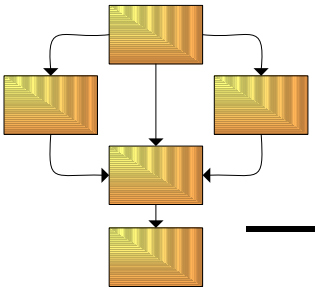


Club EBIOS

Gestion de la continuité des activités

Mémento

Date	:	18 novembre 2008
Statut	:	Approuvé
Nombre de pages	:	49
Responsable des travaux	:	Cyril DEMONCEAUX
Validation	:	Cercle de concertation concerné
Approbation	:	Cercle stratégique

Club EBIOS, 72 avenue Gaston Boissier, 78220 VIROFLAY

Ce document a été réalisé par le Club EBIOS

Responsable des travaux :

- Cyril DEMONCEAUX

Contributeurs :

- Jean-Luc ALLARD
- Anne COAT-RAMES
- Jean-Louis FLEISCH
- Matthieu GRALL
- Cyril MOURLON
- SAGEM SECURITE (Loïc BOURNON)
- TEAMLOG (Jean-Jacques BUREAU)

Contributeurs invités :

- Lydie BRONDEL, du ministère de l'Économie, des finances et de l'industrie
- David GUENEZAN, de THALES SECURITY SYSTEM
- Sandrine LAFFAURIE, d'EDELWEB

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante (voir formulaire de recueil de commentaires en fin de document) :

Club EBIOS
72 avenue Gaston Boissier
78220 VIROFLAY

contact[at]club-ebios.org

Table des matières

INTRODUCTION 5

CONTEXTE DE RÉDACTION 5

OBJECTIF DU MÉMENTO 5

CONTENU DU MÉMENTO 5

1 PRÉSENTATION DES CONCEPTS 6

1.1 LES ORGANISMES FACE À LA CONTINUITÉ 6

1.2 L'INCIDENT ET LA CRISE, ÉVÈNEMENTS PORTANT ATTEINTE À LA CONTINUITÉ DE L'ORGANISME 6

1.3 LA GESTION DE LA CONTINUITÉ PERMET DE TRAITER LES INCIDENTS ET LES CRISES 7

1.4 LES NIVEAUX DE CONTINUITÉ, LE BAROMÈTRE DE L'ORGANISME 8

2 LA CONTINUITÉ DES ACTIVITÉS, UN PROCESSUS TRANSVERSE DE LA SSI 9

2.1 UN EMPLOI SPÉCIFIQUE DE LA GESTION DE RISQUES 9

2.2 LE BON ÉLÈVE DE LA DÉFENSE EN PROFONDEUR 9

2.3 UN PROCESSUS TRANSVERSE DU SGSSI 9

3 LA GESTION DE LA CONTINUITÉ DES ACTIVITÉS EN 4 PHASES ITÉRATIVES 10

4 LE RÉFÉRENTIEL DE LA CONTINUITÉ DES ACTIVITÉS 12

4.1 LA POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION (PSSI) 12

4.2 LE PLAN DE CONTINUITÉ DES ACTIVITÉS (PCA) 12

4.3 L'APPRÉCIATION DES RISQUES LIÉS À LA CONTINUITÉ DES ACTIVITÉS (BIA) 12

4.4 LES PLANS DE CONTINUITÉ 12

4.5 LE TABLEAU DE BORD 13

4.6 LA MAIN COURANTE 13

4.7 L'ANNUAIRE DE GESTION DE LA CONTINUITÉ 13

4.8 LES PROCÉDURES D'ESCALADE 14

4.8.1 Description 14

4.8.2 Têtes de déclenchement 14

5 ORGANISATION DANS LA GESTION DE LA CONTINUITÉ 15

5.1 LES ACTEURS DE LA GESTION DE LA CONTINUITÉ, RÔLES ET RESPONSABILITÉS 15

5.1.1 Le comité de gestion de continuité 15

5.1.2 Le gestionnaire des plans de continuité 15

5.1.3 La cellule de veille 15

5.1.4 Le gestionnaire d'incidents 16

5.1.5 Le comité de crise ... 16
5.1.6 Le responsable d'un plan de continuité ... 17
5.1.7 La cellule de coordination ... 18
5.1.8 Les équipes opérationnelles ... 18
5.1.9 Le responsable des moyens généraux ... 19
5.1.10 Le personnel utilisateur ... 19

