ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE
DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES D'INFORMATION

GUIDE RELATIF A L'ELABORATION D'UN PLAN DE CONTINUITE ET DE REPRISE D'ACTIVITES

SOMMAIRE

I. INTRODUCTION

1. Contexte

En application des dispositions de l'article 8 du décret n° 2-15-712 du 12 Joumada II 1437 (22 mars 2016) fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale, les organismes concernés sont tenus de concevoir et de 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.

2. Définition du Plan de Continuité d'Activité (PCA)

La gestion de la continuité d'activité est définie 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 ».

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.

3. Objet du document

Le présent guide apporte une démarche méthodologique permettant l'élaboration d'un plan de continuité d'activités, ainsi que des conseils et des bonnes pratiques qui vont servir pour retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation importante. Il s'adresse à la direction générale ou au secrétariat général, aux responsables et aux personnels concernés par la gestion de la continuité et reprise d'activités.

Ce guide décrit de manière détaillée cinq grandes phases de la démarche de gestion de la continuité et reprise des activités :

1. Définir le périmètre, identifier les objectifs et les activités essentielles ;
2. Déterminer les attentes de sécurité pour tenir les objectifs ;
3. Identifier, analyser, évaluer et traiter les risques ;
4. Définir la stratégie de continuité d'activités ;
5. Mettre en œuvre et assurer l'appropriation.

II. DEMARCHE DE GESTION DE LA CONTINUITE ET REPRISE DES ACTIVITES

1. Définir le périmètre, identifier les activités essentielles et les objectifs

Cette étape vise à préciser le périmètre géographique et fonctionnel de l'organisme qui doit être pris en compte pour la mise en place du PCA. De la définition du périmètre découlera l'identification des actifs et des activités qui sont essentielles pour l'atteinte des objectifs de l'organisme. Cette étape représente une première analyse des ressources, dites « critiques », nécessaire au bon fonctionnement de l'organisme.

1.1. Définition du périmètre

La définition du périmètre doit d'abord résulter d'une analyse des champs géographique et organisationnel pris en compte. Certaines parties de l'organisme 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). Il en résulte généralement l'établissement de plusieurs PCA distincts sous la responsabilité des dirigeants des organismes respectifs.

Cette démarche permet la description des activités essentielles ainsi que des processus et ressources qui sont critiques pour ces activités. Il en résulte d'apprécier le niveau de risque acceptable par l'organisation et d'orienter en conséquence la stratégie de continuité. Cette orientation peut être conçue soit vers une approche privilégiant la continuité des activités essentielles, soit, au contraire, vers une approche acceptant plus facilement les pertes d'activité associées à la prise de risque.

1.2. Identifier les activités essentielles

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. Elles sont considérées comme «essentielles » lorsqu'elles sont nécessaires pour l'atteinte des objectifs de l'organisme et pour 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.

1.3. Cartographier les processus et les flux

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 en sortie des

systèmes d'information, ainsi que les échanges physiques (électricité, eau, matières premières…).Ce travail d'identification doit être réalisé à partir d'entretiens avec les responsables des métiers et des processus et il doit être validé par la direction.

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 et elle se décline assez naturellement à partir de la cartographie des processus.

2. Déterminer les attentes de sécurité pour tenir les objectifs

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.

2.1. Identifier et formaliser les besoins de continuité

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

→ **Le niveau de service minimum**

Ce seuil peut être défini comme un pourcentage de conformité minimum ou un pourcentage de produits/services commandés livrés à la date/heure convenue. (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).

→ **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).

→ **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).

Pour illustrer la notion de DMIA, 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 pourvoir fonctionner en mode dégradé permet une interruption maximale (DMIA) du fonctionnement normal 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).
- Pouvoir transférer le personnel sur des postes nouveaux.
- Faire éventuellement appel à l'intérim.

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 la normale).
- Les modalités acceptables de fonctionnement en mode dégradé.

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 trop complexe n'est pas recommandée. Le choix du périmètre final du PCA relève de la direction générale.

→ **Calculer les coûts du 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.).

2.2. Mesurer les conséquences d'une interruption de service

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 non-respect des obligations légales et réglementaires, sanctions possibles …).
- Impacts opérationnels (coûts de réparation …).
- Conséquences sociales (chômage technique, impact sur les partenaires…).
- Conséquences psychologiques (démotivation, perte de moral…).
- Conséquence sur l'environnement (pollution…).
- Perte de valeur, d'image ou de réputation, et donc perte de confiance ou de marché, voire perte de l'activité.

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 (qu'augmente quand la durée de l'interruption augmente).

