnels, en cas de dépassement des autorisations de plafond usuelles, dans des situations de très graves dégâts subis.

➡ **Une attention particulière devra être apportée aux interdépendances entre entités et notamment aux effets en cascade. La démarche suivante est proposée en ce sens :**

1. **La première étape** consiste à identifier les liens en chaîne entre les organisations,
• **Selon la nature de ces liens :**
- géographique (co-localisation et donc dépendance des parties communes, ou proximité créant une vulnérabilité aux catastrophes voisines : explosions, incendies, toxicité de l'atmosphère, etc.),
- logique, avec dépendance directe (fournisseur de produits ou service, ayant un rôle essentiel dans la chaîne d'approvisionnement),
- Logique, avec dépendance indirecte (moyens de transport publics, état des routes),
- fonctionnel (certains traitements dépendent de prestations assurées par des sous-traitants).

• **Résultant d'une vulnérabilité partagée** entre organisations sans lien entre elles :
- utilisation d'un même matériel ou logiciel critique,
- utilisation d'un même fournisseur de service (c'est typiquement le cas d'organisations différentes ayant sous-traité l'hébergement de leurs centres informatiques à une même société).
• **Consécutifs à une catastrophe** touchant une vaste zone géographique et par conséquent affectant directement des organisations indépendantes se trouvant dans cette zone ou, sans qu'elles soient directement affectées, subissant les contrecoups d'autres organisations directement affectées avec lesquelles elles ont de fortes interdépendances :
- crise sanitaire contagieuse grave,
- catastrophe naturelle.

2. **La deuxième étape** consiste à analyser les menaces, les vulnérabilités, les impacts et la propagation de ces impacts le long de la chaîne des interdépendances.
Il est alors possible de formaliser :
• Les exigences entre partenaires liés par contrats (cf. le cas des partenaires externes, vu au paragraphe précédent).
• Les spécifications de certaines installations ou fonctions dont la gestion est partagée, et qui devront respecter des exigences de continuité d'activité,
• Les modalités de coordination durant une crise (partage des renseignements de veille, des informations sur le sinistre, mise en réseau des responsables de PCA, constitution de dispositifs d'assistance et d'aide aux décisions, partage de l'analyse de situation).
• La mutualisation possible de certaines ressources permettant de faciliter la communication, l'intervention ou la continuité d'activité, sous réserve de règles de priorité d'accès.
• Les modalités de coordination après la phase d'urgence, quand il s'agit de reprendre les activités économiques, de prioriser collectivement l'enchaînement des étapes pour améliorer l'efficacité des efforts et la rapidité de la reprise.
• Le cas particulier de la chaîne logistique doit faire l'objet de la plus grande attention car elle inclut le pilotage des flux du four-

Page suivante

nisseur à l'utilisateur final pour atteindre l'objectif souhaité par l'organisation. La fonction de gestion de la chaîne logistique doit notamment assurer le lien avec les fonctions « achats », « relations clients » et « gestion de la vie des produits », tout en assurant les moyens pour la « fabrication » et la « maintenance/réparation ». Les effets d'une perte de ressource critique peuvent donc aisément se propager le long de la chaîne logistique, si les dispositifs décrits plus haut ne sont pas mis en œuvre.

➔ **Enfin, les « partenaires » recouvrent également les organismes externes qui reçoivent, en aval, des services ou des produits de l'organisation.** L'organisation doit en effet se préoccuper des conséquences que pourrait avoir un dysfonctionnement ou un arrêt de son activité sur son environnement direct ou indirect. C'est notamment le cas des opérateurs désignés « d'importance vitale » parce que leur bon fonctionnement est essentiel pour celui de la société (la sécurité ou la capacité de survie de la Nation, son potentiel de guerre ou économique, la santé ou la vie de la population)[19].
L'analyse de risque ne doit donc pas se limiter aux risques pour l'organisation, mais doit inclure les risques pour son environnement, ses partenaires situés en aval ou ses clients. Le plan de continuité doit ainsi prendre en compte les conséquences en aval, qui sont en dehors du périmètre strict de l'organisation, mais dont les besoins de continuité peuvent être très forts. Un tel travail peut nécessiter une collaboration avec les services de l'État, gardiens de l'intérêt général.

19 /Article R. 1332-1 du code de la défense.

# LES RELATIONS AVEC LES SERVICES DE L'ÉTAT

**OBJECTIF**

L'État assure différentes fonctions qui ont une place très importante dans l'analyse de risque, la prévention, la protection, la préparation et la gestion de crise, l'intervention et la mise en place de PCA. Il s'agit ici d'aider l'organisation à identifier ces fonctions.

**Le rôle de l'État, qui doit être intégré dans les PCA des entreprises, résulte de sa fonction de gardien de l'intérêt national.** Il s'agit d'un rôle essentiel lors de grandes crises dépassant ce qu'une organisation peut affronter seule. En effet, face aux situations de chaos le rôle de l'État consiste notamment à apprécier les priorités dans l'intérêt général, définir des stratégies collectives de réponse, donner du sens à l'action, engager des moyens nationaux et communiquer auprès de la population sur une large échelle.

Le dialogue entre les services de l'État et les organisations est animé dans les territoires sous l'autorité des préfets. Il est essentiel pour assurer une bonne préparation et gérer correctement un plan de continuité d'activité. Cette démarche doit être proactive, c'est-à-dire qu'une organisation ne doit pas attendre la crise pour identifier les services de l'État avec lesquels elle peut ou doit communiquer et collaborer. Les actions de préventions et protection, les mécanismes de remontée d'incidents et d'alerte, la coordination lors des interventions, la gestion des priorités, l'affectation des ressources, la communication et le fonctionnement au mieux en mode dégradé sont des domaines d'échanges nécessaires avec l'État. La connaissance préalable des correspondants et la compréhension de leurs missions sont par conséquent fondamentales.

Comme toute organisation, l'État est déjà fortement concerné par l'élaboration de PCA pour assurer la continuité des missions régaliennes. Il est également porteur d'une démarche de PCA sociétal. Gardien de la continuité des activités essentielles pour le fonctionnement de la Nation, il contribue à l'élaboration et à la mise en place des PCA des organisations publiques et privées, de plusieurs façons. Les dispositifs et domaines d'action, listés ci-après de manière non exhaustive, sont donnés pour exemple :

➡ **Analyse, prévention et gestion des risques :**
- Prescriptions légales et réglementaires pour certains secteurs (bancaire, santé…) ou certaines activités (transport collectif, activités dangereuses pour la population, activités d'importance vitale pour le fonctionnement de la Nation…).
- Coordination des programmes nationaux de R&D en technologies de sécurité.
- Sites d'information nationaux sur les risques (naturels, de nature terroriste, sécurité économique, sécurité informatique, etc.).
- Sites d'information de préfectures, avec le schéma directeur départemental d'analyse et de couverture des risques (ex : SDACR).
- Démarche nationale de résilience, plans de prévention, protection et intervention (cf. plans nationaux, cartographie des risques, etc.).
- Assistance des services de la direction centrale du renseignement intérieur, de la gendarmerie nationale ou de la direction de la protection et de la sécurité de la défense pour analyser les vulnérabilités et préconiser des mesures de protection (Voir fiche 13).

➡ **Veille et information :**
- Structures et dispositifs de veille des ministères.
- Sites ministériels d'information sur les risques et les crises, assistance aux voyageurs à l'étranger…
- Services de renseignement.

Page suivante

• Mécanismes d'alerte (dispositifs Vigipirate, suivi des crues…).
• Organismes exerçant des missions de services publics (Météo France, IRSN…).

➡ **Gestion de crise :**
• Architecture nationale de gestion de crise contribuant à la cohérence de l'action, du plus haut niveau de l'État jusque dans les territoires, en liaison avec les préfets aux niveaux zonal et départemental, avec les collectivités territoriales et les principaux opérateurs concernés.
• Élaboration des stratégies de réponse, déclenchement des plans d'intervention, mobilisation des parties prenantes, gestion des priorités, engagement de moyens nationaux.
• Communication avec le public (informer, communiquer les consignes comportementales…),.
• Relations avec les pays étrangers et l'Union européenne.

➡ **Contribution directe au fonctionnement des plans de continuité :**
• Appui méthodologique et diffusion de bonnes pratiques pour la continuité des activités et la résilience nationale.
• Coordination des acteurs locaux par les préfectures.
• Coordination des acteurs nationaux par la cellule interministérielle de crise.
• Décisions en matière d'arrêt ou de continuité d'activité[20].
• Actions de coordination, de mutualisation et de gestion des priorités.
• Gestion juridique des situations exceptionnelles, notamment le fonctionnement en mode dégradé.
• Réquisitions et apport de ressources exceptionnelles.

20 /Des différences d'appréciation rendent indispensable le dialogue entre l'État et les organismes concernés lorsqu'il s'agit d'interrompre certaines activités ou certains services afin de limiter un risque résiduel (parce que cela répond à un besoin local urgent ou parce que la reprise de l'activité interrompue est trop onéreuse pour les entreprises concernées).

