MINISTÈRES
TRANSITION ÉCOLOGIQUE
COHÉSION DES TERRITOIRES
MER

Liberté
Égalité
Fraternité

Guide méthodologique

Elaboration d'un PCA/PRA Cyber en service déconcentré (SD)

Mai 2022

Historique des versions du document

Version	Date	Commentaire
1.0	Mai 22	Version initiale.

Affaire suivie par

Prénom NOM - service
Patrick GUILHOU, SNUM/UNI/DRC, CMSI – Adjoint au chef du département
Bertrand BOUVY, SNUM/UNI/DRC, CMSI (Conseiller en management des Systèmes d'Information)

Rédacteur

Cyril PATRIGEON, expert en cybersécurité, Société CONIX

Relecteurs

- Société CONIX : Sylvain CONCHON, expert en cybersécurité
- SNUM/UNI/DRC : Patrick GUILHOU, Bertrand BOUVY, pilotes de la démarche
- SNUM/DSGC : Alain GOERGEN, Chef du département ; Jean-François BOUTIER, Adjoint ; Delphine AUGER
- Services déconcentrés membres du Groupe de Travail :
    - DRIEAT Ile de France : Jean-Luc WISNIEWSKI, chargé de mission sécurité ; Gaël BINTEIN, chef du département SI et numérique
    - DREAL Pays de Loire : Sylvain PICARD, responsable de l'unité informatique
    - DREAL Corse : Jacques NICOLAU, RSSI – chef du service connaissance, information, logement ; Pierre-Ange MARTOS, chef de l'unité logistique et informatique
    - DIR Ouest : Guirec MORVAN, responsable du pôle systèmes d'information
    - DIRM Méditerranée : Jean-Bernard COSTES, RSSI – Secrétaire Général ; Alexandre BINDL, chef de l'unité informatique – moyens généraux

SOMMAIRE

Table des matières

Synoptique de la démarche

Documentation

Collecter l'existant pour faciliter la démarche

Besoins

Collecter les besoins de continuité métier

Scénarios

Elaborer les scénarios de continuité

Gestion de crise

Préparer la gestion de la crise Cyber

Périmètre

Préciser et délimiter la démarche

Risques

Identifier les risques principaux

Stratégie

Définir la stratégie à mettre en œuvre

Bilan

Ce qui a bien fonctionné
Ce qui peut être amélioré

01. La démarche PCA/PRA Cyber en 2 minutes

Le présent document méthodologique est exhaustif et détaillé afin de soutenir la réalisation d'un PCA/PRA Cyber propre à répondre aux enjeux des services.

Il est proposé ici un parcours de lecture rapide, permettant de connaître les points clefs du projet à engager.

Ces éléments, listés ci-dessous, sont accessibles rapidement grâce à la vignette spécifique qui est apposée aux quelques éléments à lire. Cette vignette est celle présente sur cette page, en entête, et qui sera répétée uniquement sur les pages de cette lecture rapide.

- En premier point, le schéma, proposé en page précédente, présente une vue synthétique et graphique du processus engagé lors d'un projet de PCA/PRA Cyber. [*page 4*]
- En deuxième point, une explication courte de la démarche est déclinée en début de partie 5.a – « Comment élaborer le PCA/PRA Cyber ? - Synthèse de la démarche » [*page 15*].
- En troisième point, l'« Annexe 1 – Modèle de document résultant », permet de se figurer le livrable principal de la démarche [*page 45*].
- Et en dernier point, l'« Annexe 6 – Exemple de fiche réflexe », offre une représentation de ce que seront les éléments d'aide à la décision en cas d'incident que la démarche fournira. [*page 54*]

Ces quelques éléments permettent de se représenter la démarche d'un projet PCA/PRA Cyber, et d'avoir une vue de ses livrables.

***Précision terminologique** : Le terme « Système d'Information » est utilisé ici pour rassembler l'ensemble des dispositifs, moyens et flux qui permettent la captation, le traitement, l'échange et le stockage de l'information. Il s'entend bien entendu pour les ressources numériques, mais aussi pour les documents papiers, les échanges verbaux, les interactions et l'intelligence humaine.*

La terminologie « PCA/PRA Cyber » a été choisie afin de définir l'objet attendu. Elle ne s'entend en aucun cas comme uniquement la concrétisation des résultantes des seules « attaques Cyber », ou « Perte des actifs numériques ».

02.Introduction

a) Fondements du guide

Ce guide propose des éléments de démarche destinés à faciliter l'élaboration du PCA/PRA Cyber dans les services déconcentrés (SD). La démarche proposée ici est une démarche simplifiée. Pour mettre en œuvre une méthode plus approfondie, plus formelle et plus systématique, le lecteur se reportera aux pratiques de gestion de la continuité d'activité décrite au chapitre « Pour aller plus loin… » (page 41).

La démarche permet la réalisation du Plan de Continuité d'Activité Cyber (PCA Cyber) ainsi que du Plan de Reprise d'Activité Cyber (PRA Cyber), l'objectif étant de permettre la mise en place des **mesures** qui garantissent, en situation d'incident, une **continuité** de fonctionnement des **missions** identifiées comme ayant une exigence de disponibilité élevée.

Ce document s'adresse :

- Aux équipes de direction des services déconcentrés (SD), dont le directeur en tant qu'Autorité Qualifiée de Sécurité des Systèmes d'Information (AQSSI) ;
- Aux personnes agissant sous leur responsabilité, en particulier celles impliquées dans :
    - La gestion de la continuité d'activité du service,
    - La direction et l'exploitation du Système d'Information (SI)
    - La mise en œuvre de la sécurité des SI dont le Responsable de la Sécurité des Systèmes d'Information (RSSI)

*La démarche se veut **pragmatique**, et propose des « **trucs et astuces** » pour aider à la réalisation de certaines étapes, mais aussi des « **modèles de résultats** » pour aider à la structure des réponses à apporter aux différentes étapes.*

b) Champ d'application du guide

Dans le cadre de ce guide pratique, le périmètre d'applicabilité est l'ensemble des activités quelle que soit la typologie du service déconcentré (SD) concerné, quelles que soient les finalités et le mode d'exercice de celles-ci.

Le champ d'application, quant à lui, est défini par l'ensemble des incidents ayant un impact, direct ou indirect, sur le Système d'Information et perturbant en tout ou partie les métiers concernés.

Il ne prend pas en compte les éventuelles dispositions organisationnelles qui peuvent être mises en place pour assurer la continuité des activités métier lorsque le Système d'Information n'intervient pas dans la chaîne de conséquences. Cela doit être étudié dans le cadre du plan de continuité d'activité global du service.

Pour l'ensemble de ces périmètres, le présent guide décrit une approche applicable et pragmatique à la réalisation d'un PCA/PRA Cyber.

c) Enjeux relatifs à la continuité des activités

Afin de réduire les impacts négatifs de l'indisponibilité de tout ou partie des ressources du Système d'Information nécessaires aux missions à exigence de disponibilité élevée, des mesures doivent être prévues, mises en place et vérifiées. Ces mesures, de natures organisationnelles comme techniques, peuvent intervenir :

- En amont de l'incident, pour répondre aux exigences formalisées dans la Politique Générale de Sécurité des Systèmes d'Information (PGSSI) du pôle ministériel et sa déclinaison propre au service déconcentré (SD) (Dossier PGSSI) afin d'éviter la survenance d'un incident ;

- En aval de l'incident, pour assurer un fonctionnement des missions à l'aide de moyens temporaires permettant d'en assurer la continuité.

Outre les enjeux parfois critiques liés à leur disponibilité (D), les activités peuvent être soumises à d'autres nécessités fortes de sécurité, précisées au sein du dossier PGSSI (dont l'analyse DICT des SI sensibles) :

- Nécessité d'exactitude ou d'intégrité (I) des informations traitées ;

- Nécessité de confidentialité (C) de certaines informations, par exemple lorsqu'il s'agit de données à caractère personnel ;

- Nécessité de traçabilité (T) ou d'imputabilité

Or ces contraintes doivent être prises en compte non seulement dans le fonctionnement normal du SI, mais **également en situation d'incident** où les mesures prévues par le PCA/PRA Cyber sont mises en œuvre. Ces exigences, quand elles s'ajoutent à une situation de crise, peuvent nécessiter des compromis dont les impacts doivent impérativement être compris et maîtrisés.

Les SI des services déconcentrés (SD) peuvent présenter des spécificités qui imposent des exigences particulières, voire qui interdisent l'usage de certaines solutions de continuité qui seraient acceptables dans d'autres secteurs.

Par exemple : Il n'est peut-être pas envisageable d'utiliser une solution non souveraine lorsqu'il existe des solutions nationales ou ministérielles.

Le présent guide vise à proposer une méthode pour soutenir la concrétisation du Plan de Continuité et de Reprise d'activités du Système d'Information. Ce PCA/PRA Cyber s'inscrit au sein du PCA/PRA global du service.

Le PCA/PRA Global peut déjà avoir été partiellement pensé, notamment vis-à-vis des réactions à avoir en cas de pandémie. Ces actions pensées concernent l'ensemble des moyens du service, et surement en partie les ressources numériques.

Le PCA/PRA Cyber peut tout à fait être entrepris sans que le PCA/PRA global n'existe au sein du service. Ce dernier, s'il existe, est une entrée souhaitable pour maintenir une cohérence d'ensemble. Mais, il n'est clairement pas nécessaire en tant que tel pour la bonne réalisation de la méthodologie proposée ici.

Le PCA/PRA Cyber permet de trouver réponse à l'ensemble des problématiques qui impacteraient les métiers du service via l'atteinte aux ressources numériques.

03.Définitions liées à la continuité d'activité

Incident : Situation qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise (source ISO 22300)

Plan de Continuité d'Activité (PCA) : Ensemble des mesures prévues pour maintenir une activité minimale (ou dégradée) des missions à exigence de disponibilité élevée après qu'elles aient été interrompues par suite d'un incident.

Plan de Reprise d'Activité (PRA) : Ensemble des mesures prévues pour rétablir l'activité de la structure après qu'elle ait été interrompue suite à un incident.

Mode dégradé : Un composant ou un service fourni par le SI, ou le SI dans son ensemble, est dit fonctionner en mode dégradé quand il ne rend pas l'ensemble des fonctions qu'il est censé fournir ou quand les performances de ces fonctions sont inférieures aux paramètres nominaux (temps de réponse, capacité de stockage, nombre d'utilisateurs, débit des liaisons, …)

Perte de Données Maximale Acceptée (PDMA) : Durée de production de données perdues par suite d'incident, correspondant aux données produites par les personnels réalisant les missions depuis la dernière occurrence de la sauvegarde.

Durée Maximale d'Interruption Acceptable (DMIA) : Temps maximum pendant lequel aucune solution, même dégradée, n'est à même de réaliser le service fourni par le SI ayant subi l'incident.

Sauvegarde : Opération qui consiste à dupliquer et à conserver de manière sécurisée des systèmes d'information et/ou des données contenues dans un système d'information afin d'assurer leur disponibilité et leur réutilisabilité même en cas d'incident ou d'erreur de manipulation portant atteinte à leur intégrité. Les principes généraux de sauvegarde des données doivent être définis dans un Plan de sauvegarde ; une attention particulière sera portée à la non-porosité des sauvegardes déjà effectuées avec le système d'information dans le cas d'infection de type rançongiciel notamment.

Le terme de « système à haute disponibilité » est parfois rencontré. Il désigne des systèmes qui mettent en œuvre des solutions techniques, souvent par duplication

(ou « redondance ») de leurs composants, afin de prévenir une interruption des services qu'ils fournissent.
Ces solutions ne permettent pas nécessairement de couvrir tous les scénarios d'incident envisagés et il reste nécessaire de prévoir des solutions palliatives ou des solutions de secours dans le cadre d'un PCA/PRA Cyber.

04.Les concepts clés pour élaborer un PCA/PRA Cyber

a) PCA/PRA Cyber

Une partie importante des activités des Services Déconcentrés s'appuie sur le Système d'Information pour leur bonne réalisation, et peut donc être plus ou moins fortement impactée par un événement mettant à mal la disponibilité dudit Système d'Information.