5.2 LES MOYENS ET OUTILS DE GESTION DE LA CONTINUITÉ ... 19

5.3 LES MOYENS ET OUTILS SPÉCIFIQUES À LA GESTION DE CRISE ... 20
5.3.1 Le centre de gestion de crise ... 20
5.3.2 Le site alternatif ... 20
5.3.3 La « mallette » de gestion de crise ... 20

ANNEXES ... 21

ANNEXE 1 – GLOSSAIRE ... 21

ANNEXE 2 – ACRONYMES ... 29

ANNEXE 3 – RÉFÉRENCES BIBLIOGRAPHIQUES ... 29

ANNEXE 4 – DESCRIPTION DES ACTIVITÉS DE LA GESTION DE LA CONTINUITÉ AU SEIN DU SGSSI ... 30
Phase 1 : Planifier ... 30
Phase 2 : Mettre en œuvre ... 32
Phase 3 : Vérifier ... 34
Phase 4 : Améliorer ... 36

ANNEXE 5 – CONTENU D'UN PLAN DE CONTINUITÉ TYPE ET EXEMPLES ... 37
Les différents types de procédures mise en œuvre par le plan de continuité ... 37
Contenu d'un plan type ... 38
Proformae de plan de continuité ... 39
Des exemples de plans de continuité des activités ... 40

ANNEXE 6 – L'ANNUAIRE ... 42
Informations nécessaires à la gestion de crise ... 42
Mises à jour de l'annuaire ... 42
Recherche dans l'annuaire ... 42
Proformae d'annuaire ... 43

ANNEXE 7 – LES TABLEAUX DE BORD ... 44

ANNEXE 8 – LES INTERACTIONS ENTRE LES ACTEURS DE GESTION DE LA CONTINUITÉ DES ACTIVITÉS ... 46
Gestion du PCA ... 46
Gestion d'un incident ou d'une crise ... 47

FORMULAIRE DE RECUEIL DE COMMENTAIRES ... 48

Introduction

Contexte de rédaction

Aujourd'hui, les interactions entre organismes augmentent et les délais se raccourcissent. Les organismes sont de plus en plus dépendants par rapport à leur système d'information. L'indisponibilité du système d'information peut engendrer de lourdes conséquences pour une entreprise telles qu'une incapacité à fournir un service, une perturbation de fonctionnement de tiers, une perte de l'image de marque et des pertes financières pouvant aller jusqu'au dépôt de bilan. La gestion de la continuité des activités apparaît donc comme un enjeu majeur pour assurer la survie d'un organisme.

Une étude des différents documents relatifs à la continuité des activités a permis de mettre en évidence des divergences de notions, la présentation de plans de continuité variés et l'utilisation d'un vocabulaire non homogène sans rattachement à des normes internationales existantes.

Objectif du mémento

Ce mémento a notamment pour objectif de s'accorder sur les termes en se rapprochant du référentiel de la DCSSI et les normes en cours [A détailler]. Il fixe les différents processus de la gestion de la continuité et présente les divers plans associés (contenu, domaine d'application, positionnement, acteurs concernés). Ce mémento fait référence à des guides de meilleures pratiques permettant de mettre en place au sein de l'organisme un système de gestion de la continuité des activités via la méthode de gestion des risques [EBIOS].

Ce document s'adresse aux responsables de la sécurité des systèmes d'information du secteur public ou privé souhaitant mettre en place dans leur organisme un système de gestion de la continuité de leurs activités essentielles.