# LE BILAN COÛT/AVANTAGES D'UN PCA. COMMENT ARBITRER ?

**OBJECTIF**

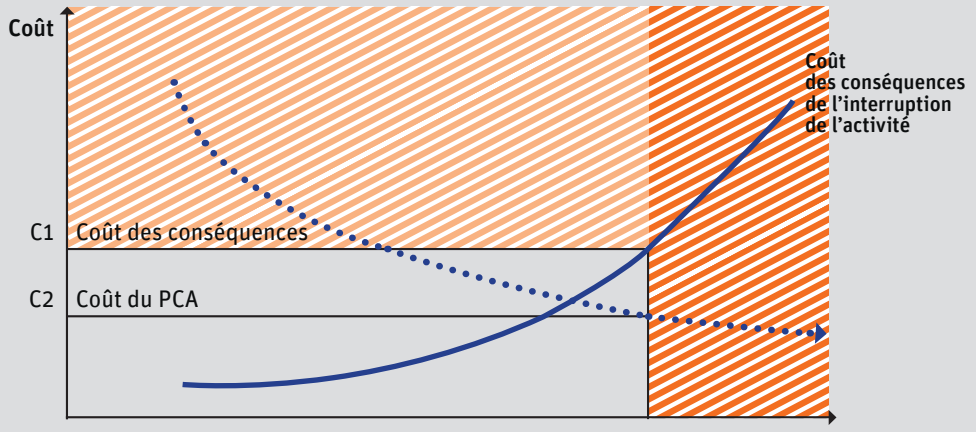
À partir des travaux réalisés précédemment il est possible de définir la bonne adéquation entre l'objectif de continuité (lié à l'attente de continuité prenant en compte l'analyse de risque et les scénarios retenus) et la réponse proposée, qui permet de garantir que l'objectif de continuité pourra être atteint en tenant compte du type de sinistre et de la ressource critique affectée.

➡ Plus l'indisponibilité est longue et plus le niveau de service demandé est élevé, plus le coût du dysfonctionnement pour l'organisation sera élevé (ce coût est à pondérer par l'appréciation de la probabilité d'occurrence).

➡ A contrario, plus l'objectif de reprise est loin et plus le niveau de service demandé est faible (notamment quand un mode dégradé est acceptable), plus le coût des solutions à mettre en œuvre sera faible.

**Le croisement de ces courbes, associé à l'appréciation du risque, permet de déterminer la stratégie de sécurité et de finaliser les objectifs de sécurité.**
Une telle démarche ne pose pas de problème quand les coûts des moyens pour mettre en place un PCA sont faibles ; car les solutions de continuité pourront être facilement validées. Par contre, si les dépenses sont importantes, l'investissement ne sera généralement accepté qu'en cas de menace imminente grave (mais

**BILAN COÛT/AVANTAGE DU MAINTIEN DE L'ACTIVITÉ**



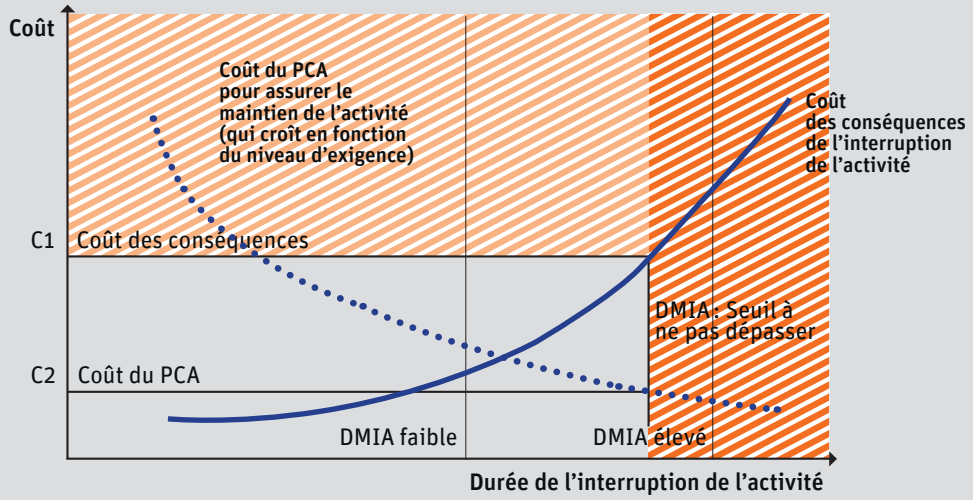

Ce schéma montre que les conséquences d'une interruption de l'activité ont un coût C1 qui correspond à la Durée Maximale d'Interruption Acceptable (DMIA).
Mais, pour ne pas dépasser ce seuil, il y a un coût du PCA, qui augmente si la DMIA diminue.
Dans le schéma ci-dessus le PCA a un coût C2, qui est inférieur au coût des conséquences éventuelles.
La comparaison entre les coûts C1 et C2 doit se faire en tenant compte de la probabilité de sinistre.

Page suivante

il sera souvent trop tard) ou si la demande est associée à une démarche de gestion du risque qui permet de valider les scénarios, de quantifier leur probabilité d'occurrence et d'optimiser les réponses possibles et la stratégie de continuité.
Le risque peut valoir d'être assumé sans PCA, si l'on prend des mesures de prévention et de protection pour le limiter. La probabilité de survenue d'un sinistre qui conduirait à une interruption d'activité diminue d'autant. Même dans le cas où le coût des conséquences éventuelles reste élevé, le risque peut valoir d'être assumé quand les avantages potentiels sont très importants en regard des coûts (découverte de nouveaux marchés, de nouveaux clients, fourniture de services attendus par les citoyens, etc.). Dans ce cas il sera plus difficile de justifier un PCA qui demande des investissements importants. Une démarche assurantielle peut alors être envisagée. En revanche, si l'occurrence du risque ne peut pas être maîtrisée (catastrophe naturelle, épidémie, etc.) et si les conséquences de l'interruption de l'activité sont importantes, il sera plus facile de justifier la mise en place d'un PCA, même si l'investissement demandé est élevé.

En fonction des objectifs (et obligations) de l'organisation et de l'appréciation des différents coûts il est possible de revoir à la baisse ou à la hausse les objectifs de continuité (par exemple en abaissant ou en augmentant la valeur de la durée de l'interruption d'activité maximale admissible). Cela a des conséquences directes sur le risque possible et sur le coût du PCA.

**FINALISATION DE LA STRATÉGIE DE CONTINUITÉ**




Ce schéma montre que les conséquences d'une interruption de l'activité ont un coût C1 qui correspond à la Durée Maximale d'Interruption Acceptable (DMIA).
Mais, pour ne pas dépasser ce seuil, il y a un coût du PCA, qui augmente si la DMIA diminue.
Dans le schéma ci-dessus le PCA a un coût C2, qui est inférieur au coût des conséquences éventuelles.
La comparaison entre les coûts C1 et C2 doit se faire en tenant compte de la probabilité de sinistre.

# DÉFINIR LA STRATÉGIE DE CONTINUITÉ D'ACTIVITÉ

**OBJECTIF**

La stratégie de continuité d'activité permet de formaliser les mécanismes de fonctionnement en modes dégradés et de reprise technique, d'identifier au préalable les priorités, de définir le niveau de service à restaurer et les délais associés. Elle permet également l'identification préalable de l'ordre de priorité de reprise et de basculement progressif sur les systèmes normaux.

➡ **À ce stade les quatre étapes précédentes du processus d'élaboration du PCA sont validées :**

- **Étape 1 :** connaissance du contexte, des objectifs et contraintes de l'organisation, des activités essentielles et processus clés.
- **Étape 2 :** connaissance des besoins de continuité des activités essentielles et processus associés, ainsi que des coûts de l'interruption d'activité.
- **Étape 3 :** identification des risques, probabilité d'occurrence et impacts, et des priorités de traitement ; établissement des scénarios à prendre en compte dans le PCA.
- **Étape 4 :** identification des mesures et valorisation des coûts du PCA et arbitrage entre coût du PCA et coût de l'interruption d'activité.

**L'optimum tel que décrit dans la fiche précédente permet, après validation par la direction, de fixer pour chaque activité essentielle et pour chaque processus/flux critique les objectifs de continuité et les actions à entreprendre en cas de sinistre pour assurer le maintien de ces objectifs.**

**Des objectifs sont également fixés pour le fonctionnement en mode dégradé s'il n'est pas possible de maintenir la continuité normale et quand la reprise d'activité se fait par étapes.**

**Recommandations :**

- Les objectifs de continuité doivent être cohérents avec la stratégie de l'organisation.
- Ils doivent tenir compte de la capacité à disposer des ressources nécessaires.
- Ils doivent être mesurables et surveillés.
- Pour leur élaboration il est recommandé de valoriser les pertes engendrées par les incidents craints.
- Il est recommandé de mener une analyse opposant le coût des mesures du PCA aux coûts des risques identifiés.

➡ **Élaboration de la stratégie :**

À partir des prérequis rappelés précédemment, la stratégie de continuité d'activité peut être déclinée. Elle va permettre de formaliser les mécanismes de fonctionnement en modes dégradés et de reprise technique, d'identifier au préalable les priorités, de définir le niveau de service à restaurer et les délais associés. Les mesures à mettre en œuvre et les procédures associées doivent rester simples. La stratégie de continuité va également permettre l'identification préalable de l'ordre de priorité de reprise et de basculement progressif sur les systèmes normaux (site informatique, bâtiment, etc.). Il est important de faire ce classement par priorité avant la survenue du sinistre, afin de prévoir, le moment venu, l'identification rapide des ressources qui seront nécessaires.

L'exemple illustré dans la fiche 15 concerne la reprise d'activité après un sinistre, avec une reprise en mode dégradé, par une solution de contournement puis un fonctionnement en mode secours, avec deux paliers successifs, avant retour à la normale.

# LA MISE EN ŒUVRE DES MOYENS NÉCESSAIRES AU PCA

**OBJECTIF**

Une fois le PCA validé, l'équipe projet doit rester impliquée pour piloter la mise en œuvre des moyens et procédures qui seront nécessaires en cas d'activation des dispositifs du plan.