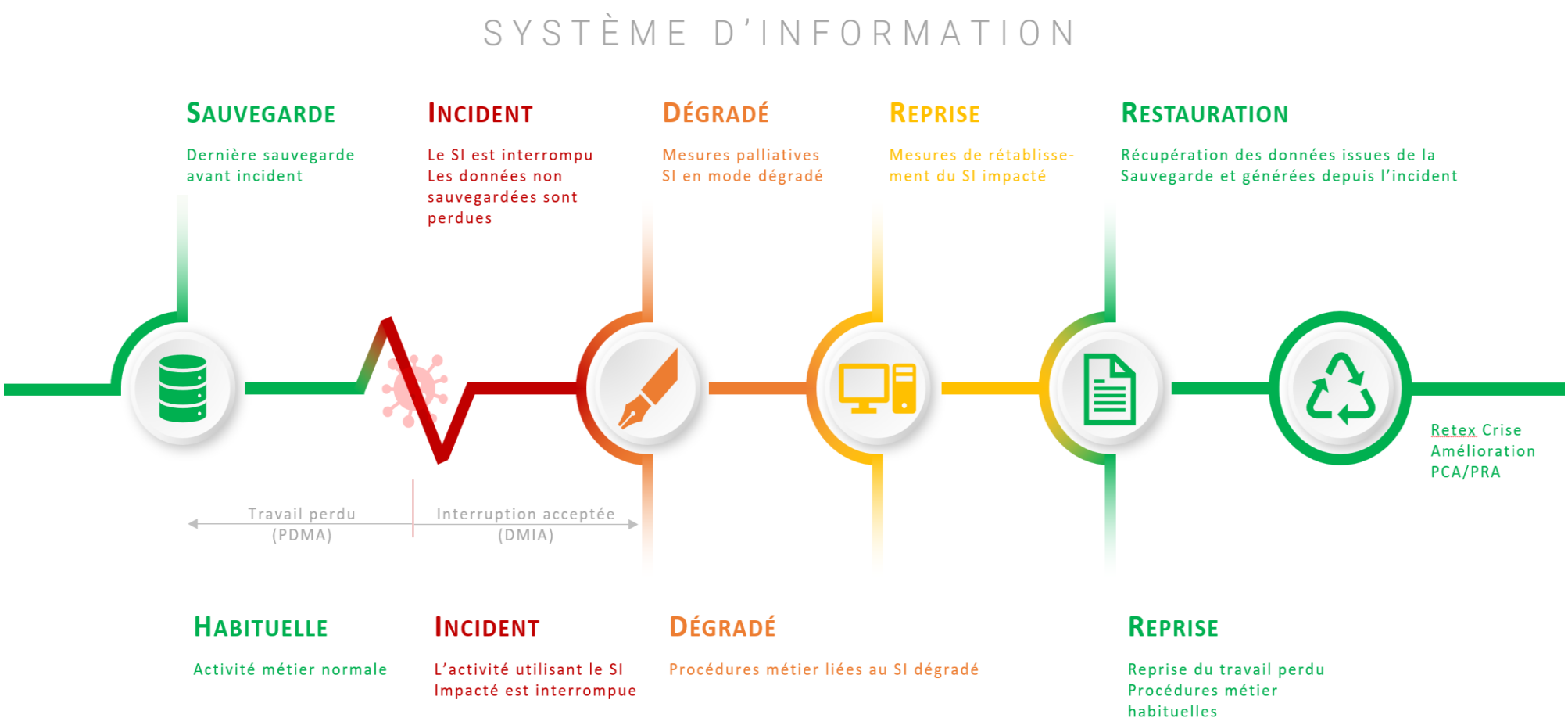
Le dispositif de **continuité** de fonctionnement est constitué de **l'ensemble des mesures** visant à répondre à divers scénarios de crises (les incidents étant eux même issus du Système d'Information ou ayant un impact sur celui-ci) afin de garantir le **maintien des missions à exigence de disponibilité élevée**. Ce maintien peut se faire temporairement selon un mode appelé « dégradé ».

Le dispositif de **reprise** d'activité vise quant à lui à permettre une remontée des missions en mode nominal.

Le mode dégradé vise à proposer une réponse rapide afin de réduire autant que possible l'interruption des missions ; la remontée au mode nominal pouvant être plus ou moins importante en fonction de l'ampleur de l'incident.

b) Traitement d'un incident qui impacte la continuité

Le schéma ci-après présente, de manière macroscopique, les différentes phases du traitement d'un incident qui impacte la continuité des missions à exigence de disponibilité élevée.


SYSTÈME D'INFORMATION
SAUVEGARDE
Dernière sauvegarde avant incident
INCIDENT
Le SI est interrompu
Les données non sauvegardées sont perdues
DÉGRADÉ
Mesures palliatives
SI en mode dégradé
REPRISE
Mesures de rétablisse-ment du SI impacté
RESTAURATION
Récupération des données issues de la Sauvegarde et générées depuis l'incident
Retex Crise
Amélioration
PCA/PRA
Travail perdu
(PDMA)
Interruption acceptée
(DMIA)
HABITUELLE
Activité métier normale
INCIDENT
L'activité utilisant le SI
Impacté est interrompue
DÉGRADÉ
Procédures métier liées au SI dégradé
REPRISE
Reprise du travail perdu
Procédures métier
habituelles
PROCESSUS METIERS

Ce schéma fait apparaître plusieurs points clés, présentés chronologiquement ci-dessous :

- **L'incident** qui provoque l'interruption du SI, par rapport auquel on identifie :
    - Les données créées avant l'incident et après la dernière sauvegarde des données, ces données peuvent être non recouvrables par un processus SI, uniquement par un processus métier de reconstruction. La durée maximale avant un incident pendant laquelle les métiers acceptent de perdre des données doit être spécifiée par l'indicateur **PDMA** (Perte de Données Maximale Acceptée).
    - La Durée Maximale d'Interruption Acceptée (**DMIA**) après survenance de l'incident. Cette durée est fixée par chaque métier, elle est liée à la nécessité de disponibilité des missions assurées par le métier. Elle est définie en fonction des contraintes propres du métier.

- Après le délai de réaction nécessaire à la détection de l'incident et à la mobilisation des acteurs, puis après le délai de décision nécessaire à la sélection des actions à mener dans le cadre de la gestion de crise, la cellule de gestion de crise déclenche la mise en application du volet « **Continuité** » du PCA/PRA Cyber :
    - La reprise progressive en **mode dégradé** du SI se fait en mettant en œuvre des mesures de fonctionnement palliatives (ou de secours). Cette reprise donne la priorité aux systèmes identifiés comme les plus critiques, à même d'assurer les missions identifiées comme ayant une exigence de disponibilité la plus élevée.
    - Pendant cette période, tout ou partie du SI fonctionne en mode dégradé, mode dans lequel il ne fournit que partiellement les services attendus. Des procédures métiers dégradées adaptées à cette réduction du niveau de service fourni par le SI peuvent alors être nécessaires.

- Le SI doit redevenir complètement opérationnel dans un **délai acceptable par les métiers**. Les missions pourront de nouveau s'appuyer sur les procédures fonctionnelles normales.
    - Les opérations de récupération / reprise des données doivent être menées. Elles portent sur les données éventuellement produites dans le cadre des procédures dégradées et de l'utilisation de moyens palliatifs d'une part, et sur la reconstitution ou la ressaisie des données perdues à la suite de l'incident d'autre part.

- La **fin de crise** peut être décrétée quand il est validé que l'ensemble des systèmes et des données sont restaurés dans un état normal et que les missions fonctionnent de nouveau en mode nominal.

Le PCA/PRA Cyber proposera à la fois des mesures pour continuer l'activité métier pendant la crise que des mesures pour rétablir au nominal le SI.

c) Réfléchir en amont du besoin de continuité

Pour que les incidents puissent être traités efficacement, le service doit **organiser la surveillance** des évènements qui interviennent au sein du Système d'Information, leur analyse et leur qualification éventuelle en incident.

Les différentes étapes de traitement d'un incident qui impacte la continuité du SI doivent être pilotées par une structure dédiée, quand nécessaire, une mobilisation de la **cellule de crise** qui est l'organe central et indispensable de la gestion de la crise Cyber.

L'organisation de continuité de fonctionnement du SI s'appuie en premier lieu sur les circuits existants au sein du service en termes de continuité d'activité globale et de gestion de crise.

05. Comment élaborer le PCA/PRA Cyber ?

a) Synthèse de la démarche

La démarche visant à produire le PCA/PRA Cyber nécessite une certaine organisation, ceci afin d'être certain de prendre en compte les risques les plus impactants pour l'organisation en priorité.

Pour ce faire nous allons détailler dans les paragraphes suivants :

L'organisation à mettre en place pour réaliser le PCA/PRA Cyber,

Les **documents** qu'il convient de collecter afin de soutenir la démarche,

La contextualisation du document à un **périmètre** connu et déclaré,

La collecte du **besoin métier** en termes de continuité,

L'analyse des risques pesant sur les objets qui permettent de réaliser les missions du service

L'élaboration des **scénarios de continuité** à mettre en place

La **déclinaison stratégique** de la gestion d'un incident

L'organisation à mettre en œuvre pour **répondre à la crise**.

Le **retour d'expérience** permettant l'amélioration du PCA/PRA Cyber

La réalisation de cette démarche constitue un projet à part entière, il impliquera un certain nombre de personnes issues des différents métiers et nécessitera une certaine charge. C'est à ce prix que le résultat sera utile et probant lors d'une crise !

Un exemple d'analyse de risque, sur une mission « fictive » à exigence de disponibilité élevée, est proposé plus avant dans le document (voir en page 29)

Le PCA/PRA Cyber : anticiper pour mieux gérer !

b) Organisation

Mener à bien ce projet n'est pas qu'une affaire de **méthodologie** à suivre, c'est également la conséquence d'une **bonne organisation**. Quelles que soient les phases du projet, s'appuyer sur les sachants du domaine sera nécessaire à une bonne réalisation et en lien avec les métiers concernés.

C'est pourquoi il convient, lors de l'organisation du projet, d'identifier clairement les **parties prenantes** qui seront en mesure d'apporter l'information nécessaire. Nous parlons ici :

- Des cadres de direction dont le chef de projet : le RSSI ou responsable clairement légitime dans l'entité,
- Des sachants des différents outils utilisés par les métiers,
- Des « sachants » de l'infrastructure du SI sous-jacente et nécessaire,
- Des personnes en mesure de renseigner sur les moyens de réduction de risques déjà existants, ainsi que des moyens de maintien en conditions opérationnelles déjà déployés. Par exemple : les tiers exploitant ou les maîtrises d'œuvre d'une partie du SI,
- Des porteurs de la documentation de gestion du risque déjà formalisée.

Tout autant lors des phases initiales de collecte d'information et des besoins, lors de la phase d'analyse et lors de la phase de réflexion sur l'organisation de continuité à mettre en œuvre, **l'adhésion** des parties prenantes au projet sera nécessaire.

Il est nécessaire que la Direction s'engage très fortement dans cette démarche d'élaboration du PCA/PRA Cyber.

En outre, un pilote projet est à désigner. Il aura pour rôle :

- De **coordonner** le projet tout au long de son déroulement,
- D'**élaborer** le PCA/PRA Cyber en relation avec le responsable du SI, le RSSI et le responsable du PCA global,
- De **rendre compte** de l'avancement du projet,
- De conduire les **exercices** nécessaires à l'entraînement à la crise à l'issue de la réalisation du PCA/PRA Cyber,
- De **maintenir** opérationnel le PCA/PRA Cyber au fil du temps.

Un pilote légitime aux commandes pour que la démarche se déroule sans accrocs !

A cette phase il est nécessaire d'identifier la forme résultante que prendront les travaux de réalisation du PCA/PRA Cyber. Il peut s'agir :

- D'un document autonome,
- D'une adjonction à un document PCA/PRA plus global existant déjà,
- D'ajouts ciblés au sein de procédures déjà existantes au sein du service,
- Ou de tout autre forme en lien avec la culture existante de gestion du risque du service.

c) Collecte préliminaire de documentation

Pour faciliter la réalisation du projet un certain nombre de documents, s'ils existent, peuvent être collectés. Nous précisons ici que ces documents ne sont **pas nécessaires** pour la réalisation du PCA/PRA Cyber, celui-ci pouvant être terminé sans aucun document complémentaire, cependant ils permettent **d'accélérer le processus** et de faire reposer la démarche sur des bases déjà établies et approuvées par ailleurs.

Collecter l'existant pour faciliter la démarche !

Une liste non exhaustive de documents utiles à la démarche est produite ci-dessous. La section de la démarche sur laquelle porte leur utilité est indiquée. De manière similaire, lors de l'explication de la démarche si un document s'avère aidant à l'étape concerné il sera pointé en référence à cette liste, et ses apports seront explicités de manière plus détaillée :

[DOC.01] **Organigramme général et détaillé :** ce document précise généralement les différents métiers du service et en indique les responsables. Il sera utile dans la définition du périmètre cible du PCA/PRA Cyber et également dans l'identification des parties prenantes avec lesquelles s'entretenir pour la récolte du besoin.