Certaines sont en revanche difficilement chiffrables et relèvent davantage d'une appréciation qualitative (à titre d'exemple 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.

3. Identifier, analyser, évaluer et traiter les risques

La démarche de gestion du risque est une démarche globale qui permet de quantifier la probabilité d'occurrence et les impacts des risques, et de 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.

Concrètement, l'organisme peut se référer au guide de gestion des risques réalisé par la DGSSI pour gérer les risques auxquels leurs systèmes d'information sont exposés.

4. Définir la stratégie de continuité d'activités

Il est clair 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.

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.

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

4.1. Définir les objectifs de continuité en mode dégradé et pour la reprise d'activité

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. Ces derniers sont formalisés par des indicateurs qui quantifient deux types d'exigences:

- Exigence concernant les systèmes en place : se définit par la 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.

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.

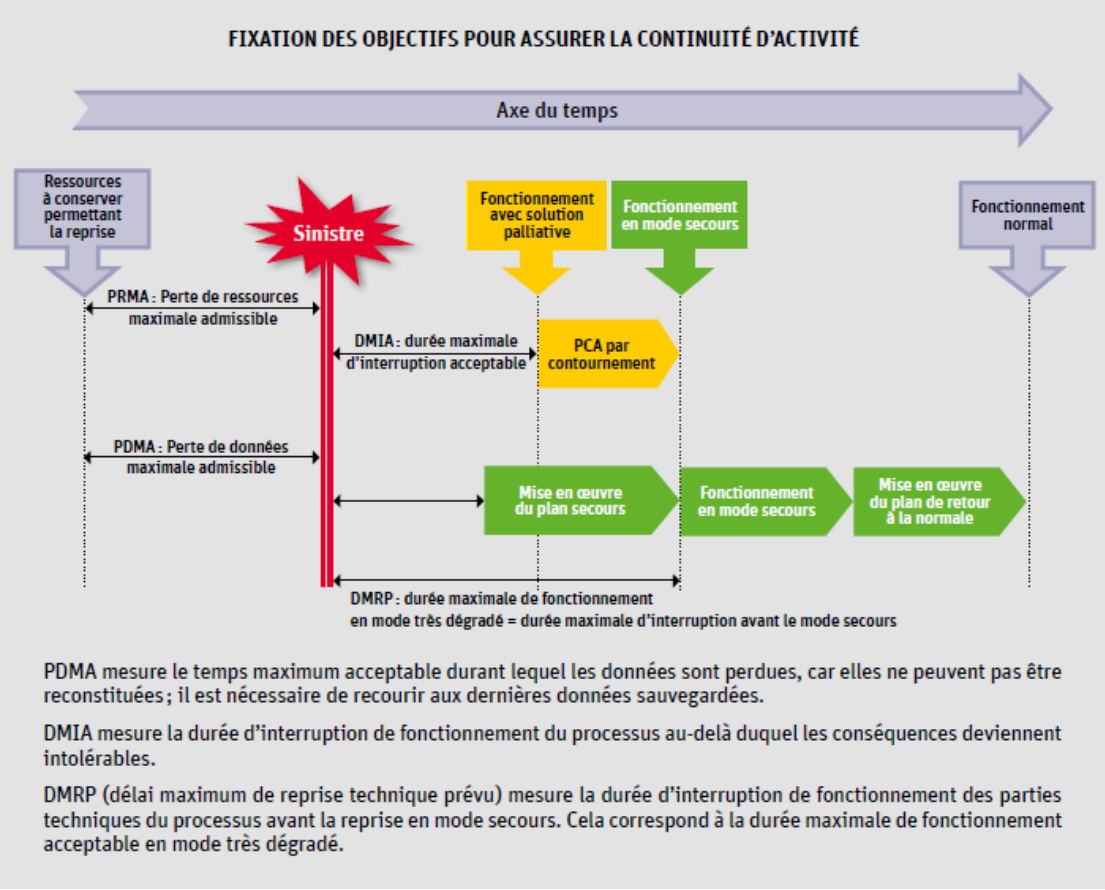
- Exigence concernant les modalités de la réponse mise en œuvre : englobe les exigences de délais pour la reprise d'activité (par la mise en œuvre planifiée d'une solution palliative, puis d'une solution de secours en mode dégradé et enfin la reprise des conditions normales) qui s'imposent aux solutions 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, 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 déclencher le mode secours est souvent une décision qui ne peut plus être annulée.

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



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.

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.