Un cahier des charges doit être transmis à chaque **responsable de ressource critique** pour définir ce qui est attendu (disponibilité de certains composants, délais de mise en œuvre, prise en compte des aspects juridiques, etc.). Ces responsables devront transmettre en retour leurs réponses concernant les modalités de mise en œuvre (délais, besoins financiers, etc.) qui seront ensuite consolidés pour validation par la direction. Il faudra également identifier ce qui est attendu des **responsables de métiers et de processus** qui devront :

- Décliner les actions, outils et procédures du PCA.
- Intégrer des procédures du PCA dans leurs propres processus.
- Élaborer la documentation pour chaque procédure (conditions de déclenchement, ressources nécessaires, effets attendus, etc.).
- Réaliser des fiches réflexes pour la première heure.
- Assurer l'accès à la documentation.

➡ **Mise en œuvre des procédures du PCA :**

- Formaliser autant que possible un nombre réduit de procédures.
- Les fiches « actions » doivent être simples et spécifiques à chaque métier.
- Disposer de « fiches réflexe » par « métier ».

Les dispositifs du PCA sont constitués de procédures et de moyens spécifiques. Le plus grand risque est que ces dispositifs soient mal connus par les personnes en charge de leur mise en œuvre. Les modalités de formation, de vérification et de maintien en condition opérationnelle du PCA sont essentielles (elles font l'objet des fiches 25 et 26).

➡ **Comment disposer des moyens nécessaires à la mise en œuvre du PCA ?**

Il faut mettre en œuvre les mesures nécessaires à la tenue de l'objectif de perte de ressources maximale admissible (PRMA) ou perte de données maximale admissible (PDMA) et rendre possible l'activation du PCA. La liste très partielle qui suit est à ce titre indicative :

- Mise en place des dispositifs et procédures qui devront avoir été préalablement définis, formalisés et intégrés dans les processus métier pour être activités au déclenchement du plan.
- Mesures spécifiques pour les ressources humaines (ex : l'organisation du système d'astreintes).
- Mesures spécifiques aux infrastructures (ex : la préparation des sites de replis).
- Mesures spécifiques aux systèmes d'information (ex : la révision de l'architecture des systèmes d'information pour faciliter la synchronisation des données, la création de points stables pour les applications interdépendantes, le découpage en plaques secourables homogènes et bénéficiant de points de synchronisation communs ; ou encore la mise en place de procédures de sauvegarde des données, avec la fréquence correspondant aux objectifs (pertes de données maximum admissible : PDMA, avant la survenue du sinistre).
- Moyens de communication spécialisés pour faire face à l'absence des moyens publics, qui pourront être utilisés en mode dégradé. Ces moyens devront être connus et utilisés en période normale pour être facilement mis en œuvre en cas de déclenchement dans le cadre du PCA.
- Mesures spécifiques à la sécurité économique, avec notamment les dispositifs de récupération des données les plus sensibles.
- Mesures spécifiques en cas de défaillance de partenaire.
- Tests de fonctionnement de ces dispositifs avec la fréquence définie.

# PROCESSUS DE GESTION DE CRISE ET PCA

**OBJECTIF**

Si un sinistre devait survenir malgré les mesures de prévention, compte tenu de sa gravité et du contexte d'incertitude sur l'évolution de la crise, les mesures de protection, d'intervention et de limitation des effets devraient être pilotées par une cellule de gestion de crise.

➡ **La fonction de la cellule de crise,** qui est décrite dans le corps du guide, est de contribuer à maîtriser l'incertitude durant la crise. En effet, l'incertitude qui entoure les événements redoutés impose de développer une stratégie de réponse qui s'appuie sur l'anticipation de scénarios plausibles, permettant d'aboutir à des choix rationnels, évitant ainsi de réagir de manière affective à ce que l'on découvre.
La gestion de crise est intimement liée au PCA. Il est en effet rare qu'il y ait une décision d'activer des dispositifs prévus par le PCA sans qu'il y ait eu décision d'activer la cellule de crise. A contrario il peut y avoir une cellule de crise pour beaucoup d'autres incidents qui ne justifient pas de mettre en œuvre le PCA. C'est la raison pour laquelle le dispositif de gestion de crise est souvent décrit dans un plan spécifique, en dehors du PCA qui y fait seulement référence. Une autre option est que le processus de gestion de crise figure dans le tronc commun lorsqu'existent plusieurs PCA. D'un point de vue organisationnel, il est fréquent que le responsable du PCA (RPCA) se trouve être également le responsable de la gestion de crise.

➡ **Procédures génériques de gestion de crise spécifiques au PCA**
Les descriptifs suivants sont des exemples génériques de procédures et fiches concernant le PCA :

• **Procédure de remontée de l'alerte jusqu'à l'activation et suivi du PCA :**
- assurer un suivi des signaux précurseurs,
- identifier des incidents majeurs menaçant le bon fonctionnement d'activités essentielles,
- faire remonter l'information du correspondant local vers le responsable du PCA, en appliquant la procédure d'escalade,
- assurer le diagnostic et la qualification de l'événement,
- identifier les signes annonciateurs d'interruption d'activité pouvant donner lieu à l'activation du PCA,
- alerter le responsable de la gestion de crise ou le directeur de l'organisation,
- décider d'activer la cellule de crise,
- décider d'activer certaines parties du PCA,
- validation de dispositifs de continuité à mettre en œuvre,
- schéma délégataire, permettant la poursuite d'activité et les délégations de signature,
- mesures spécifiques à déclencher pour un fonctionnement en mode dégradé,
- assurer un pilotage par la cellule de crise opérationnelle,
- Suivi des indicateurs de continuité d'activité.

• **Fiches spécifiques :**
- remontée d'alerte,
- qualification : lieu/nature/heure/conséquences/actions prises,
- mobilisation de la cellule de crise : lieu, configuration, convocations,
- suivi par activité/sous-activité ; état de fonctionnement et de reprise,
- retour d'expérience, fiche qui doit être remplie dès le début de la crise, après avoir nommé un responsable pour ce suivi (voir en annexe 4 le modèle de fiche RETEX),
- suivi de la bonne prise en compte des recommandations issues du RETEX,
- déclarations aux assurances,
- Prise en compte des aspects juridiques.

Page suivante

**L'annuaire de crise**
Il s'agit naturellement d'un outil essentiel pour permettre d'alerter rapidement les personnes qui ont besoin de connaître la situation dans les délais utiles compte tenu de leurs rôles dans le dispositif de crise.

**Les moyens de communication**
Des moyens de communication doivent être prévus pour l'alerte, la remontée d'information, la communication des décisions et consignes, le dialogue avec les services de l'État et les autres organisations concernées par la gestion de la crise. Des moyens «en mode dégradé» doivent être prévus en cas d'indisponibilité des moyens habituels.

**La cellule de crise**
La cellule de crise, «chef d'orchestre» de l'ensemble, est indispensable pour répondre à des situations non maîtrisées. Elle comprend notamment les fonctions suivantes (qui peuvent être regroupées ou éclatées, en veillant dans ce dernier cas à une étroite coordination entre les cellules):

- **Fonctions à assurer dans la cellule de crise:**
  - suivi et analyse de la situation,
  - anticipation,
  - cellules techniques (ou processus) capables d'analyser les conséquences sur les métiers et activités,
  - cellule d'aide à la décision (capable de simuler différentes réponses possibles, à différents paliers de la crise, et de proposer la meilleure solution, dans un contexte d'incertitude),
  - cellule de décision,
  - cellule de coordination et suivi des actions,
  - cellule de relation avec les parties prenantes (dont l'État et les partenaires),
  - cellule de communication avec les média (voir fiche 24).

- **Les participants à la cellule de crise** comprennent à titre indicatif et sans préjudice d'ouverture à d'autres expertises:
  - l'autorité désignée par la direction de l'organisation,
  - le responsable de la gestion de crise (s'il n'est pas l'autorité désignée),
  - le responsable du PCA, le directeur des risques,
  - les responsables des métiers et des processus touchés par la crise,
  - les responsables des ressources affectées par la crise,
  - Les responsables de moyens nécessaires pour la gestion de crise.

**On ne peut qu'insister sur l'importance de la (ou des) cellule(s) d'analyse de l'information et d'anticipation pour donner du sens à l'information et donc au processus de décision.**

**La cellule de relation avec les parties prenantes** (dont l'État et les partenaires) est également essentielle pour développer une démarche transverse, dans un contexte où les grandes crises ont des répercussions en cascade, par le seul effet des interdépendances. Cela permet de mieux comprendre la situation, de partager la compréhension de la situation, de mieux analyser les impacts sur l'environnement économique, de faciliter la recherche de solutions. La réponse collective existe déjà dans certains secteurs d'activité (par exemple par la mutualisation de la gestion de crise dans la grande distribution). Cette démarche, étendue aux partenaires internes de l'organisation, permet également de donner du sens à l'action, chacun se sentant mobilisé dans la même finalité. **Le lien avec les services de l'État n'est pas repris ici car il fait l'objet de la fiche 18.**

**Le lien entre la gestion opérationnelle et la gestion stratégique de la crise doit être bien compris et renforcé, de façon à fluidifier les circuits d'information.**

Page suivante

**Les aspects humains** sont essentiels dans la gestion de la crise, de part les pressions considérables qui résultent de la nécessité de réagir rapidement à l'événement, du manque fréquent d'informations fiables et de la difficulté à anticiper.