[DOC.02] **Cartographie des implantations géographiques du service** : ce document décrit l'ensemble des sites sur lesquels le service est implanté, il peut en outre y préciser les fonctions que chaque site abrite ainsi que les particularités en termes de SI. Ce document sera utile dans la définition du périmètre cible du PCA/PRA Cyber.

[DOC.03] **Inventaire des missions essentielles :** l'inventaire et évaluation des SI sensibles (approche DICT) qui peut avoir été réalisée peut-être une bonne base. Il permet de

disposer d'une liste des missions du service où le critère de disponibilité du SI qui les soutient a été évalué. Ce document sera utile dans la phase de compréhension du besoin de continuité des missions.

[DOC.04] **PCA/PRA Global :** ce document précise généralement les dispositions de continuité et de retour à l'activité qui ont été réfléchies par le service dans le cadre de risques globaux. Il peut n'exister que pour certains risques très impactants pour le service, comme le risque Pandémique, mais quel que soit son périmètre il sera un allié de poids dans la partie d'étude des risques au moment de l'évaluation des menaces. Par ailleurs, comme nous l'évoquions au paragraphe précédent il peut également être utile dans le cas où il est décidé d'adjoindre le PCA/PRA Cyber à celui-ci.

[DOC.05] **Plan de prévention aux risques naturels et technologiques :** ce (ou ces) document précise notamment les périmètres géographiques sur lesquels des risques naturels et/ou technologiques pèsent sur le service. Il propose également les mesures mises en place pour prévenir ces risques. Ce document sera donc utile dans l'analyse des risques au moment de l'évaluation des menaces, précisément en ce qui concerne les menaces naturelles et technologiques. Par ailleurs il pourra également être utile dans la partie définition du périmètre du PCA/PRA Cyber dans le cas où il convient d'apporter des précisions relatives aux disparités des différents établissements du service.

[DOC.06] **Analyse de risques (sur tout ou partie du périmètre SI) :** ce (ou ces) document s'il existe détaille une analyse de risque réalisée sur tout ou partie du SI, et à ce titre précise les menaces qui ont été retenues ainsi que les mesures d'amoindrissement du risque. Ce document sera donc utile lors de l'analyse des risques afin de corroborer les parties concernées par ce document. Par ailleurs, si les mesures proposées par l'analyse ont été mises en œuvre, cela permettra d'apprécier la gravité des risques à l'aune de ces mesures.

[DOC.07] **Plan d'actions d'amélioration du SI :** ce document liste les actions réfléchies afin d'améliorer le SI, ce sont notamment les mesures liées à la sécurité et plus précisément à la disponibilité qui sont intéressantes et utiles ici. Ce document, à l'instar du précédent, sera donc utile lors de l'analyse des risques afin de valider les cotations de vraisemblance des menaces par rapport à l'avancement des actions du plan.

[DOC.08] **Architecture du SI (globale ou détaillée) :** ce (ou ces) document précise les différents éléments qui composent le SI, l'idée ici est d'avoir une vision macro du SI qui identifie les différents réseaux, serveurs, terminaux et points d'entrée/sortie qui le compose. Dans le cas où le service dispose de plusieurs sites, il est utile de disposer des différences qui les caractérisent. Dans le cas où le service dispose de plusieurs SI (métier et bureautique par exemple), il est utile de disposer de l'architecture de chacun d'eux de manière séparée ainsi que des éventuels points de jonction qui existent entre eux. Ce document sera utile principalement dans la partie d'analyse des risques facilitant l'identification des biens supports (notion explicitée au chapitre 3.f). Il sera également utile lors de la définition du périmètre du document, ce périmètre pouvant s'appuyer sur une distinction propre à l'architecture.

[DOC.09] **Bonnes pratiques internes formalisées** : ce (ou ces) document précise l'ensemble des bonnes pratiques en vigueur au sein du service. Ces bonnes pratiques visant à

améliorer le niveau de sécurité global du service. Ce document sera utile dans la partie d'analyse des risques pour l'évaluation de la vraisemblance des menaces.

[DOC.10] **Plan d'organisation des crises** : ce document précise l'organisation qui est en place au sein du service pour gérer les crises lorsque celles-ci surviennent. Ce document sera utile lors de l'élaboration de l'organisation de crise de la démarche.

[DOC.11] **Fiches de gestion d'incidents** : ce (ou ces) document précise la manière d'agir qui a été réfléchie en réaction à un incident, que cet incident soit lié au SI ou pas. Ce document sera utile dans l'élaboration de la stratégie de continuité, mais également dans la réflexion concernant la gestion de la crise.

[DOC.12] **Plan de sensibilisation SI** : ce (ou ces) document précise les sensibilisations qui sont prodiguées à tout ou partie du personnel du service, notamment concernant l'usage qui doit être fait du SI, les actions autorisées ou non, ainsi que les comportements de sécurité à adopter. Ce document sera utile dans la partie d'analyse des risques pour l'évaluation de la vraisemblance de certaines menaces.

[DOC.13] **Charte informatique** : ce document précise les droits et usages des usagers du SI en vigueur au sein du service. De manière similaire il sera utile dans la partie d'analyse des risques pour l'évaluation de la vraisemblance de certaines menaces.

[DOC.14] **Contrats et conventions avec des tiers** : ces documents précisent les accords qui ont été décidés dans le cas de relation avec un tiers. Les services peuvent être de plusieurs natures : logicielle, matérielle et sa maintenance, fourniture de connectivité, fourniture d'énergie, location de bâtiment, mise à disposition de personnel. Lorsque ces tiers fournissent un service entrant dans le périmètre du PCA/PRA Cyber, les informations relatives aux mesures de continuité prises dans le cadre de la fourniture de ce service peuvent être formalisées en leur sein. Ce document sera utile lors de la phase d'élaboration de la stratégie de continuité. Par exemple : les contrats avec des prestataires (hébergement de site internet, contrat de maintenance d'une application locale, …) ou encore la convention avec Dreal, ou SGC, …

Cette liste de documents n'est pas exhaustive, tout document qui se révèle utile à soutenir la démarche peut être collecté à ce stade. Par ailleurs cette liste de documents n'a pas pour objectif d'être collectée en totalité, il s'agit de conseils pour faciliter la démarche d'élaboration du PCA/PRA Cyber.

d) Contexte et Périmètre

La définition du périmètre et du contexte est nécessaire et introductive de la démarche. Elle conditionne le résultat à obtenir, les investigations à mener, mais aussi les personnes à impliquer dans le projet pour couvrir l'entièreté du périmètre souhaité.

La définition du périmètre doit être mûrement réfléchie avec les personnes identifiées dans le projet, en effet un périmètre trop important impliquera une charge de travail plus conséquente et peut voir le projet ne pas aboutir. A contrario, un périmètre trop restreint peut apparaître comme anodin voire inutile et ne pas susciter l'adhésion des parties prenantes.

Conseil : *Penser le* ***périmètre par itérations successives****, à l'image de la défense en profondeur d'un SI.*

Une telle approche est intéressante dans l'optique d'un travail incrémental et pragmatique. Le PCA/PRA Cyber peut être pensé par résultats cumulatifs partant du cœur de métier et adjoignant à chaque itération des métiers ou fonctions supports supplémentaires, ou en démarrant par le cœur géographique de l'organisme et abondant à chaque itération un site supplémentaire.

Attention à avoir les ambitions de ses moyens ! Si les moyens à disposition du projet sont faibles, il est vital pour sa réussite de se concentrer sur l'essentiel.

Les différents éléments de contexte et de périmètre à préciser sont les suivants :

Le « périmètre » géographique : Le service peut être implanté sur plusieurs sites, chacun d'eux pouvant avoir ses menaces spécifiques. A ce stade il faut définir les sites qui seront retenus pour le projet, et préciser pour chacun d'eux les spécificités éventuelles (par exemple : lieu principal abritant le cœur de SI, ou encore lieu possédant des particularités l'exposant à certaines menaces, ou encore lieu domiciliant une ou des fonctions particulières).

A ce stade le document « Cartographie des implantations géographiques du service », référencé [DOC.02], contribue à soutenir cette définition.

Le périmètre fonctionnel : Le service peut avoir plusieurs périmètres fonctionnels. Il est nécessaire à ce stade de définir ceux qui seront choisis pour le projet. Les prend-on en compte en même temps ou selon un schéma itératif ? Les différents périmètres peuvent avoir des menaces complètement différentes ; ou bien l'intensité des impacts ou de la vraisemblance sur un périmètre peut distordre l'analyse sur les autres.

Il vous est fourni en Annexe 3 une liste des missions des différents services classées par « criticité » vis-à-vis du critère de la disponibilité. Cette liste est issue des différentes analyses « DICT » réalisées.

Par exemple :

La mission de vigilance hydrologique et la mission de prévention des risques anthropiques sont des missions critiques pour les DREAL/DEAL.

La mission de gestion de la pollution maritime et la mission de sauvetage en mer sont des missions critiques pour les DIRM/DM.

La mission de gestion des urgences et crises routières et la mission de gestion du trafic routier sont des missions critiques pour les DIR.

A ce stade les documents « Organigramme général et détaillé », référencé [DOC.01], « Inventaire et évaluation des SI sensibles (approche DICT) », référencé [DOC.03] et « PCA/PRA Global », référencé [DOC.04] contribuent à soutenir cette définition.

Le périmètre technique : L'architecture technique du service déconcentré (SD) peut comporter plusieurs SI distincts et destinés à des fonctions particulières. Par exemple la distinction entre un SI bureautique et un SI métier peut susciter le besoin de scinder le projet en deux sous-projets, notamment du fait des spécificités trop grandes de chacun d'eux.

A ce stade le document « Architecture du SI (globale ou détaillée) », référencé [DOC.08], contribue à soutenir cette définition.

Le contexte interne : Il est nécessaire d'identifier les éléments du contexte interne du service qui exerceront une influence sur la démarche PCA/PRA Cyber. Par exemple la culture propre de gestion de crise du service soutiendra la démarche dans sa partie d'identification de la gestion de crise. Les points sur lesquels il faut porter son attention afin d'identifier en quelle manière ils soutiendront ou influenceront la démarche sont notamment : le style de gouvernance, la politique de gestion des ressources humaines et l'existence d'astreintes ou encore la politique de gestion du SI.

Le contexte externe : De manière similaire il faut identifier les éléments exerçant une influence sur la démarche PCA/PRA Cyber issues du contexte externe du service. Nous parlons ici de la règlementation par exemple (le RGPD est une contrainte externe imposant une certaine gestion des données personnelles y compris en cas de crise), mais aussi de l'environnement social ou « culturel » auquel le service est confronté de par son implémentation géographique qui peut exercer une influence au moment de l'élaboration de la stratégie de continuité. Les éléments d'ordre juridique ou politique sont également à identifier s'ils ont un impact sur les choix possibles dans la suite de la démarche. Enfin il est nécessaire d'identifier ici l'ensemble des dépendances aux tiers portées par le service, ces dépendances peuvent être envers d'autres services du ministère, ou bien envers des services centraux du ministère, ou envers d'autres ministères, ou encore envers des tiers privés.

Pour cette partie, sans que cela soit exhaustif, vous trouverez en annexe 2 une liste des dépendances probables du service. Attention cette liste est non exhaustive, charge à vous de valider qu'il n'existe pas d'autres dépendances (notamment vis-à-vis de tiers privés). Par ailleurs, il se peut que certains éléments de cette liste ne vous concernent pas du fait de l'hétérogénéité des services du ministère.

Par exemple, pour l'applicatif CHORUS, la dépendance à signifier ici est le service SG/DAF/CIF3.

La typologie des menaces : même si l'analyse des menaces sera évoquée au niveau de l'analyse de risques, il convient dès l'origine du projet de valider le périmètre des menaces qui seront étudiées. Est-il envisagé de couvrir l'ensemble des menaces du spectre, de ne retenir que le menaces d'origine Cyber, de prendre en compte la maladresse et l'erreur humaine, d'écarter les origines intentionnelles issues du personnel du service, autant de paramètres qui sont des choix initiaux et qui orienteront le PCA/PRA Cyber.

A ce stade le document « PCA/PRA Global », référencé [DOC.04] contribue à soutenir ces choix.

***Conseil :** pour commencer, il peut être intéressant de ne choisir qu'une seule mission pour la réalisation de la première itération du PCA/PRA Cyber.*

e) Besoins de continuité

A la suite des sections précédentes, il faut désormais identifier l'attente en termes de continuité des différentes missions retenues sur les périmètres choisis.

Cette étape se déroule principalement en relation avec les **responsables** de la réalisation des **missions** conservées à ce stade. Les entretiens avec ces dépositaires visent à identifier un certain nombre de caractéristiques déterminant leur **besoin de continuité**.