4.2 Définir les exigences sur les ressources nécessaires au PCA

Cet objectif concerne :

- Les ressources humaines ;
- Les systèmes d'information et de communication ;

- Les processus et l'organisation ;
- Les infrastructures ;
- les prestataires externes et les partenaires.

a. 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 responsable 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, elles portent sur les dispositifs à préparer pour permettre la continuité des postes critiques:

- Maintenir techniquement les positions de travail critiques :
  - → 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,
  - → Protection des travailleurs concernés,
  - → Disponibilité de l'outil de travail (notamment des terminaux et moyens informatiques) et des moyens de communication,
  - → Prise en compte de la sécurité informatique (sur les réseaux, les postes de travail),
  - → Prise en compte des mécanismes de sauvegarde des données durant le fonctionnement sur site de repli.

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

- 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.

b. 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, et formaliser la maintenance avec des engagements de résultats.

- Disposer de moyens de télécommunication sécurisés de secours (par exemple systèmes d'alerte robustes).

- En cas d'externalisation des sites de secours, il est recommandé de vérifier cependant le niveau de service et les modalités de continuité, l'existence de séances d'entraînement, l'évolutivité au cours du temps, la protection des données pendant ou après l'utilisation du site de secours, etc.

- Pour les sauvegardes, il est recommandé de mettre en place une procédure de récupération assez flexible pour relancer rapidement les systèmes critiques de l'organisation et elle doit être testée sur l'ensemble des serveurs et systèmes utilisés par une activité de l'organisation et vérifiée par les responsables.

- Il est recommandé de vérifier les possibles vulnérabilités de l'opérateur de télécommunication (connaissance de l'architecture logique et physique des moyens mis à la disposition par l'opérateur).

- Il est recommandé de disposer de moyens de télécommunication indépendants d'Internet et des opérateurs publics, 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.

c. Exigences pour les processus et l'organisation

Afin d'assurer la continuité d'activité des applications et processus critiques correspondants, il est recommandé :

- D'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. Cette solution palliative précède le fonctionnement en mode secours.

- D'organiser la disponibilité de l'accès à un site distant disposant des informations« métier » essentielles, pour faciliter la continuité d'activité.

- De définir les priorités de reprise des processus, 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.

d. 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, etc.).

- 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).

e. Exigences pour les prestataires externes et les partenaires

Ces partenaires peuvent être qualifiés de critiques s'ils sont indispensables pour assurer le fonctionnement 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 :

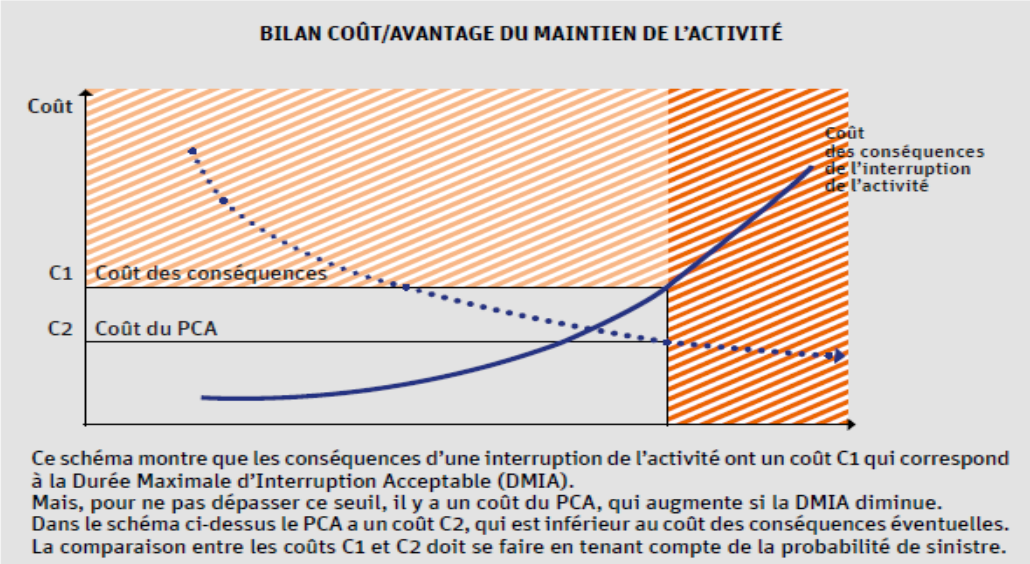
- Importance du poids du partenaire dans la valeur ajoutée de l'organisation.
- Rareté de la matière première fournie.
- Unicité du fournisseur dans un domaine d'activité.
- Absence d'autres fournisseurs ayant la même qualité de service.
- Fonctionnement sans stock.

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.

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).