**La compréhension des situations psychologiques des participants durant des périodes de stress doit permettre d'éviter des comportements pouvant conduire à de mauvaises décisions.**

**Exemples de comportements à risques en situation de crise[21] :**

- **Au début de la crise :**
  - minimisation de la gravité de certains événements,
  - absence de prise de conscience de la situation dégradée,
  - sentiment de pouvoir maîtriser la situation avec les moyens locaux.
- **Durant la crise :**
  - confiance aveugle (envers une personne ou un plan),
  - crainte de s'écarter du consensus, d'évoquer des positions différentes,
  - absence de communication avec l'extérieur, les médias,
  - absence de communication en interne, de calage des cellules,
  - incapacité à déléguer.
- **Au cœur de la crise, avec un fort stress :**
  - sur réaction face à la découverte de l'inadéquation des moyens,
  - état de choc, sidération, inhibition,
  - ou réaction en situation de panique, fuite en avant, surenchère,
  - absence d'écoute, de fonctionnement en réseau,
  - refus de se remettre en cause, de revoir la stratégie, obstination rigide,
  - ou, au contraire, changements trop fréquents, agitation stérile,
  - fatigue et actions automatiques, sans réflexion, etc.

**Pour éviter ces écueils il est nécessaire de professionnaliser les participants de la cellule de crise, au moyen de formations spécifiques et d'exercices.**

21 / Les exemples de PCA qui n'ont pas été mis en œuvre correctement dans une situation de stress pourtant prévue dans le PCA sont nombreux. 49% des sociétés affectées par les événements du 11 septembre 2001 à New-York ont déclenché leur PCA. Cependant, dans de nombreux cas, les bonnes décisions, n'ont pas été prises par la direction de ces sociétés. (www.Globalcontinuity.com).

# QUAND ET COMMENT DÉCLENCHER LE PCA ?

**OBJECTIF**

Connaître le bon moment et la manière de déclencher un PCA.

## 1. Déclenchement en phase d'alerte

Il est souhaitable de pouvoir détecter des signaux précurseurs ou annonciateurs d'un sinistre (catastrophe naturelle, accident majeur, menace terroriste, atteinte grave à l'image, etc.). Pour ce faire l'organisation doit idéalement disposer d'un service ou avoir recours à des prestations de veille, afin d'être capable d'analyser la situation, de pouvoir anticiper l'évolution des événements et déclencher à temps les procédures d'alerte interne.

Si les indicateurs et l'analyse confirment l'imminence d'un sinistre, les premières actions (en partie en mode réflexe) concernent les mesures de prévention/ protection/ intervention (qui ne sont pas traitées dans ce document).
La deuxième étape consiste à mettre l'organisation en mesure de faire face aux catastrophes possibles en activant ses mécanismes de résilience. Chaque organisation potentiellement affectée (directement ou indirectement) doit donc étudier l'opportunité de déclencher le PCA en phase d'alerte **pour un périmètre qui devra être défini et pour une durée qui devra être précisée :**

- Mobiliser les responsables du plan de continuité et de sa mise en œuvre.
- Vérifier le bon fonctionnement des dispositifs prévus en cas de déclenchement du plan de continuité.
- Vérifier la disponibilité des moyens de communication interne et des annuaires.
- Activer le dispositif d'astreintes.
- Assurer le travail de suivi, d'analyse et d'anticipation, avec montée en puissance de la cellule d'analyse.
- Effectuer l'enregistrement des informations critiques concernant l'incident, les actions entreprises et les premières décisions prises.
- **Informer si nécessaire les services d'urgence et/ou les services de l'État.**
- Identifier les moments clés de prise de décision pour :
  - déclencher la mise en place de la solution palliative,
  - déclencher la mise en place de la solution de secours,
  - identifier les points de non retour.

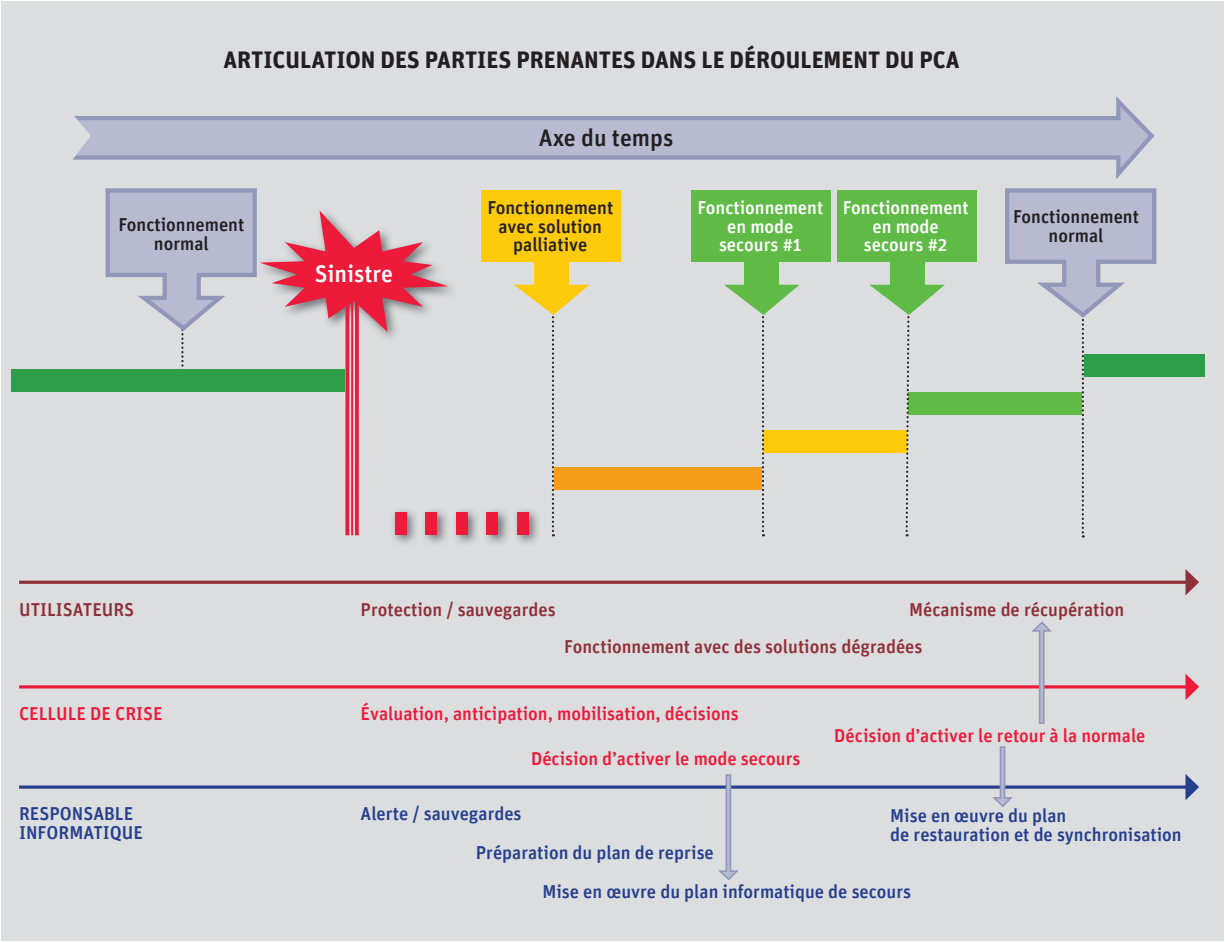
## 2. Déclenchement en phase d'activation

La décision de déclencher le PCA en phase d'activation peut être prise suite aux consignes de l'État lors d'une catastrophe naturelle touchant une zone donnée, ou à l'initiative **de chaque organisation**, en liaison avec son environnement direct (enjeux stratégiques, contrats existants, activités mutualisées touchées, etc.).
Cette phase d'activation est constituée d'une succession de décisions prises par paliers, en fonction de l'évolution de la situation et des mécanismes préalablement définis. Des dispositifs peuvent être activés successivement, par « crans » :

- Décision d'activer la cellule de crise décisionnelle.
- Décision d'activer telle solution palliative et/ou de secours.
- Modalités spécifiques en cas de basculement « à froid » ou « à chaud ».
- Activation de la cellule de crise opérationnelle pour gérer la mise en œuvre des solutions palliative et/ou de secours, etc.

Il est indispensable que chaque correspondant du PCA et que chacune des parties prenantes de sa mise en œuvre connaisse exactement quel est son rôle et l'action attendue, en fonction des consignes figurant dans le plan. Le schéma page suivante donne une idée des acteurs concernés, le responsable informatique étant mentionné ici à titre d'exemple de responsable de ressources critiques.

Page suivante




Ce tableau présente la chronologie de reprise progressive jusqu'à la reprise complète de l'activité.

**La décision d'activer la cellule de crise est une étape importante. Il vaut mieux la déclencher trop tôt que trop tard.**

**Décision de mettre en place une cellule de crise :**

- Il est recommandé que l'équipe projet PCA mette en place et maintienne à jour un annuaire de crise, accessible sous plusieurs formes et largement diffusé.
- Il est recommandé que le PCA décrive les moyens de communication, les sources d'informations et les besoins en locaux et postes de travail nécessaires pour permettre à la cellule de crise de fonctionner.
- Il est recommandé que le PCA comporte une phase d'escalade qui permette d'adapter les mesures déclenchées à la gravité identifiée de l'incident. À cette fin, le PCA doit déterminer, au préalable, les indicateurs et leurs valeurs seuils qui caractériseront la gravité de l'incident.
- Il est nécessaire que la cellule de crise comporte un personnel chargé de tenir à jour une main courante des actions décidées.

### 3. Reprise d'activité en mode secours

La reprise d'activité en mode secours impose de prendre la décision de basculer sur d'autres ressources, ce qui veut dire qu'il peut ne plus être possible de revenir à la situation antérieure. Ce choix doit être fait en connaissance de cause, sur la base de l'estimation de la durée de l'interruption de l'activité et du délai requis pour mettre en œuvre le mode secours.