Il est donc utile, pour chaque mission, chaque processus et chaque flux retenu d'identifier les constituants suivants :

- Une **description** détaillée de la mission (du processus ou du flux), elle vise notamment à s'accorder sur un contenu commun et défini. Par ailleurs elle précise les enjeux et contraintes de la mission en question.

- Une liste de ses éventuelles **dépendances** (amonts ou avals) à d'autres missions (processus ou flux), il sera précisé notamment les dépendances critiques ainsi que les partenaires qu'elles impliquent.

- Les **ressources** nécessaires à sa réalisation. Ces ressources sont de différents ordres (voir ci-dessous pour plus de détail). Il faut également préciser les ressources qui sont considérées comme critiques (celles dont il n'est pas possible de se passer pour la réalisation de la mission). Il est important également d'identifier celles qui sont liées à une dépendance de celles qui sont gérées en propres par le service.

- La durée d'indisponibilité maximale acceptable (appelée également **DMIA**), première des attentes en termes de continuité.

- Les **impacts** d'une indisponibilité supérieure à la DMIA. Les impacts peuvent être de plusieurs natures (voir ci-dessous pour plus de détails).

Conseil : *L'identification des impacts d'une indisponibilité permet de valider le niveau de DMIA retenu.*

- La perte de données maximale acceptable (appelée également **PDMA**), deuxième des attentes en termes de continuité.

- Le niveau de **service minimum** acceptable (en deçà duquel la mission est considérée comme complètement interrompue), la mission peut par exemple être considérée comme suspendue lorsque le réseau est indisponible, ou bien seulement considérée comme perturbée étant en mesure de fonctionner en mode « hors-ligne » sans gêne pendant une courte période. Il est utile à ce stade de décliner sur les différents éléments supports cette distinction de l'acceptabilité de l'interruption de la mission, qui n'entraîne pas forcément une interruption complète et donc une indisponibilité de celle-ci.

- Des **modes dégradés** éventuels palliatifs. Les modes dégradés possibles nécessitent probablement des ressources pour pouvoir être réalisables, il est important à ce stade d'identifier ces ressources nécessaires.

Une DMIA courte doit être justifiée par au moins un impact majeur en cas d'indisponibilité !

Les ressources peuvent être de plusieurs natures :

- **Humaines** : personne clef réalisant tout ou partie de la mission et dont les compétences ne sont pas redondées,

- **Matérielles** : dispositif technique nécessaire à la réalisation de la mission qu'il n'est pas possible de rétablir aisément. Par exemple un ordinateur avec

ou sans caractéristiques particulières (comme des dispositifs de capture ou d'enregistrement, ou encore des dispositifs techniques encore plus spécifiques).

- **Infrastructure** : architecture technique permettant à la mission de se réaliser, et sans laquelle elle n'est plus possible (par exemple infrastructure de surveillance à l'aide de sondes, réseau informatique, …).

- **Applicatives** : application locale (sur poste ou serveur du service ou prestataire locale) ou nationale (centre serveur) permettant de réaliser la mission et sans laquelle elle n'est plus réalisable (par exemple environnement de gestion des méls, espace de travail collaboratif, applicatif métier particulier, …)

- **Information** (formalisée ou non) : données nécessaires à la réalisation de la mission et sans lesquelles il n'est pas envisageable de la produire dans les mêmes conditions (par exemple statistiques réalisées à partir de relevés quotidiens, sans relevé la statistique n'est plus probante).

- **Diverses** : nous parlons ici des énergies nécessaires à la réalisation de la mission (électricité, chauffage), mais aussi de l'environnement de travail (bâtiment, bureau, chaise, …), mais encore des moyens de transports. Toute ressource nécessaire à la réalisation de la mission ne pouvant apparaître dans les sections précédentes.

L'analyse des impacts peut être réalisée au travers de cas fictifs de survenance d'un risque majeur ; par exemple perte totale du SI par suite d'un Ransomware, ou bien encore départ d'une personne ressource clef.

Les impacts peuvent être exprimés sous plusieurs axes (Les métriques propres au Pôle Ministériel issues de l'annexe B de la PGSSI sont rappelées en annexe 7 du présent document) :

- **Financiers** : avec une échelle allant de l'impact budgétaire limité pour le service aux pertes conséquentes pour le ministère.

- **Environnementaux** : avec une échelle allant de l'impact mineur pour une ressource naturelle aux pertes irrémédiables pour une ressource naturelle au niveau zonal.

- **Image** : avec une échelle allant d'une simple plainte d'un usager à des campagnes médiatiques nationales.

- **Vie des personnes** : avec une échelle allant de l'inconfort pour une personne à un accident grave ou décès de personnes.

- **Règlementaires ou juridiques** : avec une échelle allant d'une sanction interne au ministère à une condamnation pénale d'un agent ou du ministère.

- **Désorganisation** (externe ou interne) : avec une échelle allant d'une adaptation limitée à une mobilisation importante de moyen ou ressources supplémentaires.

Conseil : *A l'issue de cette étape, vous pouvez établir une fiche par mission à exigence de disponibilité élevée faisant apparaître les différents éléments collectés. Cette fiche vous sera utile dans la section suivante d'analyse des risques. Un exemple de fiche vous est proposé en annexe 4.*

f) Etude des risques

Une fois l'ensemble des missions à exigence de disponibilité élevée définies la suite de la démarche consiste à effectuer l'analyse des risques pesant sur le service et impactant les missions sélectionnées. Il est proposé ici une méthodologie **d'analyse de risques simplifiée**.

Si vous souhaitez avoir une approche plus approfondie de l'analyse des risques, vous pouvez vous référer au guide méthodologique du SGDSN, ou encore à la méthodologie EBIOS RM, dont les références sont en fin de document.

Le principe de cette version simplifiée d'analyse des risques est de sérier les menaces disponibles dans la base de données des menaces (disponible en annexe 5) et d'identifier au moins une mission à exigence de disponibilité élevée qui serait impactée par l'occurrence de cette menace pour pouvoir la sélectionner dans la suite du processus.

Il est bien entendu que les menaces qui ont été exclues du périmètre de la réalisation du PCA/PRA Cyber en introduction de la démarche (lors de la définition du contexte et périmètre) ne doivent pas être analysées à ce stade.

Comme la base de données des menaces le présente, chaque entrée dispose d'un certain nombre de précisions utiles pour cette analyse, nous les détaillons ici :

- **Type** : c'est la famille de menace à laquelle appartient la menace unitaire. Cette famille permet de savoir si l'analyse doit être réalisée ou non en adéquation avec les choix préliminaires qui ont été faits lors de la définition du contexte et périmètre.

- **ID** : identifiant de la menace, ceci est un artifice de notation afin de rendre plus aisé la manipulation de la menace dans l'analyse plutôt que d'utiliser sa description ou son titre.

- **Menace** : titre synthétique de la menace, il s'agit ici de nommer de manière concise la menace.

- **Commentaires** : dans cette colonne une explication de la menace est dispensée, pour certaines menaces l'explication est sommaire, pour d'autres elle est plus complète afin de bien saisir l'objet de celle-ci.

- **Conséquences** possibles : dans cette colonne des explications non exhaustives sont apportées pour aider à identifier les répercussions possibles sur la disponibilité de chacune des menaces. Il est alors plus aisé de la retenir ou non.

- **Portée** : Les colonnes de portée indiquent à quelle typologie de ressources la menace peut s'appliquer, cela aide à identifier l'adéquation de la menace avec les ressources nécessaires à la mission à exigence de disponibilité élevée en cours d'analyse.

- **Délibérée** : cette dernière colonne indique si cette menace peut être réalisée de manière délibérée. Lorsque c'est le cas, et si le choix de considérer la menace interne a été retenu lors des décisions préliminaires, la vraisemblance de ladite menace doit être majorée.

Dans le cas où la menace en cours d'analyse s'applique à l'une des missions à exigence de disponibilité élevée définies au paragraphe précédent, il faut la retenir et ensuite il est nécessaire d'en mesurer la vraisemblance (ou la plausibilité).

La vraisemblance d'une menace est affaire d'expert ! Vous devez vous appuyer sur les experts de chaque typologie de menace pour cette mesure.

Vous trouverez en annexe une échelle de mesure de la vraisemblance afin de vous guider dans la numération de cet indicateur. Par ailleurs, comme il est spécifié sur la note précédente, la vraisemblance est une affaire d'expert. Cela équivaut à dire que pour chaque typologie de menace, c'est l'expert du domaine qui est en mesure de définir la juste numération de la vraisemblance grâce à l'échelle proposée.

Il est évident que le spécialiste du système d'information n'est le mieux à même de définir une vraisemblance viable lorsque l'étude porte sur les menaces naturelles, humaines ou encore légales. Chaque domaine doit être évalué par des personnes concernées et aguerries au sujet évoqué.

L'harmonisation globale de ces estimations n'est pas chose aisée, certains domaines disposant de statistiques très précises sur l'avènement d'une menace lorsque d'autres n'en sont pas encore à cette mathématisation. L'échelle de vraisemblance est suffisamment « linguistique » (et non mathématique) pour aider à cette harmonisation, chaque expert ayant la capacité de traduire dans son périmètre l'attendu pour le PCA/PRA Cyber.

A ce stade le document « PCA/PRA Global », référencé [DOC.04] ; ou encore le document « Plan de prévention aux risques naturels et technologiques », référencé [DOC.05], ou encore le document

« Analyses de risques », référencé [DOC.06] peuvent être des aides au choix et à la mesure de plausibilité des menaces.

> ***Conseil :*** Dans une première version du PCA/PRA Cyber, il est conseillé de se contenter de retenir les menaces de plausibilité 3 ou 4 pour des missions à exigence de disponibilité élevée de DMIA 3 ou 4. En effet, les risques les plus critiques sont à traiter en priorité, les autres risques peuvent être abordés dans une seconde phase, par exemple lors de l'amélioration continue du document.

A l'issue de cette étape une liste de risques est donc obtenue, où une menace fortement plausible pèse sur au moins une mission fortement critique. Cette liste servira dans le paragraphe suivant pour établir la liste des scénarios de continuité retenus.

Essayons sur un exemple fictif !

Pour mieux comprendre cette partie d'analyse de risques, prenons un exemple, l'identification des missions à exigences de disponibilité élevées a été établie et a fourni les deux missions fictives ci-dessous (que nous nommerons « Mission A » et « Mission B » pour l'exemple), voici les fiches missions « simplifiées » de ces deux missions.

Nom de la mission	Mission A			
Description	Mission de réalisation d'actions régulières avec un outil métier			
Interfaces entrantes	Données en provenance d'un autre système			
Interfaces sortantes	Mise à disposition sur une plateforme nationale du résultat de l'action			
Ressources				
Humaines	Compétences redondées (non critique, non dépendance)			
Matérielles	Un ordinateur particulier est nécessaire (critique, non dépendance)			
Infrastructure	Réseau (critique, dépendance)			
Applicatives	Outil métier accessible via un navigateur (critique, dépendance)			
Informationnelles	Données entrantes (critique, dépendance)			
Bâtiments	N/A			
DMIA				4
PDMA			3	
Modes dégradés possibles				
Réalisation de l'action depuis un autre site tant qu'une connexion réseau et un accès VPN sont disponibles. Pas d'alternative à l'outil métier !				

Nom de la mission	Mission B			
Description	Mission de surveillance de l'état d'une ressource			
Interfaces entrantes	Aucune			
Interfaces sortantes	Aucune			
Ressources				
Humaines	Compétences unique (critique, non dépendance)			
Matérielles	Un ordinateur standard (non critique, non dépendance)			
Infrastructure	Réseau (critique, dépendance)			
Applicatives	Outil métier de surveillance accessible via un navigateur (critique, dépendance)			
Informationnelles	N/A			
Bâtiments	N/A			
DMIA			3	
PDMA				
Modes dégradés possibles				
Réalisation de l'action depuis n'importe quel média disposant d'une connexion réseau et d'un VPN				

Pour faciliter l'exercice il a été décidé au niveau de la définition du contexte et du périmètre de ne retenir que les menaces de types Cyber, on utilise donc uniquement la section « Attaques Cyber » de la base de connaissances des menaces. ! Bien entendu ce choix restreint doit être écrit dans le document final et si possible justifié !