4.3. Arbitrage du bilan coût/avantages d'un PCA

Plus l'indisponibilité est longue et plus le niveau de service demandé est élevé, plus le coût du dysfonctionnement pour l'organisation sera élevé. 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 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. 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.

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), en fonction des objectifs (et obligations) de l'organisation et de l'appréciation des différents coûts. Cela a des conséquences directes sur le risque possible et sur le coût du PCA.

4.4. Elaborer la stratégie de continuité d'activité

À partir des étapes décrites précédemment, la stratégie de continuité d'activité peut être déclinée. Elle va permettre de formaliser les mécanismes de fonctionnement en modes dégradé 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.

5. Mettre en œuvre et assurer l'appropriation

La gestion de crise 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. Il est possible par la suite 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.

5.1. La mise en œuvre des moyens nécessaires au PCA

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.

→ 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 indicatif:

- Mise en place des dispositifs et procédures qui devront avoir été préalablement définis, formalisés et intégrés dans les processus métier pour être activés 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, la mise en place de procédures de sauvegarde des données).
- Moyens de communication spécialisés 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 en cas de défaillance de partenaire.
- Tests de fonctionnement de ces dispositifs avec la fréquence définie.

→ Processus de gestion de crise et PCA

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 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 de gestion de crise qui concerne également le PCA :

- Procédures liées à la remontée de l'alerte jusqu'à l'activation et suivi du PCA :
  - ✓ Définir un mécanisme de 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,
  - ✓ valider les dispositifs de continuité à mettre en œuvre,
  - ✓ définir un schéma délégataire, permettant la poursuite d'activité et les délégations de signature,
  - ✓ identifier les mesures spécifiques à déclencher pour un fonctionnement en mode dégradé,
  - ✓ assurer un pilotage par la cellule de crise opérationnelle,
  - ✓ Suivre les indicateurs de continuité d'activité.

- Fiches spécifiques permettant de décrire:
  - ✓ Le suivi de la remontée d'alerte,
  - ✓ La quantification de la crise :

lieu/nature/conséquences/actions prises,
- ✓ Les modalités de mobilisation de la cellule de crise : lieu, configuration, convocations,
- ✓ Le retour d'expérience, fiche qui doit être remplie dès le début de la crise, après avoir nommé un responsable pour ce suivi.

→ 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 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 et coordination des actions,
  - ✓ Analyse des conséquences sur les métiers et activités,
  - ✓ Prise de décision,
  - ✓ Relation avec les parties prenantes (dont l'État et les partenaires),
  - ✓ Communication avec les média.

- Les participants à la cellule de crise comprennent à titre indicatif et sans préjudice d'ouverture à d'autres expertises :
  - ✓ le responsable de la gestion de crise,
  - ✓ le responsable du PCA,
  - ✓ 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.

5.2. Déclenchement du PCA

→ 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'organisme 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 concernent les mesures de prévention/ protection/ intervention.

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, dans ce cas il est nécessaire de:

- 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 ou de secours, et identifier les points de non-retour.

→ Déclenchement en phase d'activation

La décision de déclencher le PCA en phase d'activation peut être prise suite aux consignes des autorités compétentes 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, 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 :

- Décision de mettre en place la cellule de crise.

- Décision d'activer ou de mettre en place telle solution palliative et/ou de secours.
- Modalités spécifiques en cas de basculement« à froid » ou « à chaud ».

→ **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 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.

→ **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.
- Il est recommandé, dès le début de la crise, de vérifier que les ressources nécessaires pour la reprise en fonctionnement normal soient prévues et soient progressivement réunies.

5.3. PCA et communication de crise

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 :

1. Le personnel (responsables des métiers et des processus, responsables des activités, tout le personnel, les sous-traitants).
2. Les fournisseurs et clients de l'organisation, qui ont besoin de connaître les dispositifs du PCA et de sa mise en œuvre.
3. Les autres partenaires concernés par la mise en œuvre du PCA.
4. Les services de l'État.
5. 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.

5.4. Les indicateurs d'efficience du 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 (établissement de la liste des postes critiques), les relations avec les fournisseurs (formalisation des exigences, contrôles).

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. 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 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.

5.5. Le maintien en condition opérationnelle du PCA

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 comme expliqué ci-dessous.

→ **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 s'agit 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.

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

- Audit interne périodique, 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 – système de management de la continuité d'activité) par auto-évaluation ou par un organisme de certification tiers.
- Questionnaires d'auto-évaluation sur la connaissance et l'efficacité du PCA.
- Exercices, y compris avec les partenaires stratégiques.
- Vérification du fonctionnement du dispositif d'amélioration continue.