Le PCA doit prévoir les priorités de rétablissement, car il n'est généralement pas possible de reprendre tous les processus arrêtés en mode secours, ainsi que les niveaux de service à assurer. Il en est de même pour les ressources

Page suivante

à préserver et protéger dès le début de la crise, pour permettre la reprise d'activité en mode secours.
Il est recommandé que le responsable de la reprise d'activité et ses correspondants soient mobilisés dès le début de la crise pour apprécier les modalités de mise en œuvre du ou des mode(s) secours.

Le mode secours n'a généralement pas vocation à s'éterniser. Il est donc nécessaire de prendre en compte la durée maximale admissible du mode secours pour anticiper les décisions appropriées.

### 4. Plan de retour en fonctionnement normal

Le retour en fonctionnement normal doit se préparer dès le début de la crise sous la conduite du responsable du PCA.

Certaines fonctions auront été préalablement définies et rédigées dans le PCA :
- Identification préalable de l'ordre de reprise.
- Gestion du dispositif d'intervention et de restauration en fonction des priorités de reprise.
- Dispositif de basculement progressif sur les systèmes normaux (site informatique, bâtiment, etc.).
- Durée maximale de fonctionnement sur le système de repli.

Il est recommandé de prévoir la possibilité d'un fonctionnement pérenne sur le site de repli, sans qu'il y ait de retour au mode normal antérieur.
Il est recommandé, dès le début de la crise, de vérifier que les ressources nécessaires pour la reprise en fonctionnement normal sont prévues et sont progressivement réunies.

*Note : La phase de retour en mode normal nécessite souvent une forte coordination entre des organisations différentes pour permettre la reprise la plus rapide possible de l'activité économique.*

# PCA ET COMMUNICATION DE CRISE

**OBJECTIF**

Compte tenu du besoin d'impliquer de nombreuses personnes, d'assurer la cohérence d'ensemble, l'usage d'une méthodologie commune et la bonne mise en œuvre des mesures retenues, la communication est essentielle au succès du PCA.

➡ **Les différents moments de la communication interne sont :**

• **Avant et durant l'élaboration du plan, avec les objectifs suivants :**
- sensibiliser les parties prenantes,
- montrer l'implication de la direction,
- expliquer la méthode et le rôle attendu des parties prenantes.

• **Une fois le plan validé, il s'agit alors d(e) :**
- expliquer la stratégie de continuité,
- s'assurer que les ressources nécessaires sont disponibles et que les exigences seront intégrées dans les processus métier,
- aider les responsables à s'investir dans la mise en œuvre du PCA,
- expliquer les modalités de vérification et promouvoir une démarche d'amélioration continue du PCA.

• **Lors du déclenchement du plan, la communication vise à :**
- mobiliser les parties prenantes,
- rappeler les actions à préparer puis à mettre en œuvre,
- transmettre les décisions et consignes,
- afficher les résultats obtenus.

➡ **Les différents destinataires de la communication en temps de crise sont :**

• D'abord le personnel (responsables des métiers et des processus, responsables des activités, tout le personnel, les sous-traitants présents).

• Puis les fournisseurs et clients de l'organisation, qui ont besoin de connaître des dispositifs du PCA et de sa mise en œuvre.

• Les autres partenaires concernés par la mise en œuvre du PCA.

• Les services de l'État et des collectivités territoriales.

• Le grand public.

**Recommandations**

• Il est recommandé que le PCA désigne le responsable chargé de diffuser les informations pendant la crise, ainsi que les éléments de langage types, adaptés aux différents scénarios craints.

• Ce responsable doit être connu de tous les interlocuteurs potentiels de l'organisation. Son autorité doit être assez élevée au sein de la hiérarchie de l'organisation pour que ses discours soient crédibles et ne pâtissent pas des délais inhérents aux processus de validation hiérarchique.

# LES INDICATEURS D'EFFICIENCE DU PCA

**OBJECTIF**

Il est recommandé de disposer d'indicateurs regroupés dans un tableau de bord qui donne une mesure globale de l'efficience du plan et de sa mise en œuvre. Cette liste d'indicateurs est utilement annexée au PCA.

➡ **Des indicateurs, permettant de mesurer l'avancement du projet, doivent être suivis par l'équipe projet.** Ils concernent les aspects techniques (architecture du système d'information, réseaux de communication sécurisés), les infrastructures (mise en place d'un site de repli), les ressources humaines (révision éventuelle de la convention collective, établissement de la liste des postes critiques), les relations avec les fournisseurs (formalisation des exigences, contrôles). Un bilan à date prédéfinie permettra de corriger des écarts éventuels.

➡ **Il faut par la suite disposer d'indicateurs de performance des procédures de mise en œuvre du PCA** et des mesures définies dans les différents plans métiers, par les responsables de ressources et notamment informatique. Il s'agit de mettre à la disposition des différents responsables chargés d'un rôle spécifique dans la mise en œuvre du PCA un instrument de mesure pour vérifier l'efficacité de leurs actions et les améliorer si nécessaire :

- Disponibilité des ressources spécifiques.
- Processus du PCA intégrés dans les processus normaux et référencés.
- Gestion de l'impact de ces processus spécifiques sur le fonctionnement de l'organisation.
- Présentation aux instances représentatives du personnel.
- Fiches réflexes par métier.
- Vérification que les procédures restent simples (par exemple, avoir la même procédure d'évacuation, quelle que soit la cause du sinistre).
- Besoin de soutien par une assistance à la conduite du changement.

➡ **Par ailleurs des indicateurs devront être définis pour mesurer l'efficacité du PCA.**
Il s'agit là de vérifier d'abord que la stratégie de continuité répond aux objectifs fixés, tels que :

- Maintenir la disponibilité des activités essentielles (tenir un niveau de DMIA spécifié pour chaque activité essentielle).
- Disposer d'indicateurs pour mesurer le niveau de l'activité normale et de l'activité en mode dégradé.
- Protéger le patrimoine applicatif et informationnel.
- Tenir la durée et le niveau de service assuré en mode dégradé, pour chaque activité essentielle, en cas de déclenchement du plan.
- Limiter la durée d'indisponibilité des activités essentielles de l'organisation et la quantité de données perdues en cas de déclenchement du plan, tant au moment de la bascule vers le site de secours qu'au retour vers le site principal.
- Assurer le traitement des besoins par ordre de priorité.
- Assurer le mode secours et le rétablissement selon les priorités établies.
- Ne pas dépasser le coût du PCA validé.
- Réduire la complexité des solutions du PCA.
- S'appuyer sur l'analyse de risque des activités et des processus de l'organisation.
- Revoir cette analyse de risque en cas de découverte de nouveaux risques importants.
- Améliorer la résilience en étendant progressivement les scénarios pris en compte.
- Disposer d'une organisation rôdée et bien entraînée à réagir aux événements, y compris aux problèmes imprévus, etc.

**Finalement des indicateurs peuvent permettre de suivre les valeurs d'évolution du PCA** comme le délai depuis les derniers exercices réalisés, depuis la dernière remise à jour de l'analyse de risque ou celle des différents éléments de la documentation du plan.

# LE MAINTIEN EN CONDITION OPÉRATIONNELLE DU PCA

**OBJECTIF**

Identifier les points clés des contrôles à effectuer pour s'assurer que le PCA est opérationnel et le reste dans la durée.

➡ **Le PCA doit bien faire apparaître :**
- La hiérarchisation des priorités.
- L'organisation et le processus pour la prise de décision.
- Les moyens mobilisables.
- Les processus spécifiques au PCA.
- Les dispositifs et les ressources qui doivent être connus et rester disponibles.
- Les contrôles.
- Le dispositif d'amélioration continue.

**Une fois le plan établi et validé, les ressources doivent être effectivement identifiées, les modifications indiquées doivent être effectuées, les procédures revues et intégrées dans les processus « métier », et les contrôles doivent être effectifs.**

➡ **Le plan doit être vivant et faire l'objet de contrôles réguliers :**
- Vérifications périodiques.
- Entretien des dispositifs de secours.
- Tests des procédures de bascule.
- Exercices et entraînement (simulés ou réels).
- Tenue à jour du plan.
- Mesure du niveau de maturité.
- Révision des procédures et dispositifs.
- Retour d'expérience et exploitation des RETEX.

**Rédaction de la documentation du PCA :**
- Il est recommandé de disposer d'un outil de gestion documentaire pour gérer et entretenir la documentation.
- Il est recommandé qu'une copie (papier et/ou numérique) de la documentation soit stockée sur un site distant de l'organisation, dans un lieu sécurisé et accessible en fonction des scénarios.

➡ **Les exercices :**
Les exercices sont un moyen pertinent pour valider l'efficience et l'efficacité du PCA. Chaque exercice doit être pensé et organisé en fonction de ce que l'on veut vérifier. Il peut s'agir par exemple de vérifier :
- La procédure d'alerte (par un exercice sur table).
- Le fonctionnement de la cellule de crise (par un exercice simulé, avec activation de la cellule de crise).
- Les procédures techniques de basculement en mode secours (par la mise en œuvre réelle et périodique).
- La coordination des différentes parties prenantes, lors d'un exercice de réponse à un incident grave simulé.

**Exercices de validation du PCA :**
- Il est recommandé de s'assurer que la formation des personnels aux procédures techniques a bien été ciblée et réalisée avant de déclencher les premiers exercices.
- Il est recommandé de tester les éléments critiques du plan au moins une fois par an.
- Il est recommandé de tester régulièrement la procédure de récupération des sauvegardes et de s'assurer de son efficacité et de ses performances par rapport aux besoins de l'organisation.