La première des menaces de la base dans cette section est le « Piégeage de matériel », qui est défini comme suit :

Type	ID	Menace	Conséquences possibles	Commentaires	Portée (HMRAIB[1])
Attaque Cyber	ATT.01	Piégeage de matériel	Matériel inutilisable ou en baisse de capacité	Le piégeage est initialement utilisé pour accéder à l'information ou pour exploiter une vulnérabilité dans le but de s'introduire dans le SI, cependant il peut également engendrer une baisse ou une perte de disponibilité de l'usage du bien.	MR

Dans cet exercice, la vraisemblance de cette menace est évaluée à **3**, notamment du fait que la menace est jugée courante (à l'issue de l'analyse des différentes sources à son sujet[2]), mais amoindrie par le fait que le service (de l'exercice) dispose de moyens de protection à son encontre, et que le personnel est sensibilisé aux bonnes pratiques en termes de cybersécurité.

Ici il s'agit d'un cas fictif, représentant cependant le cheminement de pensée devant amener à l'évaluation de la menace et la justification de cette cotation.

Nous constatons que cette menace pèse sur les éléments ressources de types Matériels ou Infrastructures.

En croisant ces informations avec la fiche de la Mission A, nous établissons que nous devons retenir cette menace car la Mission A (de niveau de DMIA de **4**) dispose de ressources Matérielles critiques.

Nous retenons donc le risque suivant pour la suite de nos travaux :

« **Piégeage de matériel entrainant l'indisponibilité d'une ressource critique (ordinateur) à la réalisation d'une mission à exigence de disponibilité élevée** »

[1] Portée HMRAID correspond aux portées sur les types de ressources **H**umaines, **M**atérielles, inf**R**astructures, **A**pplicatives, **I**nformationnelles et **B**âtiments.

[2] Par exemple, conférence de l'ANSSI sur le sujet : www.ssi.gouv.fr/agence/publication/quelle-confiance-dans-les-composants-materiels/

Comme la menace a été retenue sur la Mission A il n'est pas nécessaire de poursuivre son analyse sur les autres missions. Nous pouvons donc continuer avec les autres menaces de la section en suivant le même procédé. Nous classons ensuite les risques retenus suivant la hiérarchie suivante :

- En premier lieu, les risques issus d'une vraisemblance à 4 et portant sur une mission dont la DMIA est également à 4
- En second lieu, les autres risques (3,4) ou (4,3)

Un brin de patience et de la rigueur permettent de venir à bout de cette étape de manière sûre.

Astuce : *Lorsque la menace s'applique de manière différente en fonction d'un critère non spécifié dans la mission (par exemple pour une mission réalisée sur plusieurs sites, une menace de type naturelle peut avoir une vraisemblance non similaire en fonction du site) prenez en compte « le pire » scénario pour faire votre analyse.*
Vous pourrez ensuite restreindre la réponse à apporter en fonction du site.
Si le risque est probant, il ne faut pas le laisser passer !

g) Traitement des scénarios de risques retenus

A ce stade une **liste** composée d'un certain nombre de **risques classés** par criticité est établie.

Il convient donc désormais de sélectionner tout ou partie de cette liste pour élaborer la stratégie et les scénarios de continuité.

> ***Conseil :*** *ne pas sélectionner une trop grande quantité de risques lors de la première élaboration du PCA/PRA Cyber. Une liste courte avec des sujets bien maîtrisés sera plus utile qu'une liste très exhaustive faite sans approfondissement.*

Avant de poursuivre sur la stratégie de continuité, il est utile à ce stade de mener une réflexion sur les traitements possibles des risques identifiés. L'objectif ici étant d'identifier les mesures qui peuvent être initialisées et qui permettront d'amoindrir l'impact ou la vraisemblance du risque.

Les traitements possibles sont de plusieurs natures :

- **Terminer le risque** : cela consiste à avoir une action qui élimine le risque par l'absence d'une de ses composantes. Terminer un risque est un des traitements les plus complexe à mettre en œuvre généralement.

  Exemple : s'il est identifié un risque d'incendie dans une salle serveur, une façon de terminer le risque est de migrer le service offert dans le cloud. Attention, dans le cas de cet exemple, le risque est terminé certes, mais d'autres risques peuvent apparaître, du fait du cloud, qui n'existaient pas préalablement, et qu'il faudra donc analyser.

- **Traiter le risque** : cela consiste à considérer le risque comme accepté à condition de diminuer une de ses composantes. On peut par exemple jouer sur la vraisemblance de la menace, ou bien encore sur la gravité des impacts, ou encore sur les deux. Le risque existe toujours à l'issue, mais sa criticité est moindre, il a été traité !

  Exemple : toujours avec le risque d'incendie dans une salle serveur, une façon de traiter le risque sur le plan de la vraisemblance d'occurrence est d'équiper la salle serveur de détecteurs de fumées. La façon de traiter le risque sur le plan de la gravité de l'impact est d'équiper la salle serveur d'extincteur.

- **Transférer le risque** : cela consiste à faire porter le risque par un tiers. C'est ce que l'on fait en prenant une assurance. Le risque financier consécutif à un risque physique est absorbé en tout ou partie par l'assureur. On a transféré le risque de perte financière.

- **Tolérer le risque** : c'est le traitement le plus simple, puisqu'il consiste à accepter le risque en l'état et à ne rien faire de plus que ce qui est déjà en place. Dans le cas de traitement du risque par amoindrissement de la vraisemblance et/ou de l'impact, le risque résiduel résultant est considéré comme toléré.

Comment trouver des mesures de traitement, par amoindrissement de la vraisemblance ou de l'impact, pour chacun des risques ?

Pour chacune des typologies de risques, de la même manière que l'évaluation de la vraisemblance est une affaire d'expert, et qu'il vous a fallu faire appel aux experts desdits domaines pour la mesurer, vous devez faire **appels** à ces **experts** pour vous aider à **identifier des mesures de gestion des risques**.

En ce qui concerne les risques Cyber en particulier, la littérature en la matière est prolifique, l'ANSSI dispose de multiples guides pour vous aiguiller sur les bonnes pratiques à mettre en œuvre pour tel ou tel domaine, bon nombre de grands éditeurs du monde Cyber en fournissent également. Chacune de ces bonnes pratiques a pour effet de traiter partiellement certains risques.

Par exemple, la préconisation de mise en place d'une authentification à double facteur, a pour effet de traiter en partie le risque d'usurpation d'identité (risque qui n'apparaît pas dans un PCA/PRA Cyber car n'entraîne aucune rupture de disponibilité). Cependant ce risque augmente la vraisemblance de tous les risques nécessitant un accès au SI.

De la même manière, la préconisation de mise en place de solutions antivirales, régulièrement misent à jour, a pour effet de traiter en partie le risque de piégeage logiciel.

Il existe un certain nombre de guide thématiques disponibles sur Internet permettant d'identifier les mesures préconisées pour traiter partiellement le risque.

Le Pôle Ministériel dispose d'infrastructures informatiques nationales comportant d'importants mécanismes de sécurité et propose une offre de services sur le déploiement des infrastructures locales des services déconcentrés (antivirus, pare-feu, chiffrement des postes nomades, …). Cette politique technique évolue régulièrement au vu de l'état des menaces.

h) Stratégie de continuité

La stratégie de continuité vise à déterminer la manière dont l'occurrence des risques sera traitée. La définition d'une stratégie à un niveau global (quel que soit le risque) est nécessaire, mais il convient également de décliner cette stratégie à chacun des risques retenus pour assumer leurs spécificités.

Quels sont les points sur lesquels il convient de mener une réflexion et d'apporter un choix concernant la stratégie de continuité ?

- Le premier point consiste à positionner le curseur entre le dédoublement de toutes les ressources afin de ne subir aucune perte de continuité en cas de crise et l'acquisition et la reconstruction de l'ensemble des ressources impactées par la crise au moment de celle-ci. Il s'agit principalement d'un positionnement financier, mais pas uniquement ; des conséquences humaines et procédurales sont également à prendre en compte.

  Il est bien entendu que majoritairement c'est un « **juste milieu** » qui sera sélectionné, il doit donc s'agir ici de déterminer ce juste milieu. L'identification de ce point sera cruciale dans l'édification de la gestion de la crise.

> ***Conseil :*** *Le choix d'avoir des ressources « de rechange » pour les ressources critiques des missions à exigence de disponibilité élevée semble un choix de « juste milieu », minimisant à la fois l'impact financier d'une telle solution et également l'impact sur le temps de recouvrement à la suite d'une crise.*

- Le deuxième point consiste à définir le **niveau de mode dégradé** qu'il convient d'atteindre. Est-ce que le choix est mis sur un recouvrement rapide avec un mode dégradé sommaire, ou bien sur un recouvrement en deux étapes en passant par un mode dégradé plus construit.

  De la même manière, le choix ici est à réfléchir selon plusieurs angles. Tout d'abord l'aspect financier du problème, puisque le mode dégradé du type « crayon-papier » à un impact bien moindre en termes de coût qu'une solution de type « serveur de secours ». Ensuite sur l'aspect facilité de mise en œuvre par la gestion de crise. Le critère de maintenabilité de la mission est également indispensable à prendre en compte dans ce choix. Et enfin le dernier critère concerne la récupérabilité des données générées pendant le mode dégradé.

- Le troisième point introduit la notion **d'ordonnancement** lors du traitement du risque. Dans le cas d'un risque majeur ayant un impact global et conséquent sur un service, les équipes en charges de gérer la crise ne seront sûrement pas en mesure de remonter l'ensemble des ressources impactées

de manière immédiate et simultanée. Il y aura des choix de précédence à faire.

Le premier critère de choix est bien sûr la criticité des missions impactées, mais cela n'est peut-être pas suffisant, la charge peut être telle qu'un second niveau de priorité doit être proposé. Cette priorisation ne peut être décidée durant la crise par l'équipe projet en charge de régler la crise. C'est pourquoi elle doit être réfléchie également en amont.

Conseil : *Une façon de traiter ce point peut être d'établir à l'avance une liste des postes critiques à remonter en ayant plusieurs niveaux de lecture.*

<u>Premier niveau</u>, seul un service est impacté, les postes du service sont alors remontés dans l'ordre décrit.

<u>Second niveau</u>, plusieurs services sont impactés, les postes sont alors remontés dans un ordre globalisé. L'astuce du « s'il n'y en avait qu'un à remonter » peut s'avérer utile pour établir cet ordre globalisé.

- Le quatrième point est l'aide au traitement du risque que l'on souhaite avoir au moment de la crise. Il peut être décidé de se contenter des grands axes de continuité qui ont été réfléchis globalement ci-dessus. Il se peut également qu'un choix plus pragmatique soit souhaité, avoir pour chacun des risques une « **fiche réflexe** » permettant de guider la réaction à avoir lors de la crise, couvrant chacun des temps de la crise : les actions d'urgences pour minimiser l'impact et l'envergure, les actions de déploiement du mode dégradé, les actions de remonter au mode nominal et les actions de récupération des données.

  Dans le cas d'un choix d'outil de type « fiche réflexe », il est nécessaire de travailler sur ces documents au moment de la réflexion du PCA/PRA Cyber. Il est bien entendu qu'il faille travailler sur la forme du document pour qu'il rejoigne la volonté de pragmatisme souhaitée, mais également sur le fond afin que le document soit utile au juste niveau lors de la crise.

Un exemple de fiche réflexe est disponible en Annexe 6

i) Gestion de la crise

L'organisation de la gestion de crise doit se faire autant que possible en s'adossant aux principes en vigueur au sein du service, notamment si le service dispose déjà d'une organisation de gestion de

crise. Il ne conviendra dans un tel cas que d'adjoindre les particularités d'une crise aux éléments déjà existants.

Il est donc défini ici une **aide à la gestion de la crise** dans le cas où aucun dispositif existant n'est disponible au sein du service.

Déclenchement de la crise

Le premier point à réfléchir et organiser est la partie constituant le **déclenchement de la crise**. Quels sont les vecteurs de détection, d'alerte et de qualification d'un incident ?

Lorsque l'incident survient en interne au sein du service, il faut mettre en place une culture de la remontée d'information aux bonnes personnes. Pour cela, les personnes destinataires doivent être identifiées et communiquées en amont des crises.

Conseil : *Pour tout incident de type cyber (mail étrange, comportement étrange d'un matériel, extinction, inaccessibilité, …) il peut être prévu une boîte mél spécifique afin de pouvoir rendre compte. Il doit bien entendu être prévu une alternative en cas de perturbation de l'accès au système de mél.*

Cellule de crise

Le deuxième point à organiser concerne la **cellule de crise**. Il s'agit d'un organe exceptionnel déclenché par l'alerte à la suite d'incident permettant d'agir pour résoudre la crise. Cette cellule doit au minimum être composée de personnes pouvant endosser les rôles suivants :

- **Décision** : il faut que la cellule de crise soit dotée d'au moins une personne en capacité de décider. C'est-à-dire ayant les pouvoirs suffisants pour prendre des décisions urgentes sans avoir à faire valider préalablement sa décision. Le périmètre de ces décisions est bien entendu dépendant de la crise.