Contenu du mémento

Ce mémento présente les concepts liés à la continuité des activités (chapitre 1) et leurs places dans la SSI (chapitre 2). Les activités propres à la gestion de la continuité sont ensuite présentées selon 4 phases itératives (chapitre 3). Le référentiel (chapitre 4), l'organisation (chapitre 5) et les outils associés sont ensuite développés.

Des annexes complètent le document par un glossaire, les acronymes, les références bibliographiques et un ensemble d'explications pratiques.

1 Présentation des concepts

1.1 Les organismes face à la continuité

La plupart des organismes n'ont pas conscience de leur dépendance vis-à-vis de leur système d'information et n'imaginent pas que leur activité métier puisse être mise en cause sans préavis.

Tous les organismes gèrent quotidiennement des situations à problème. Une majorité se résout rapidement, selon les compétences et le savoir-faire interne et n'a pas d'impact sur l'organisme. Cependant certaines difficultés plus sérieuses peuvent altérer le fonctionnement normal des activités et avoir ainsi un impact sur la continuité de l'organisme. L'interruption d'un service pendant une durée « incompatible avec le métier de l'entreprise » peut altérer la confiance des clients, des fournisseurs et des actionnaires et porter préjudice à la réputation et à la santé financière de l'entreprise.

On constate que ces évènements peuvent avoir une ampleur plus ou moins importante et des conséquences sur l'organisme.

1.2 L'incident et la crise, évènements portant atteinte à la continuité de l'organisme

Le cycle de continuité des activités englobe tous les événements susceptibles d'avoir des conséquences sur la continuité de l'organisme. Pour des raisons de simplification, nous retiendrons dans ce document deux types d'évènements que sont l'incident et la crise.

Un incident est un évènement, anticipé ou non, qui perturbe le cours normal des activités de l'organisation ayant un faible impact sur l'organisme. Les conséquences potentielles à court et moyen termes sur la continuité des activités essentielles de l'organisme sont faibles. Un incident, s'il n'est pas maîtrisé, peut entraîner une crise. On rencontre des incidents tous les jours.

Une crise est un évènement soudain causant des pertes et des dommages importants, entraînant une interruption d'une ou plusieurs activités critique et un arrêt de l'organisme. La crise nécessite le recours à un comité de crise et, le cas échéant, à un site alternatif. Une crise a des impacts à long terme et peut avoir des conséquences sur la survie même de l'entreprise.

Une crise nécessite le déploiement d'une organisation, de moyens et de ressources exceptionnelles afin d'assurer la continuité des activités de l'entreprise.

La mise en place d'un système de gestion de la continuité des activités apparaît déterminant compte tenu de ces différents évènements.

1.3 La gestion de la continuité permet de traiter les incidents et les crises

La gestion de la continuité des activités définit les actions permettant la mise en place d'une structure organisationnelle, logistique et technique visant à réagir face à des incidents ou des crises afin de garantir à tout moment un niveau de service acceptable.

La gestion de la continuité des activités inclut donc l'ensemble des activités liées à la gestion des incidents et à la gestion de crise. La gestion de la continuité permet aussi bien de faire face à un incident qu'à une crise. Selon le niveau de criticité de la situation, l'organisme va déployer une organisation, des moyens et des plans adaptés.

Quelle que soit la stratégie adoptée par l'organisme pour maintenir ses activités en toute situation, elle doit pouvoir répondre à :

- l'urgence : par exemple, un plan de secours informatique assurera la maîtrise des dégâts provoqués par un incident afin de rétablir un fonctionnement minimal du SI ;
- le retour à la normale : un plan de continuité métier assurera la liaison entre le mode de fonctionnement minimal et le fonctionnement nominal ;
- la montée en puissance : une gestion de crise devient nécessaire lorsque l'organisme est impuissant face aux dégâts provoqués malgré les plans de secours et de continuité. Le scénario développé peut nécessiter la mise en place d'une cellule de crise destinée à piloter les efforts de l'ensemble de l'organisme. Les plans de continuité doivent être déclenchés en fonction du niveau de continuité de l'organisme.