**Le contrôle documentaire et les rencontres avec les responsables de la mise en œuvre du PCA :**
**Il est possible de vérifier par un simple contrôle documentaire que les ressources, procédures et organisations prévues dans le PCA répondent bien sur le papier à ces objectifs.** Il s'agit

Page suivante

d'une tâche d'audit visant à vérifier que les ressources, procédures et organisations prévues dans le PCA sont effectivement en place, ou peuvent être mises en place dans les délais prévus. **Il convient également de vérifier que les plans, documentations, directives et consignes sont connus et accessibles facilement, en toutes circonstances, et propres à l'usage immédiat.**

Il faut enfin **apprécier la formation, la connaissance, la compétence et la compréhension du rôle que doit tenir chaque personne ayant une mission définie dans le cadre du PCA.**

**Cette vérification de capacité** peut être faite de manières différentes et parfois complémentaires :

- Audit interne périodique, et mise en place et exploitation des résultats des contrôles effectués.
- Surveillance régulière et revues de performance.
- Vérification de la conformité avec les normes (notamment ISO 22301) par auto-évaluation ou par un organisme de certification tiers et accrédité.
- Questionnaires d'auto-évaluation sur la connaissance et l'efficacité du PCA.
- *Benchmarking*, par comparaisons avec d'autres organisations.
- Tests réguliers des dispositifs techniques.
- RETEX systématiques suite à tout événement grave.
- Exercices, y compris avec les partenaires stratégiques.
- Vérification du fonctionnement du dispositif d'amélioration continue.

# ASPECTS JURIDIQUES ASSOCIÉS
## À LA MISE EN ŒUVRE D'UN PCA

**OBJECTIF**

Prendre conscience qu'il est nécessaire de vérifier la conformité du PCA et des mesures proposées avec les lois et règlements (code du travail, code du commerce, code de la défense, code civil, code pénal, etc.).

La continuité d'activité doit nécessairement être appréhendée à travers le prisme de la responsabilité juridique de l'entreprise. Le plan de continuité d'activité à vocation à jouer, dans une situation de fait exceptionnelle, sans pour autant que le droit ne s'inscrive dans cette logique d'exception conformément à la maxime : « à situation exceptionnelle, responsabilité ordinaire ».

En fait, il s'agit d'appréhender la responsabilité de l'organisation qui met en œuvre le plan de continuité, de sa défaillance, voir de son absence. Cela suppose de connaître l'origine et la force obligatoire des textes applicables à l'entreprise en matière de continuité d'activité. La responsabilité juridique est entendue de façon extensive et l'intégralité des aspects de la responsabilité, tant au plan pénal, que civil (responsabilité contractuelle et délictuelle), doit être examinée.

**Quelques points d'attention :**

- Le chef d'entreprise peut être tenu pénalement responsable d'une faute d'imprudence, d'une négligence, d'un manquement à une obligation de prudence ou de la mise en danger délibérée de la personne d'autrui [22].

- Le respect des règles qui relèvent de la responsabilité sociale et environnementale doit être recherché (notamment pour ce qui concerne la prévention des risques professionnels[23] et environnementaux).

- Le code du commerce dispose qu'un rapport descriptif des principaux risques doit être présenté aux assemblées générales de sociétés anonymes[24].

- Le respect des textes est facilité quand il s'agit de mesures de sécurité, car elles font l'objet de prescriptions spécifiques (textes normatifs). Cela est plus complexe pour les règles de sûreté (protection contre les actes de malveillance ou de terrorisme) pour lesquels il n'y a pas de norme, mais seulement des principes généraux (sauf dans des cas très spécifiques) décrits, par exemple, dans les obligations imposées aux « opérateurs d'importance vitale ».

**Le transfert à une autre entreprise de certaines missions n'exonère pas pour autant automatiquement l'entreprise délégataire de sa responsabilité, notamment quand elle conserve la maîtrise d'œuvre du dispositif concerné.**

22 / Article 121-3 du code pénal.
23 / Articles L. 4121-1 à L. 4121-5 du code du travail.
24 / Article L. 225-100 du code de commerce.

# LEXIQUE

Il est conseillé de consulter le Lexique structuré de la continuité d'activité, rédigé par le Club de la Continuité d'Activité, qui propose une liste de définitions très complète.

Nous proposons ici de courts extraits de terminologie normalisée.

| | Définitions | Références |
|---|---|---|
| **GESTION DE LA CONTINUITÉ D'ACTIVITÉ** | | |
| **Gestion de la continuité d'activité** | Processus de management holistique qui identifie les menaces potentielles pour une organisation ainsi que les impacts que ces menaces, si elles se concrétisent, peuvent avoir sur les opérations liées à l'activité de l'organisation, et qui fournit un cadre pour construire la résilience de l'organisation avec une capacité de réponse efficace préservant les intérêts de ses principales parties prenantes, sa réputation, sa marque et ses activités productrices de valeurs. | ISO 22301 : 2012(F) |
| **Continuité d'activité** | Capacité de l'organisation à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur. | ISO 22301 : 2012(F) |
| **Plan de continuité d'activité** | Procédures documentées servant de guide aux organisations pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation. | ISO 22301 : 2012(F) |
| **Objectif minimal de continuité d'activité** | Niveau minimal de services et/ou de produits acceptables par l'organisation pour atteindre ses objectifs métiers pendant une perturbation. | ISO 22301 : 2012(F) |
| **Durée maximale d'interruption acceptable DMIA** | Temps nécessaire pour que les impacts défavorables pouvant résulter de la non fourniture d'un produit/service ou de la non réalisation d'une activité, deviennent inacceptables. | ISO 22301 : 2012(F) |
| **Perte de données maximale admissible PDMA** | La perte maximale de données (liée aux sauvegardes) pour que celle-ci soit d'un niveau acceptable par les services utilisateurs. Par exemple, au démarrage après un sinistre, les données peuvent dater de la veille au soir, du matin, ou du moment du sinistre, selon la procédure de réplication/sauvegarde utilisée. | CCA/AFNOR |
| **GESTION DES RISQUES** | | |
| **Risque** | Effet de l'incertitude sur l'atteinte des objectifs<br>(Un effet est un écart, positif et/ou négatif, par rapport à une attente).<br>Cette définition a été revue lors du développement de la norme ISO 31000 : 2009 ; elle abandonne la vision de l'ingénieur (« *le risque est la combinaison de probabilité d'événement et de sa conséquence* ») pour coupler les risques aux objectifs de l'organisation : « *le risque est l'effet de l'incertitude sur les objectifs* ». | ISO 73 |
| **Appréciation du risque** | Ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque. | ISO 73 |
| **Management du risque** | Activités coordonnées dans le but de diriger et piloter une organisation vis-à-vis du risque. | ISO 73 |
| **Source de risque** | Tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un risque. | ISO 73 |
| **Vulnérabilité** | Propriétés intrinsèques de quelque chose entraînant une sensibilité à une source de risque pouvant induire une conséquence. | ISO 73 |
| **Conséquences** | Effet d'un événement affectant les objectifs. | ISO 73 |
| **Résilience** | Capacité d'adaptation d'un organisme dans un environnement complexe et changeant. | ISO 73 |
| **Attitude face au risque** | Approche d'un organisme pour apprécier un risque avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque. | ISO 73 |
| **Goût du risque** | Importance et type d'opportunité qu'un organisme est prêt à saisir ou à préserver ou de risque qu'il est prêt à prendre. | ISO 73 |
| **Propriétaire du risque** | Personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer. | ISO 73 |

# RÉFÉRENCES

Ce guide a vocation à poser les principes et les règles d'élaboration d'un PCA, sans se substituer aux différents guides ou normes existant sur le sujet, mais en y faisant référence. Son objectif, par une approche volontairement globale, est d'apporter les éléments de bonne pratique et de cohérence nécessaires au dialogue entre les responsables des travaux d'élaboration de PCA de différentes organisations, publiques ou privées. Il s'adresse donc aux administrations, aux collectivités et aux entreprises.

**➡ Exemples de pertes de continuité d'activité :**

- Infonetics Research, avril 2007, white paper *"Reducing Downtime Costs with Network-Based IPS"*.
- *Hazards and vulnerability in modern societies – using the example of a large-scale outage in the electricity supply - TAB report no. 141. Berlin 2010, 264 pages.* http://www.tab-beim-bundestag.de/en/publications/reports/ab141.html
- Fukushima(rapport IRSN/DG/2012-001).

**➡ Enquêtes :**

- Tendances mondiales en matière de résilience et de gestion du risque métier (Enseignements de l'étude IBM Global Business Resilience and Risk Study 2011).
- Report on the Accenture 2011 Global Risk Management Study.
- Étude 2011 du CRED (*Centre for Research on the Epidemiology of Disasters*).

**➡ PCA dans le secteur bancaire et financier :**

- Principes directeurs en matière de continuité d'activité, le forum tripartité, comité de Bâle sur le contrôle bancaire, août 2006.
- Règlement n° 97-02 du 21 février 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement portant sur la réglementation prudentielle des établissements de paiement.
- Règlement n° 93-05 du 21 décembre 1993 relatif au contrôle des grands risques.
- Les dispositifs de gestion des risques et de contrôle interne (Autorité des marchés financiers).
- La directive MIF (*Markets in Financial Instruments Directive*), publiée au *Journal officiel de l'Union européenne* le 30 avril 2004.
- *Solvency II* pour le secteur des assurances.