- **Analyse** : il faut que la cellule de crise soit dotée d'au moins une personne en capacité d'analyser les informations en provenance du terrain afin de comprendre les phénomènes à l'œuvre, mais également d'anticiper les scénarii d'évolution possibles. Il peut être perspicace, si le service dispose de suffisamment de ressources humaines en la matière, de séparer le rôle d'analyse (qui permet de comprendre pour agir) du rôle d'anticipation (qui permet de prévoir pour agir mieux)

- **Communication** : il faut que la cellule de crise soit dotée d'au moins une personne en charge de la communication de crise. Cette communication doit être envisagée vers l'interne (les agents du service), pour informer de la

situation, de la connaissance actuelle de l'incident et de son état, des temps prévisibles de recouvrement et de toute avancée de la situation. La communication doit également être envisagée vers l'externe, notamment dans le cas où des usagers sont impactés par l'incident, mais aussi envers les instances nécessaires auxquelles il faut rendre compte.

- **Traçage** : il faut que la cellule de crise soit dotée d'au moins une personne en charge de noter l'intégralité des décisions prises, des actions engagées, des informations obtenues, des communications faites. Ce verbatim chronologique a pour objectif de pouvoir faire un retour d'expérience de la gestion de la crise et de permettre une amélioration de celle-ci.

Conseil : *Il peut être utile de décliner la cellule de crise en plusieurs niveaux, plus ou moins dotés en personnels, afin de n'avoir que le strict nécessaire à la gestion de la crise en fonction de sa gravité.*

Dans cette cellule de crise, sont conviés également des personnes ayant un des rôles définis ci-dessus :

- Le ou les **responsables métiers** des missions impactées par la crise,
- Le ou les **responsables des sites** impactés par la crise,
- Le correspondant **Délégué à la Protection des Données** lorsque des données sont impactées par la crise,
- Le ou les représentants des **prestataires** concernés par la crise.

*Il est fortement recommandé de désigner un **correspondant unique** entre la cellule de crise et les équipes techniques en charge du rétablissement. Ce correspondant devra être le seul à pouvoir communiquer avec les équipes, autant pour donner les consignes issues de la cellule de crise, que pour remonter les informations issues de ces équipes.*
*Cette équipe agissant pour le rétablissement au plus vite du système doit être autant que possible « **mise sous bulle** » pour qu'elle ne subisse pas d'interruption parasite inutile à ce stade. Notamment de personnels la sollicitant pour des problématiques anecdotiques ou tout simplement pour « s'informer » sur le temps avant recouvrement.*

Moyens de crise

Le troisième point à organiser et à prévoir concerne les moyens nécessaires à la bonne gestion de la crise. Il convient ici de lister, notamment afin que cela soit vérifié régulièrement, l'ensemble des « outils » qui seront nécessaires à la bonne gestion de crise.

Sans que cette liste soit exhaustive, vous trouverez ci-dessous une aide à l'édification d'une telle liste de moyens de crise :

- Salle de crise physique (dont la couverture GSM est suffisante pour l'ensemble du personnel présent en cellule de crise)
- Salle de crise de repli (en cas d'impact sur la salle primaire)
- Salle de crise virtuelle (en cas de nécessité de type pandémie ou indisponibilité totale d'un site)
- Annuaire de crise (avoir une version imprimée de cet annuaire en cas d'indisponibilité totale du SI)
- Main courante (Utilisé par la personne en charge du traçage des événements)
- Outils de communication résilients (gsm, messagerie alternative, tchat alternatif, visioconférence alternative, …)
- Fiches rôles et fiches réflexes (si ces documents ont été réfléchis préalablement, ils peuvent être utile pour soutenir l'action des différents intervenants de la cellule de crise)
- Chronologie d'une gestion de crise (si ce document a été réfléchi préalablement, il peut être utile pour ne rien oublier dans l'avancement de la résolution de crise)
- Cartographie des SI (permet d'aider à l'anticipation de la crise, ainsi que d'aider aux décisions éventuelles d'isolement pour non-contagion)
- Liste de parties prenantes à informer (usagers, fournisseurs, services, autorités)
- Registre des traitements de données à caractère personnel
- Moyens électriques suffisants (en fonction de la durée de la crise, les personnes présentes en cellule de crise auront besoin de charger leur GSM, ordinateur portable, …, il faut le bon nombre de prise et que la charge soit tenable par le réseau électrique)
- Ecran de projection dans la salle de crise (pour faciliter le partage d'information au sein de la cellule de crise)
- Tableau blanc et moyens d'écriture fonctionnels adéquats
- Ordinateur portable de secours

- Véhicule à disposition de la cellule de crise (notamment dans le cas où le service est sur plusieurs sites)

- Moyens d'accès au réseau alternatif (par exemple connexion cellulaire activable, dans le cas d'une coupure d'accès au réseau du service)

- Des bouteilles d'eau et des repas chauds (on ne peut pas se nourrir que de sandwich lorsque la crise dure)

06. Faire vivre le PCA/PRA Cyber

a) S'entraîner et vérifier régulièrement

Une fois le PCA réalisé il est nécessaire d'en vérifier l'efficacité. Pour ce faire il est possible d'approcher cette étape selon plusieurs méthodes complémentaires.

Le document peut être vérifié par un tiers de confiance, pour ce faire le service peut s'appuyer par exemple sur un CMSI du ministère. La conception puis le ré examen régulier du PCA/PRA Cyber peuvent être conduits avec l'appui des Conseillers en Management des Systèmes d'Information (SNUM/UNI/DRC) et en lien avec le Département Sécurité Gestion de Crise (SNUM/DSGC).

Par ailleurs, certaines parties du plan, notamment certaines parties très techniques peuvent être testées pour valider de leur bon fonctionnement et de l'estimation de durée. Par exemple : reconstruction d'un ordinateur pour un agent à partir d'un poste vierge.

Conseil : *Si des fiches réflexes ont été rédigées, il peut être utile pour l'objectif ici présenté, de réaliser une relecture régulière de celles-ci (par exemple tous les trimestres) par l'ensemble des parties prenantes d'une crise. L'objectif n'étant pas ici de les amender, mais juste de les connaître et de ne pas les découvrir en cas d'incident !*

De plus le document doit être vérifié par des exercices, planifiés ou imprévus, qui proposeront de valider telle ou telle partie du PCA/PRA Cyber, en effectuant un focus sur un incident en particulier. L'exercice « PIRANET » est un exemple de vérification par l'exercice du PCA/PRA Cyber.

Enfin, il doit également être vérifié régulièrement que les prérequis nécessaires à la bonne gestion de la crise soient disponibles et opérationnels.

L'objectif étant de vérifier l'intégralité du caractère opérationnel du document sur une période donnée (par exemple 5 ans), afin que l'ensemble des parties prenantes dont l'objectif est de résoudre une crise, soient préparées et aient connaissance des actions à engager avant la survenance de l'incident.

Conseil : *Dans le cas où les crises ont été quantifiées en niveaux de criticité, il peut être intéressant de prévoir un planning où les crises plus critiques (et donc*

plus complexes à tester) soient réparties sur une durée plus longue, et celles plus simples sur une périodicité plus courte.

b) Maintenir à jour

Maintenir à jour le document est tout aussi important que de s'entraîner aux risques identifiés. Une périodicité de mise à jour doit être définie afin que soient réalisées régulièrement plusieurs actions importantes :

Une relecture de l'ensemble du document, avec une fréquence élevée, par exemple annuelle, afin qu'à la fois le processus d'élaboration mais aussi les conclusions soient intégrées par les personnes concernées.

Une revue de l'ensemble du document, avec une fréquence plus faible, par exemple triennale, afin de prendre en compte les évolutions nécessaires issues soit du service lui-même, d'une éventuelle réorganisation de ses missions ou de ses moyens, d'un changement de l'architecture du SI, ou bien de l'apparition (ou disparition) de menaces dans le champ d'investigation du PCA/PRA Cyber.

L'ensemble des actions de maintien du document et des capacités d'actions sont à intégrer dans un planning globalisé. Principalement pour qu'elles ne se superposent pas de trop et provoquent une surcharge de travail sur le document sous plusieurs axes simultanés.

Conseil : *Il est conseillé de positionner sur un plan pluriannuel, par exemple quinquennal, l'ensemble des actions d'exercice et de maintien à jour de manière équitablement réparties. Ce planning pourra être diffusé aux personnes concernées.*

07. Addenda

a) Pour aller plus loin…

Au-delà des éléments exposés dans ce guide, il peut être souhaité de disposer d'une méthode plus détaillée afin d'élaborer le PCA/PRA de l'organisation, ou bien pour avoir une approche de l'analyse des risques plus précise et outillée.

A cette fin, trois documents en particulier peuvent être utiles :

- Pour l'élaboration du PCA/PRA, à un premier niveau, opérationnel et pratique, le « Guide pour réaliser un plan de continuité d'activité » publié par le SGDSN [Réf. n°1] propose une démarche exhaustive, détaillée dans des fiches pratiques très complètes ;

- Toujours pour l'élaboration du PCA/PRA, à un second niveau, beaucoup plus formel, la norme ISO 22301 « Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences » [Réf. n°4] définit la démarche et l'organisation nécessaire à la gestion maîtrisée et à l'amélioration continue de la continuité d'activité.

- Enfin pour une analyse de risque plus riche et plus outillée, la méthodologie EBIOS RM permettra d'avoir une approche plus fine. La méthode EBIOS RM est LA méthode d'appréciation des risques publiée par l'ANSSI, avec le soutien du Club EBIOS. « La méthode EBIOS Risk Manager – Le Guide) [Réf. n°8]

Il convient de noter que les deux premiers documents traitent de la gestion de la continuité au sens large, et ne sont pas focalisés sur les aspects propres au Système d'Information. Les éléments qu'ils proposent restent néanmoins valides et peuvent également être utilisés pour le plan de continuité global de la structure.

Par ailleurs, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) propose trois documents complémentaires et plus focalisés afin d'aider à la mise en place d'exercices de crises Cyber. Comme il a été évoqué dans ce document, l'exercice est nécessaire à l'élaboration d'un PCA/PRA Cyber en adéquation avec le réel au sein du service déconcentré (SD), mais aussi nécessaire à « l'entrainement des troupes » afin de faire face au mieux lors d'une crise réelle.

- Le premier d'entre eux, « Crise d'origine Cyber, les clés d'une gestion opérationnelle et stratégique » publié par l'ANSSI [Réf. n°5], par le retour d'expérience de grands acteurs français donne des éléments permettant une organisation efficace d'une crise cyber. Ce guide vient en soutien des éléments qui ont été évoqués au sein du présent document ;

- Le second, « Organiser un exercice de gestion de crise Cyber » publié par l'ANSSI [Réf. n°6], approfondi la notion d'exercice de crise Cyber qui a été brièvement abordée dans le présent document. Il offre un cadre

méthodologique, ainsi que des exemples afin d'aider à la construction de ses exercices nécessaires ;

- Le dernier, « Anticiper et gérer sa communication de crise Cyber » également publié par l'ANSSI [Réf. n°7], propose quant à lui de soutenir la démarche de communication lors d'une crise cyber. La partie communication a également été brièvement abordée dans ce document, mais mérite tout autant une préparation minutieuse.

b) Glossaire

- **DMIA** : Durée Maximale d'Interruption Acceptable
- **PCA** : Plan de Continuité d'Activité
- **PCI** : Plan de Continuité Informatique
- **PDMA** : Perte Maximale de Données Admise
- **PRA** : Plan de Reprise d'Activité
- **PRI** : Plan de Reprise Informatique
- **SI** : Système d'Information
- **SSI** : Sécurité des Systèmes d'Information

c) Documents de référence

1. Guide pour réaliser un plan de continuité d'activité (2013 - SGDSN) [http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf]
2. Référentiel de bonnes pratiques : Plan de continuité d'activité (2011 - AFNOR BG Z 74-700) [https://www.boutique.afnor.org/fr-fr/norme/bp-z74700/plan-de-continuite-dactivite-pca/fa172269/1137]
3. Lexique structuré de la continuité d'activité (2012 – Club de la Continuité d'Activité) [https://www.clubpca.eu/document/view/7647966b7343c29048673252e490f736]
4. Continuité des activités – ISO 22301 (2012 – Organisation Internationale de Normalisation) [https://www.iso.org/fr/news/2012/06/Ref1602.html]
5. Crise d'origine Cyber, les clés d'une gestion opérationnelle et stratégique (2021 – ANSSI) [https://www.ssi.gouv.fr/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-strategique/]

6. Organiser un exercice de gestion de crise Cyber (2021 – ANSSI) [https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/]

7. Anticiper et gérer sa communication de crise Cyber (2021 – ANSSI) [https://www.ssi.gouv.fr/guide/anticiper-et-gerer-sa-communication-de-crise-cyber/]

8. La méthode EBIOS Risk Manager – Le guide (2018 – ANSSI) [https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/]

Annexe 1 – Plan type du PCA/PRA Cyber

Il vous est proposé ci-après un modèle de document résultant (PCA/PRA Cyber). Ce modèle n'est clairement pas le seul possible, vous pouvez également vous appuyer sur celui existant en interne au niveau du service, par exemple celui qui a été utilisé pour la rédaction du PCA/PRA Global.

I) Introduction
Chapitre introductif du document

II) Contexte
II.1) Périmètres
Chapitre définissant les périmètres retenus : géographique, fonctionnel, technique. Les contextes internes et externes sont également décrits.

II.2) Missions et métiers
Chapitre listant les missions et métiers qui ont été retenus pour l'objet du document.

II.3) Organisation et Infrastructure du SI
Chapitre décrivant à grandes mailles l'architecture du (ou des) SI retenus pour le présent document.

III) Continuité
III.1) Activités essentielles
Chapitre décrivant les activités essentielles permettant de réaliser les missions et métiers.

III.2) Ressources critiques
Chapitre décrivant les ressources identifiées comme essentielles à la réalisation des activités.

IV) Analyse de risques
IV.1) Menaces principales
Chapitre listant les menaces principales qui ont été retenues (parmi celles qui ont été retenues, on ne liste ici que celles ayant une vraisemblance supérieure ou égale à 3)

IV.2) Scénarios principaux
Chapitre listant les scénarios de risques principaux retenus à l'issue de l'analyse de risque.

V) Principes de continuité
Chapitre listant les choix principaux dictant la gestion de la continuité. On décrit d'abord les choix qui ont été fait de manière globale, puis une déclinaison par risque peut être réalisée à la suite, ou en annexe.

VI) Gestion de la crise
Chapitre décrivant la gestion réfléchie d'une crise. On précise le comment du déclenchement de la cellule de crise, la constitution de ladite cellule (en déclinant les rôles prévus).
Ce chapitre liste également les moyens nécessaires à la bonne gestion d'une crise, ainsi que la chronologie de la crise et les différents jalons la constituant.

VII) Maintien en condition opérationnelle

Chapitre décrivant les dispositions prises pour entretenir le document, réaliser les différents exercices d'entrainement à la crise.

VIII) Annexes

En annexe il est utile de rappeler : l'ensemble des fiches réflexes (si le choix à été fait d'en réaliser), la liste des biens supports retenus pour l'analyse de risque avec l'évaluation des impacts, la liste des menaces évaluées pour l'analyse de risque avec leur vraisemblance, éventuellement la liste des risques non retenus en première rédaction pour amélioration future.

IX) Annuaire

Ce dernier chapitre, qui lui-même est une annexe, liste l'ensemble des personnes utiles à la gestion de la crise ainsi que les moyens de les contacter.

Annexe 2 – Aide à l'identification des dépendances

Les listes proposées ci-dessous **n'ont pas pour objectif d'être exhaustives**, elles sont définies ci-dessous pour vous soutenir dans la démarche d'identification de vos dépendances.

Périmètre – Services Centraux	Dépendance identifiée
SI Financier (Chorus, Chorus formulaire, …)	SG/DAF/CIF3
Messagerie, Active Directory, GPO, Poste de Travail, Serveur EOLE, NextCloud, RIE	SNUM/UNI/DETN
Odyssée, Agora, SA2P, PCAET,	DGEC/SD7
TIPI, SAGT, SAGACITE, ISIDOR	DGITM
Immatriculation des navires, Permis, Titre aux marins, …	DGITM/DAM
Prévention risques (technologiques, sanitaires et naturels)	DGPR/DAGSI
SI RH (Renoirh, Rgprime, …)	DRH
Cerbere, VPN, Chiffrement, IGC/CAE, Antivirus	SNUM/DSGC
Opérateur de télécommunication	RIE
Services de partage de fichiers	Osmose, France Transfert, …
Solution de communication (visio-conférence, messagerie instantanée, …)	Webconf, Tchap

Périmètre – Divers	Dépendance identifiée
Locataire d'un bâtiment	Bailleur
Flotte de téléphone cellulaires	Opérateur téléphonique
Alimentation électrique	Fournisseur d'énergie
Chauffage	Fournisseur d'énergie
Flotte de véhicule en location	Loueur
Flotte de véhicule	Fournisseur de carburant
Opérateurs de télécommunication	Privé

Annexe 3 – Listes de missions à exigence de disponibilité élevée

Cette liste n'est pas figée !

DREAL / DEAL

4	La vigilance hydrologique
	La prévention des risques anthropiques
3	Le registre de contrôle des véhicules routiers
	Energies air éolien
	Changement climatique
	Ouvrage hydraulique
	Paiement
	Médical

DIRM / DM

4	Sécurité maritime – gestion de la pollution maritime (POLMAR)
	Sécurité maritime – sauvetage en mer (SECMAR)
	Centre de sécurité des navires
3	Police des pêches
	Contrôle des ports
	Surveillance de la navigation
	Ressources Humaines
	Finance
	Délivrance des titres

DIR

4	Gestion des urgences et crises routières
	Gestion du trafic routier
3	Base de données de la gestion routière
	Viabilité hivernale
	Ressources Humaines
	Budget et Comptabilité
	Juridique

Annexe 4 – Exemple de fiche de synthèse d'un processus

Fiche de synthèse d'une Mission à exigence de disponibilité élevée

Nom de la mission :	
Nom du **responsable** :	

Description de la mission (incluant les enjeux et les contraintes de celui-ci) :

Description des **interfaces** et flux externes :

Liste des **activités** métier **rattachées** :

Les **ressources** associées (en précisant celles qui sont **C**ritiques, ainsi que les **D**épendances) :

	C	**D**
Humaines		
Matérielles		
Infrastructures		
Applicatives		
Informationnelles		
Bâtiments		

Les attentes en termes de continuité :

DMIA		**PDMA**	

Les **conséquences** d'une interruption de d'activité :

Principaux impacts Financiers, ou Environnementaux, ou d'Image, ou d'Atteinte à la vie des personnes, ou Réglementaires et légales ou de Désorganisation

Les **modes dégradés** possibles :

Annexe 5 – Base de connaissance des menaces

Type	ID	Menace	Conséquences possibles sur le fonctionnement du SI	Commentaires	Portée						Interne
					Humaine	Matérielle	Infrastructure	Applicative	Informationnelle	Bâtiment / Site	
Dommage Physique	PHY/01	Incendie	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable.		X	X	X			X	X
	PHY.02	Dégât des eaux	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable.	Inondation interne (rupture de canalisation / climatisation)		X	X			X	X
	PHY.03	Pollution	Inaccessibilité des locaux	Proximité d'un site Sevezo	X					X	
	PHY.04	Accident majeur	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable.	Accident routier	X	X	X			X	X
	PHY.05	Destruction de matériel	Matériel endommagé (baisse de capacité). Matériel inutilisable	Destruction volontaire ou involontaire par un humain d'un matériel		X	X				X
	PHY.06	Poussière / Corrosion	Matériel endommagé (baisse de capacité). Matériel inutilisable	Mauvais entretien / Absence de détection		X	X				X
Catastrophe naturelle	NAT.01	Chaleur / Froid exceptionnel	Matériel endommagé (baisse de capacité). Matériel inutilisable	Chaleur/froid excessive et au-delà des limites supportées par un équipement	X	X	X			X	
	NAT.02	Phénomène sismique	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable		X	X	X			X	
	NAT.03	Phénomène météorologique intense	Inaccessibilité des locaux.	Tempête / Neige / Grêle	X					X	
	NAT.04	Foudre	Matériel endommagé (Baisse de capacité). Matériel inutilisable.	En fonction de la proximité d'impact et de la présence de protection la gravité peut être conséquente	X	X	X			X	
	NAT.05	Inondation	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable	Inondation externe (montée des eaux fluviales, submersion en proximité de littoral, tsunami, rupture de barrage)	X	X	X			X	
	NAT.06	Phénomène volcanique	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable	En zone adéquate	X	X	X			X	
	NAT.07	Avalanche	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable	En zone adéquate	X	X	X			X	
	NAT.08	Glissement de terrain	Inaccessibilité des locaux. Matériel endommagé (baisse de capacité). Matériel inutilisable	En zone adéquate	X	X	X			X	
Services essentiels	ESS.01	Panne de climatisation	Matériel endommagé (baisse de capacité). Matériel inutilisable	Impact dépendant de la redondance éventuelle et de la durée d'interruption		X	X				X
	ESS.02	Panne d'électricité	Matériel momentanément inutilisable.	Impact dépendant de la redondance éventuelle, de moyen de secours (groupes électrogènes) et de la durée d'interruption		X	X				X
	ESS.03	Panne de chauffage		En fonction des condition climatiques, la gêne peut être impactante pour la continuité d'action des personnes	X						X
	ESS.04	Panne de réseau	L'accès aux applicatifs externe n'est plus possible, de même pour les données et les échanges	Il est question ici de la perte de connectivité réseau exogène au service. Cela ne concerne pas par exemple la rupture de connexion du fait d'une panne électrique ou encore de la défaillance d'un routeur.			X				

Type	ID	Menace	Conséquences possibles sur le fonctionnement du SI	Commentaires	Portée						
					Humaine	Matérielle	Infrastructure	Applicative	Informationnelle	Bâtiment / Site	Interne
Rayonnements	RAY.01	Electromagnétique	Matériel endommagé (baisse de capacité). Matériel inutilisable	EMP : spectrum.ieee.org/electromagnetic-warfare-is-here et www.industrie-techno.com/article/attaques-a-impulsions-electromagnetiques-les-reseaux-de-plus-en-plus-vulnerables.31955		X	X				X
	RAY.02	Thermique	Matériel endommagé (baisse de capacité). Matériel inutilisable	Une proximité trop grande avec des sources de chaleur forte à intense peut provoquer une usure prématurée du matériel voire sa défection.		X	X				X
Légal	LEG.01	Changement de législation	Peu rendre l'utilisation de certaines technologies impossible. Certains constructeurs peuvent devenir interdit d'usage. Certains logiciels devenir impossible d'utilisation d'un fait de la restriction législative.	Le changement législatif peut s'anticiper par une veille adéquate. Cependant, une fois la loi et le décret d'application promulgués, il n'est pas possible (sauf à contrevenir à la législation) de passer outre. Les délais sont cependant souvent accordés pour s'adapter (ex RGPD)		X	X	X	X		
Tiers	TIE.01	Fin de contrat avec un tiers	Perte d'usage immédiat des matériels/logiciels/services en cas de location. Perte de maintenance en cas d'achat.	La fin de contrat est anticipable		X	X	X	X	X	
	TIE.02	Rupture de contrat	Perte d'usage immédiat des matériels/logiciels/services en cas de location. Perte de maintenance en cas d'achat.	La rupture de contrat n'est pas anticipable si elle est à l'initiative du tiers. Des clauses légales de compensation sont possibles, mais l'indisponibilité engendrée est immédiate.		X	X	X	X	X	
	TIE.03	Disparition du tiers contractant	Perte d'usage immédiat des matériels/logiciels/services en cas de location. Perte de maintenance en cas d'achat.	La disparition d'un tiers contractant, à l'instar de la rupture de contrat est peu prévisible, à l'inverse de la rupture elle ne pourra donner lieu à compensation a priori. L'indisponibilité engendrée est immédiate.		X	X	X	X	X	
	TIE.04	Fin de vie logicielle	La fin de vie d'un logiciel peut entraîner un arrêt total et définitif du service rendu en cas d'anomalie (du fait de la disparition de la maintenance associée)	Certains logiciels en fin de vie, sous licence achetée, s'arrêtent purement et simplement de fonctionner à l'échéance de la licence.				X	X		
	TIE.05	Fin de vie matérielle	La fin de vie matérielle peut entraîner un arrêt total et définitif en cas d'anomalie.	Les matériels en fin de vie ne s'arrêtent pas de fonctionner, cependant leur mise à jour et/ou maintenance devient impossible		X	X				
	TIE.06	Obsolescence programmée	L'obsolescence programmée d'un matériel entraîne un arrêt de fonctionnalité de celui-ci à une date imprévisible	Bien qu'interdites ces pratiques existent (par exemple certains constructeurs ont été condamnés pour de telles pratiques. Exemple Apple en 2020 www.economie.gouv.fr/dgccrf/transaction-avec-le-groupe-apple-pour-pratique-commerciale-trompeuse)		X	X				
Humain	HUM.01	Grève endogène	Une grève interne peu empêcher l'accès à des sites rendant impossible l'exécution de certaines tâches et pouvant provoquer une indisponibilité de certaines fonctions/services. Le personnel en grève peu également être nécessaire à la réalisation de certaines actions et les rendre indisponibles.	Porter son attention dans le cas de personnes identifiées comme clef	X		X	X	X	X	
	HUM.02	Grève exogène	Un mouvement social externe au service peut prendre pour cible l'établissement et bloquer son accès, entraînant une indisponibilité des fonctions assurées par le personnel ayant normalement un accès à celui-ci	En fonction de l'importance du mouvement social, les conséquences temporelles peuvent être plus ou moins importantes. Il est complexe d'avoir des moyens d'actions sur une grève exogène, seuls des moyens de contournements seront à réfléchir.	X		X	X	X	X	
	HUM.03	Départ d'une personne clef	La fonction/service à laquelle la personne était affectée peut s'arrêter d'être réalisable faut du savoir-faire suffisant dans l'organisme	Un départ peut être prévu et gérable (démission, licenciement, retraite, mutation), ou imprévu (décès)	X		X	X	X		
	HUM.04	Perturbation d'une personne clef	La fonction/service à laquelle la personne est affectée est perturbée et sa disponibilité peut être mise en cause	La perturbation peut venir d'éléments endogènes à l'organisation (cadre de travail, relation avec les collègues, stress, …) ou exogènes (problèmes familiaux, état de santé, …)	X		X	X	X		
	HUM.05	Surcharge d'une personne clef	La fonction/service à laquelle la personne est affectée est perturbée et sa disponibilité peut être mise en cause	Lorsque la charge de travail d'une personne clef est supérieure à ses capacités, et ce de manière durable, la fonction qu'elle assume est perturbée et peut être partiellement indisponible	X		X	X	X		