**➡ Gestion du risque pour les sociétés cotées :**

- Le COSO est un référentiel de contrôle interne défini par le *Committee Of Sponsoring Organizations of the Treadway Commission*. Il est utilisé notamment dans le cadre de la mise en place des dispositions relevant des lois Loi Sarbanes-Oxley, SOX ou Loi de sécurité financière, LSF, pour les entreprises assujetties respectivement aux lois américaines ou françaises. Le référentiel initial appelé COSO1 a évolué depuis 2002 vers un second corpus dénommé COSO 2.
- La directive européenne 2006/46/CE.
- La loi du 3 juillet 2008 a transposé cette directive dans le droit français et complété, par la même, la Loi de Sécurité Financière (LSF) du 1er août 2003. Il en est résulté une modification des articles L. 225-37 et L. 225-68 de code du commerce qui a étendu l'objet du rapport du président sur les procédures de contrôle interne aux procédures de gestion des risques mises en place par les sociétés faisant appel public à l'épargne.

**➡ Méthodologies :**

- Club de continuité d'activité : Lexique structuré de la continuité d'activité, livre blanc n°1, version 2.0.
- Club de continuité d'activité : Guide de bonnes pratiques de la continuité d'activité à l'attention des Directions des Ressources Humaines.
- Club de continuité d'activité : Plan de Continuité d'Activité & Gestion de Crise – Fascicule pratique de la mise en place du travail occasionnel à distance (TOAD).
- Ministère de la Défense : Guide DGSIC n°004 portant sur la rédaction des plans de continuité d'activité (PCA) et plan de reprise d'activité (PRA) 23/07/2010.

Page suivante

- Ministère de la Défense : Guide DGSIC n°005 dispositions pratiques et techniques de continuité informatique, 10/12/2010.
- Modèle CMMI® qui permet de classer en cinq niveaux de maturité les pratiques de l'entreprise ; pour atteindre chaque étage, l'entreprise doit mener des actions d'amélioration au niveau des processus clés.
- Méthodes d'analyse de défaillance et de leurs effets (AMDEC, HACCP, 6 sigma, etc.).
- La cartographie : un outil de gestion des risques (AMRAE).
- La gestion des risques : Olivier Hassid (DUNOD, 2008).
- Retour d'expérience et maîtrise des risques : Jean-Luc Wybo et Wim Wassenhove (collection sciences du risque et du danger, édition Lavoisier).
- La méthode de gestion des risques EBIOS www.ssi.gouv.fr/.
- Le guide de l'intelligence économique, délégation interministérielle à l'intelligence économique (Hachette 2012), qui donne des solutions de bonnes pratiques et un guide d'autodiagnostic.

**➡ Normalisation :**

- Projet de guide ISO 73 Management du risque — Vocabulaire.
- ISO/22301 Sécurité sociétale — Gestion de la continuité des affaires — Exigences.
- ISO/FDIS 31000 Management du risque — Principes et lignes directrices.
- ISO/IEC 27002 Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information.
- ISO 26000 – responsabilité sociétale des organisations.
- AFNOR Référentiel de bonnes pratiques, Plan de continuité d'activité (PCA), BP Z74-700, 11 avril 2011.
- IRGC risk management framework.

**➡ Obligations et guides de bonnes pratiques :**

- Portail du Gouvernement pour la prévention des risques majeurs www.risques.gouv.fr www.prim.net
- Délégation interministérielle à l'Intelligence économique (D2IE) www.intelligence-economique.gouv.fr
- Agence nationale pour la sécurité des systèmes d'information www.ssi.gouv.fr/ http://www.securite-informatique.gouv.fr/
- Le Haut Comité Français de la Défense Civile (HCFDC) https://www.hcfdc.org/asso/
- Le Club de la continuité d'activité http://www.clubpca.eu/
- La valorisation des actifs immatériel présentée par l'Observatoire de l'immatériel http://www.observatoire-immateriel.com/
- Site d'information http://www.info-crises.fr/
- Plans de protection des risques (naturels, techniques, environnementaux).
- Le document unique d'évaluation des risques DUER, créé par le décret n° 2001-1016 du 5 novembre 2001, qui a transposé la directive européenne sur la prévention des risques professionnels.
- Circulaire DGT 2007/18 du 18 décembre 2007 relative à la continuité de l'activité des entreprises et aux conditions de travail et d'emploi des salariés du secteur privé en cas de pandémie grippale.
- Circulaire DGAFP du 26 août 2009 visant à assurer la continuité du service public dans les administrations de l'État et des collectivités locales en cas de pandémie grippale.
- Code du travail article L. 4121-1 « L'employeur prend les mesures nécessaires pour assurer la sécurité et protéger la santé physique et mentale des travailleurs. Ces mesures comprennent : 1° Des actions de prévention des risques professionnels et de la pénibilité au travail ; 2° Des actions d'information et de formation ; 3° La mise en place d'une organisation et de moyens adaptés. L'employeur veille à l'adaptation de ces mesures pour tenir compte du changement des circonstances et tendre à l'amélioration des situations existantes ».
- Code du travail article R. 4121-1 « L'employeur transcrit et met à jour dans un document unique les résultats de l'évaluation des risques pour la santé et la sécurité des travailleurs à laquelle il procède en application de l'article L. 4121-3.Cette évaluation comporte un inventaire des risques identifiés dans chaque unité de travail de l'entreprise ou de l'établissement (...) » et art. R.4741-1. « Le fait de ne pas transcrire ou de ne pas mettre à jour les résultats de l'évaluation

Page suivante

des risques, dans les conditions prévues aux articles R. 4121-1 et R 4121-2, est puni de l'amende prévue pour les contraventions de 5e classe ».

- Code du travail article L. 1222-11 « En cas de circonstances exceptionnelles, notamment de menace d'épidémie, ou en cas de force majeure, la mise en œuvre du télétravail peut être considérée comme un aménagement du poste de travail rendu nécessaire pour permettre la continuité de l'activité de l'entreprise et garantir la protection des salariés. Les conditions et les modalités d'application du présent article sont définies par décret en Conseil d'État ».
- Le dispositif de sécurité des activités d'importance vitale selon le code de la défense (notamment ses articles R. 1332-1 à R. 1332-42, pris sur le fondement de ses articles L. 1332-1 à L. 1332-7), constitue le cadre permettant d'associer les opérateurs, publics ou privés, au système national de protection contre le terrorisme, d'analyser les risques et d'appliquer les mesures de leur niveau en cohérence avec les décisions des pouvoirs publics.
- Sécurité des transports (OEA, C-TPAT, Megaport, CSI, ISPS, ADR…).
- Exigences spécifiques à l'activité (SEVESO, TMD, REACH, RoHS…).
- Article L. 225-100 du code de commerce « Le rapport [présenté en assemblée générale des sociétés anonymes] comporte également une description des principaux risques et incertitudes auxquels la société est confrontée ».
- Code civil, notamment l'article 1382 « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer ».
- Code pénal, code de commerce, etc.

# FICHE GUIDE SYNTHÉTIQUE
## POUR L'AUTO-ÉVALUATION DES BONNES PRATIQUES

| ETAPES ET ACTIONS | OUI | NON | OBSERVATIONS |
|---|---|---|---|
| **1. Définition du contexte, identification des objectifs et des activités essentielles.** | | | |
| 1.1. La direction est-elle fortement impliquée ? | | | |
| 1.2. Un chef de projet doté des compétences, de l'autorité et de l'autonomie nécessaires a-t-il été nommé ? | | | |
| 1.3. Le contexte et le périmètre de PCA ont-ils été précisés ? | | | |
| 1.4. Les objectifs, les activités essentielles, les flux et les ressources critiques ont-ils été identifiés ? | | | |
| 1.5. Les processus de l'organisation ont-ils été cartographiés ? | | | |
| 1.6. Les flux entre les systèmes d'information supportant les processus ont-ils été cartographiés ? | | | |
| **2. Déterminer les attentes de sécurité pour tenir les objectifs.** | | | |
| 2.1. Les systèmes de téléphonie, serveurs de fichiers et messagerie ont-ils été intégrés dans les systèmes critiques de l'organisation ? | | | |
| 2.2. Les ressources critiques « dures » ont-elles été prises en compte ? | | | |
| 2.3. Les ressources immatérielles ont-elles été prises en compte ? | | | |
| 2.4. Les niveaux de fonctionnement en mode dégradé sont-ils explicités ? Ont-ils été validés en liaison avec le(s) « client(s) » ? | | | |
| 2.5. Les niveaux dégradés de prestations des fournisseurs ont-ils été pris en compte ? | | | |
| 2.6. L'échelle de mesure des conséquences d'interruption validée avec les responsables est-elle identique pour tous les processus ? | | | |
| **3. Identifier, analyser, évaluer et traiter les risques.** | | | |
| 3.1. Si une analyse de risques préexistait, a-t-elle été reprise pour en vérifier la pertinence ? | | | |
| 3.2. L'analyse des risques a-t-elle permis d'identifier ceux contre lesquels il est prioritaire de se protéger ? | | | |
| 3.3. Le PCA global repend-t-il en autant de composantes les scénarios de risques retenus ? | | | |
| 3.4. Le PCA prend-t-il en compte les risques opérationnels pour lesquels l'interruption d'activité résulte de la perte de ressources critiques ? | | | |
| 3.5. Les partenaires des secteurs publics et privés susceptibles d'être concernés par les scénarios ont-ils été identifiés ? | | | |
| 3.6. Les interdépendances et les effets en cascade ont-ils été pris en compte ? | | | |
| **4. Définir la stratégie de continuité d'activité.** | | | |
| 4.1. Les objectifs de continuité sont-ils cohérents avec ceux de l'organisation, mesurables, et tiennent-ils compte des ressources nécessaires ? | | | |
| 4.2. Les objectifs de continuité en mode dégradé et pour la reprise d'activité sont-ils cohérents avec les scénarios de risques retenus ? | | | |
| 4.3. L'ordre de priorité des procédures, des ressources, de la reprise et du basculement progressif sur les systèmes normaux est-il identifié ? | | | |
| 4.4. Les exigences vis-à-vis des « partenaires » ont-elles été prises en compte de manière réciproque ? | | | |
| 4.5. Les services de l'État et les organisations partenaires du PCA sont-ils identifiés et connus ? | | | |
| 4.6. La stratégie a-t-elle été validée par la direction ? | | | |