Type	ID	Menace	Conséquences possibles sur le fonctionnement du SI	Commentaires	Portée						Interne
					Humaine	Matérielle	Infrastructure	Applicative	Informationnelle	Bâtiment / Site	
	HUM.06	Maladie grave d'une personne clef	La fonction/service à laquelle la personne est affectée est perturbée et sa disponibilité peut être mise en cause	On entend par dégradation des capacités, toutes conséquences d'une maladie provoquant une baisse significative d'efficacité de la personne ; que cette maladie soit reconnue ou non en tant que handicap.	X		X	X	X		
Attaque « Cyber »	ATT.01	Piégeage de matériel	Matériel inutilisable ou en baisse de capacité	Le piégeage est initialement utilisé pour accéder à l'information ou pour exploiter une vulnérabilité dans le but de s'introduire dans le SI, cependant il peut également engendrer une baisse ou une perte de disponibilité de l'usage du bien.		X	X				X
	ATT.02	Piégeage de logiciel	Logiciel inutilisable ou en baisse de capacité	Le piégeage est majoritairement utilisé pour accéder aux informations contenues dans le logiciel, ou transitant par celui-ci, cependant il peut également engendrer une baisse ou une perte de disponibilité de l'usage du logiciel et/ou des données qu'il contient				X	X		X
	ATT.03	Ransomware	Le ransomware est un piégeage particulier, son objectif est de rendre inaccessible les données présentes sur les objets contaminés de manière momentanée (jusqu'à paiement d'une rançon)	Principalement issus d'attaque par phishing, même si on note une évolution vers des attaques primaires autres à base d'utilisation de 0day. Bien que la conséquence première du Ransomware soit de rendre indisponible les données chiffrées, les matériels et logiciels exploitant ces données peuvent être de facto indisponibles également.		X	X	X	X		X
	ATT.04	Attaque DDoS	Une attaque de type DoS (Deny of Service) ou DDoS (Distributed Deny of Service) a pour objectif de provoquer une défaillance du SI de manière totale ou partielle.	Principalement issus d'attaques externes visant des services ouverts pour lesquels l'attaquant tente de saturer le service par une demande valide mais excessive. On note l'apparition de quelques cas d'attaques internes ayant bénéficié d'intrusions préalables par un autre biais. Elle est volontairement distinguée de la panne matérielle car des moyens de protection contre les attaques DDoS existent.			X	X				X
	ATT.05	Attaque MitM	Une attaque de type MitM (Man in the Middle) a pour objectif premier d'écouter les échanges sur un réseau, voire de les modifier ; cependant elle peut entraîner une baisse d'efficacité de celui-ci, voire une indisponibilité.				X				X
	ATT.06	Attaque par ajout de matériel destructeur	Une attaque par ajout de matériel destructeur peut entraîner la perte totale du matériel ciblé.	Les attaques par ajout de matériel destructeur nécessitent l'accès à ces matériels. Par exemple, l'introduction d'une clef USB « tueuse » (injection de courant à très haut ampérage) www.presse-citron.net/usb-killer-la-cle-usb-tueuse-de-pc-est-disponible-a-la-vente/		X	X				X
	ATT.07	Vol de matériel	Matériel et données contenues inutilisables	La vraisemblance est augmentée avec un support portable, léger et/ou amovible		X	X		X		X
Défaillances	DEF.01	Panne de matériel	Matériel et données contenues inutilisable momentanément ou de manière permanente			X	X		X		
	DEF.02	Dysfonctionnement du matériel	Matériel en baisse de capacité	Une mauvaise connectique, un défaut de fabrication, des erreurs erratiques sont des exemples de défaillances		X	X				
	DEF.03	Panne de logiciel	Logiciel inutilisable momentanément ou de manière permanente. A un niveau global ou simplement sur une fonctionnalité. Les données manipulées par le logiciel peuvent elles aussi être indisponibles.	Une utilisation anormale d'un logiciel peut entraîner une panne, mais également un défaut d'installation, ou encore une quantité de tests insuffisante.				X	X		
	DEF.04	Dysfonctionnement de logiciel	Logiciel inutilisable partiellement et de manière erratique.	Une utilisation anormale d'un logiciel peut entraîner un dysfonctionnement d'une partie de celui-ci. Un défaut d'installation ou encore une quantité de tests insuffisante. Un espace restreint du matériel hôte peut également être la cause.				X	X		
	DEF.05	Perturbation de la maintenabilité du SI	Perturbation générale ou partielle et potentiellement erratique du SI, des applicatifs y fonctionnant et des données stockées	Une maintenance insuffisante ou trop « décalée », ou encore non préparée peut être la cause de cette menace.		X	X	X	X		

Type	ID	Menace	Conséquences possibles sur le fonctionnement du SI	Commentaires	Portée						
					Humaine	Matérielle	Infrastructure	Applicative	Informationnelle	Bâtiment / Site	Interne
	DEF.06	Perturbation de la maintenabilité d'une application	Perturbation générale ou partielle et potentiellement erratique de l'application et des données manipulées	Une maintenance insuffisante ou trop « décalée », ou encore non préparée peut être la cause de cette menace				X	X		
	DEF.07	Dépassement de capacité d'un matériel/logiciel	Peut provoquer l'arrêt de la fonction/service opéré par le matériel/logiciel saturé			X	X	X	X		X
Exceptionnel	EXC.01	Pandémie	Une pandémie perturbe l'activité de l'organisme, pouvant entraîner l'arrêt de certaines fonctions. Cela peut également entraîner la surcharge de certaines fonctions habituellement peu utilisées	En fonction de la gravité, de l'étendue et de la rapidité de propagation, cela peut prendre de cours une organisation dans sa « réorganisation ». Combinant plusieurs problématiques : localisation, éventuelle perte humaine, ressources, …	X	X	X	X	X		
	EXC.02	Attaque terroriste	Une attaque terroriste peut provoquer l'arrêt complet de l'organisme, la perte d'une ou plusieurs personnes, l'arrêt de service ou de fonction	En fonction de l'importance de l'attaque, de sa proximité et de la visée (ou non) de l'organisme, les conséquences possibles vont du négligeable au plus important	X	X	X			X	

Annexe 6 – Exemple de fiche réflexe

Fiche réflexe : *(indiquer ici l'identification du risque traité)*

Gravité de la crise	*indiquer ici le niveau de gravité de la crise traitée par cette fiche*
Niveau de Cellule	*indiquer ici le niveau de cellule de crise qui doit être convoqué*
Temps prévus	*indiquer ici les temps prévus pour les différents modes (dégradé, nominal)*

Description des mesures d'urgences :

indiquer ici les mesures d'urgences identifiées permettant de réduire l'impact de la crise ou son envergure.

Passage en mode dégradé :

indiquer ici les mesures à prendre pour permettre de mettre en œuvre le mode dégradé nécessaire à la continuité d'activité

Retour au mode nominal :

indiquer ici les mesures à prendre pour permettre au SI impacté par la crise de revenir au mode nominal

Récupération des données :

indiquer ici les mesures à prendre pour récupérer les données telles qu'existantes avant la crise et y adjoindre les données générées pendant le mode dégradé. Devront également être identifié les mesures à prendre pour reconstruire les données perdues

Aide :

indiquer ici toutes les informations permettant de faciliter la gestion de la crise.

Annexe 7 – Echelles

Echelle de Gravité en fonction de la typologie de l'Impact

	1 - Mineure	2 - Importante	3 – Majeure	4 - Critique
Politique et image de marque	Plaintes ou doléances limitées d'usagers ou partenaires.	Plaintes ou doléances importantes d'usagers ou partenaires. Mentions limitées dans la presse.	Campagnes dans des médias locaux ou campagnes limitées dans des médias nationaux. Mouvements de protestation locaux ou limités. Perte limitée de pouvoir de négociation.	Campagnes dans des médias nationaux ou internationaux. Mouvements de protestation importants. Perte importante de pouvoir de négociation.
Désorganisation interne ou externe	Nécessité d'adaptation limitée du mode de fonctionnement habituel.	Augmentation de la charge de travail. Doléances ou plaintes des équipes. Stress élevé des équipes.	Bouleversements importants de la vie des personnes. Mobilisation limitée de moyens ou ressources supplémentaires. Perte limitée de productivité. Mouvements ou protestation limités.	Mobilisation importante de moyens ou ressources supplémentaires. Perte importante de productivité. Mouvements de protestation importants.
Légal et réglementaire	Sanction interne au ministère.	Condamnation civile d'un agent du ministère. Mention du Ministère dans une affaire civile ou pénale.	Enquête administrative. Condamnation ou amende prononcée à l'encontre du Ministère.	Condamnation pénale d'un agent du Ministère ou du Ministère.
Financier et économique	Impact budgétaire limité pour le Ministère.	Pertes supérieures à 10 millions d'euros pour le Ministère. Impact économique ou financier limité pour un partenaire du Ministère.	Pertes supérieures à 50 millions d'euros pour le Ministère. Impact économique ou financier important pour un partenaire du Ministère.	Pertes supérieures à 200 millions d'euros pour le Ministère. Impact économique ou financier critique pour un partenaire du Ministère.
Atteinte à la vie des personnes	Inconfort ou stress élevé des personnes.	Blessure légère d'agents ou de personnes extérieures au Ministère.	Blessure lourde d'agents ou de personnes extérieures au Ministère.	Accident grave impliquant un nombre important de personnes. Décès de personnes.

Echelle de Vraisemblance

	1 – Très improbable	2 - Improbable	3 - Probable	4 – Très probable
Vraisemblance	La vraisemblance du scénario est faible.	La vraisemblance du scénario est significative.	La vraisemblance du scénario est élevée.	La vraisemblance du scénario est très élevée.

Echelle DMIA (Disponibilité Maximale d'Interruption Acceptable)

	1 – Sans garantie	2 - Standard	3 - Elevé	4 - Critique
DMIA	N'est pas considéré comme gênant si l'indisponibilité dépasse 48h	Perturbe l'activité si l'indisponibilité est comprise entre 4h et 48h	Nuit à l'activité si l'indisponibilité est comprise entre 2h et 4h	Nuit gravement à l'activité si l'indisponibilité est inférieure à 2h

Echelle PDMA (Perte de Données Maximale Acceptable)

	1	2	3	4
PDMA	Une perte des deux dernières journées est acceptable	Une perte de la dernière journée est acceptable	Une perte des 4 dernières heures est acceptable	Aucune perte de donnée n'est acceptable

Matrice de Risques

4 - Critique				
3 – Majeure				
2 – Importante				
1 – Mineure				
Gravité / Vraisemblance	**1 – Très improbable**	**2 - Improbable**	**3 - Probable**	**4 – Très probable**

Acceptation du risque	Mineur	Important	Majeur	Critique

MINISTÈRES
TRANSITION ÉCOLOGIQUE
COHÉSION DES TERRITOIRES
MER

Liberté
Égalité
Fraternité