Page suivante

| 5. Mettre en œuvre et assurer l'appropriation du plan | | | |
|---|---|---|---|
| 5.1. Les actions de communication inhérentes au lancement, à l'appropriation et à la mise en œuvre du PCA ont-elles été prévues ? | | | |
| 5.2. Les mesures à mettre en œuvre et les procédures associées sont-elles simples et accessibles ? | | | |
| 5.3. Les dispositifs, moyens et ressources nécessaires à la mise en œuvre du PCA sont-ils disponibles et/ou en place ? | | | |
| 5.4. Les personnels responsables sont-ils désignés, informés et formés aux procédures prévues dans le PCA ? | | | |
| 5.5. Les indicateurs, les dispositifs itératifs de vérification, contrôles, exercices et évolution du plan sont-ils conçus et déclinés ? | | | |
| 5.6. Les procédures de sauvegarde/récupération et les moyens critiques du PCA seront-ils contrôlés périodiquement ? | | | |

# FICHE MODÈLE D'ANALYSE ET D'ÉVALUATION DES RISQUES POUR UNE SITUATION DONNÉE

## 1. Évaluation du risque (naturel, accidentel, terroriste…) ou de la situation retenue

| Catégorie | Sous catégorie |
|---|---|
| Température extrême (TE) | Grand froid |
| **Périmètre pris en compte** *(La caractérisation d'un risque peut nécessiter de définir son périmètre d'application. Par exemple une inondation peut concerner une faible étendue ou une vaste étendue.)* | **Référence du risque** *(La référence sera définie dans le document de synthèse)* |
| Local et national | TE 1 |
| **Date de rédaction** | **Date de révision** |
| Janvier 2013 | Janvier 2015 |

**Description générale du risque** (fournir les données générales de description du risque)
- La plupart des causes….
- Les phénomènes…
- Danger à cinétique lente, rapide, à impact local, régional…

**Évolution historique** (fournir les données historiques pour apprécier la probabilité d'occurrence et souligner une éventuelle évolution)
20XX
- ----------
19XX
- ----------

**Prospective 2015** (tendances et perspectives : fournir les tendances lourdes concernant l'évolution du risque ou de la situation retenue. Par exemple pour les températures extrêmes, on s'attend non pas à une augmentation sensible de leur nombre mais plutôt à une intensification du phénomène liée aux conséquences du changement climatique)

**Tendances et évolution pour le danger ou la crise**

**Scénarios de dégradation naturelle des phénomènes** (Identifier des scénarios possibles en fonction de l'évolution probable du risque ou de la situation)

## 2. Probabilité ou vraisemblance de la situation retenue

| Situation | Périmètre pris en compte | Probabilité |
|---|---|---|
| Température extrême (TE) | Nationale | 1 |
| Température extrême (TE) | Locale | 5 |

Page suivante

## 3. Impact (synthèse de l'analyse)

| Situation | Périmètre pris en compte | Impact |
|---|---|---|
| Température extrême (TE) | National | 1 |
| Température extrême (TE) | Local | 2 |

### Détail des impacts

| | Niveau moyen de l'impact | Types d'impact | Sous critères | Valeur de l'impact par sous critères et commentaires éventuels |
|---|---|---|---|---|
| Mineur | 2 | Humain | 1.1 Nombre de morts<br>1.2 Nombre de blessés | 1<br>2 |
| | | Social | 2.1 Nombre de personnes<br>2.2 Effet psychologique | 2<br>2 |
| | | Financier | 3.1 Coût global | 2 |
| | | Contractuel | 4.1 Incidences sur les engagements | 2 |
| | | Opérationnel | 5.1 Effets directs<br>5.2 Déficience des sous-traitants | 3<br>3 |
| | | Environnement | 6.1 Impact environnemental | 1 |
| | | Image | 7.1 Impact sur la réputation | 1 |
| | | Juridique | 8.1 Responsabilité civile ou pénale<br>8.2 Obligations réglementaires | 1<br>1 |

### Vulnérabilité et résilience

- Éléments d'appréciation sur la vulnérabilité et la résilience du secteur et des personnes concernées

## 4. Évaluation globale

| Situation retenue | Sous catégorie | | |
|---|---|---|---|
| Température extrême | Grand froid | | |
| **Périmètre** | **Impact** | **Probabilité ou vraisemblance** | **Cotation du risque** |
| Nationale | 1 | 1 | 1 |
| Locale | 2 | 5 | 7 |
| **Dispositif de planification**<br>• ..... | | | |
| **Gestion de crise (préciser les capacités existantes ou à acquérir)**<br>• ..... | | | |

# FICHE MODÈLE DE RETEX

Pour chacune des étapes suivantes, décrire les faits, les problèmes rencontrés, les solutions utilisées pour les résoudre :

**➡ Caractéristique de l'événement :**
- Caractéristique de l'incident initial.
- Facteurs aggravants.
- Cinétique.
- Périmètre.
- Activités affectées et caractéristiques (dysfonctionnement ou arrêt, durée).
- Phénomènes en cascade.

**➡ Alertes :**
- Détection de signes précurseurs.
- Analyse.
- Alerte.
- Mobilisation.
- Décision d'activation de la cellule de crise (délais).

**➡ Gestion de crise :**
- Délais de mise en œuvre.
- Fonctionnement.
- Acteurs.
- Connaissance de la situation.
- Anticipation.
- Décisions.
- Coordination.
- Communication.

**➡ Planification de la mise en œuvre du PCA :**
- Activités affectées.
- Processus affectés et ressources perdues.
- Existence de plan disponible et adapté à la situation.
- Bonne mise à jour du plan.
- Connaissance du plan.
- Clarté et facilité de mise en œuvre du plan.
- Fonctionnement du dispositif d'appui, de l'expertise métier et processus.

**➡ Mise en œuvre du PCA :**
- Bonne évaluation de la situation et de son évolution.
- Décisions connues.
- Pertinence des décisions.
- Mise en œuvre des procédures.
- Disponibilité des ressources pour mettre en œuvre le PCA.
- Respect des délais (DMIA pour les différents modes dégradés et les différentes activités essentielles affectées).
- Efficacité du PCA.

**➡ Implication des parties prenantes :**
- Consultation des parties prenantes internes.
- Dialogue avec les services de l'État.
- Consultation des fournisseurs, des clients.

**➡ Respect des obligations :**
- Aspects juridiques.
- Réglementation.

**➡ Communication associée au PCA :**
- Communication interne.
- Communication avec les partenaires.
- Communication avec le public.
- Pertinence des messages.
- Réaction des médias.

**➡ Circulation de l'information :**
- Information suffisante.
- Information utile.
- Bonne remontée de l'information terrain.
- Problèmes techniques (moyens de transmission).
- Traçabilité de l'information.
- Bonne communication entre les différentes entités.
- Constatation d'incohérences dans les informations.
- Connaissance du niveau de fonctionnement des activités essentielles.
- Connaissance du niveau de perte des ressources critiques.
- Connaissance de l'impact sur les partenaires externes.

**➡ Gestion du PCA :**
- Maîtrise de la situation.
- Utilisation des indicateurs pertinents.
- Clarté des rôles des différents acteurs.
- Contribution des correspondants du PCA.

Page suivante

- Rôle du responsable du PCA.
- Bonne coopération des différents services.
- Bonne gestion de la cinétique.
- Régularité des points de situation en cohérence avec la cinétique des événements.
- Bonne utilisation des outils (points de non retour, point de décision...).
- Traçabilité des décisions.
- Difficultés de langage (vocabulaire technique).

➡ **Fonctionnement du PCA :**
- Activation conforme aux décisions.
- Efficacité des procédures.
- Bon fonctionnement des modes palliatifs et de secours.
- Actions rapides et dans les temps impartis des différents acteurs.
- Difficultés techniques rencontrées.
- Niveaux de services.

➡ **Gestion des ressources :**
- Conditions de travail.
- Disponibilité des ressources pour mettre en œuvre le PCA.
- Bon suivi de l'engagement des ressources.
- Bonne utilisation des ressources nécessaires pour le PCA.
- Fonctionnement des moyens externes.
- Relations avec les fournisseurs et sous-traitants.

➡ **Gestion du retour à la normale :**
- Anticipation.
- Décisions au bon moment.
- Disponibilité des ressources nécessaires.
- Reprise des données.
- Respect des délais.
- Coopérations avec les clients et fournisseurs.
- Bonne gestion des aides financières et des assureurs.

➡ **Conclusions :**
- Points positifs.
- Points négatifs.
- Problèmes rencontrés.
- Axes d'amélioration concernant :
  - Le PCA.
  - La formation.
  - La préparation.
  - Les relations avec les parties prenantes externes.

# NOTES

SGDSN
SECRÉTARIAT GÉNÉRAL
DE LA DÉFENSE ET DE
LA SÉCURITÉ NATIONALE

51, boulevard de la Tour-Maubourg
75700 Paris 07 SP
Courriel : courrier.sgdsn@sgdsn.gouv.fr