1.4 Les niveaux de continuité, le baromètre de l'organisme

Selon l'événement, un incident ou une crise, le niveau de service rendu par l'organisme est plus ou moins dégradé. Ce niveau est appelé niveau de continuité. Dans le cas où l'événement serait mal géré, la situation peut empirer. Le passage d'un niveau à l'autre doit être connu de tous afin de déclencher les plans adaptés. La cellule de veille a la charge de suivre le niveau de continuité de l'organisme. L'échelle suivante présente les différents niveaux de continuité de l'organisme.

Libellé	Activité	Atteinte	Impact
Fonctionnement optimal de l'organisme	Un monitoring constant de la situation est assuré afin de détecter les situations à risques et les alertes au plus tôt.	Aucune atteinte	Aucun impact
Fonctionnement de l'organisme faiblement perturbé	Activation des plans de continuité concernés La résolution de la situation ne nécessite pas la mise à disposition de ressources exceptionnelles.	Pas d'interruption d'activités critiques.	Impact à court terme.
Fonctionnement de l'organisme fortement perturbé	Détection d'une crise ou d'une mauvaise gestion d'un incident. Activation des plans de continuité concernés	Une ou plusieurs activités critiques sont menacées. Interruption d'activités critiques possible.	Impact à moyen terme
Fonctionnement de l'organisme arrêté	Détection d'une crise ou d'un incident échappant au contrôle. Activation des plans de continuité concernés (plan de crise) Mise en place de la cellule de crise Activation du site alternatif éventuel	Pérennité de l'organisme potentiellement remise en cause.	Impact à long terme.

Maintenant que nous nous sommes entendus sur la notion de gestion de la continuité, les différents événements et l'échelle de niveau de continuité, nous allons découvrir comment s'articule la continuité dans la sécurité des systèmes d'information.

2 La continuité des activités, un processus transverse de la SSI

2.1 Un emploi spécifique de la gestion de risques

La gestion de la continuité n'est qu'une utilisation spécifique de la gestion de risques. L'appréciation des risques permet dans un premier temps d'identifier et de hiérarchiser les risques ayant un impact sur la continuité de l'organisme (cf. *chapitre 4.3 L'appréciation des risques liés à la continuité des activités*). Tous les composants du risque peuvent ensuite être couverts (élément menaçant, vulnérabilités, impacts) par la mise en place de mesures en amont (mesures de prévention, de protection et de détection) mais également de mesures de réaction en aval, pour la réduction de l'impact (mise en place d'une organisation de gestion de la continuité, de plans de continuité spécifiques et de ressources associées).

2.2 Le bon élève de la défense en profondeur

Le mémento de la DCSSI sur la défense en profondeur définit la défense en profondeur appliquée au système d'information comme une défense globale coordonnant plusieurs lignes de défense et couvrant toute la profondeur du système. La défense en profondeur est dynamique et suffisante.

La gestion de la continuité des activités couvre ces deux aspects.

D'une part, la mise en place d'une organisation de gestion de la continuité, permettant la remontée d'alerte et l'activation de plans de continuité adaptés à l'évènement et au niveau de continuité de l'organisme, forme une défense « dynamique ».

D'autre part, la couverture de l'ensemble des composants du risque par des mesures techniques et organisationnelles de protection (réduction de l'opportunité de la menace par la couverture de l'élément menaçant et des vulnérabilités), de détection et de réaction (réduction de l'impact) par le déploiement de plans de continuité constitue une défense « suffisante ».

Le risque est réduit en amont par des mesures et par ailleurs, dans un souci de défense en profondeur, des mesures de réaction sont mises en place pour réduire les impacts du risque sur l'organisme au cas où ce dernier surviendrait tout de même. Cette approche permet de mettre en place plusieurs lignes de défense caractéristiques de la défense en profondeur.

2.3 Un processus transverse du SGSSI

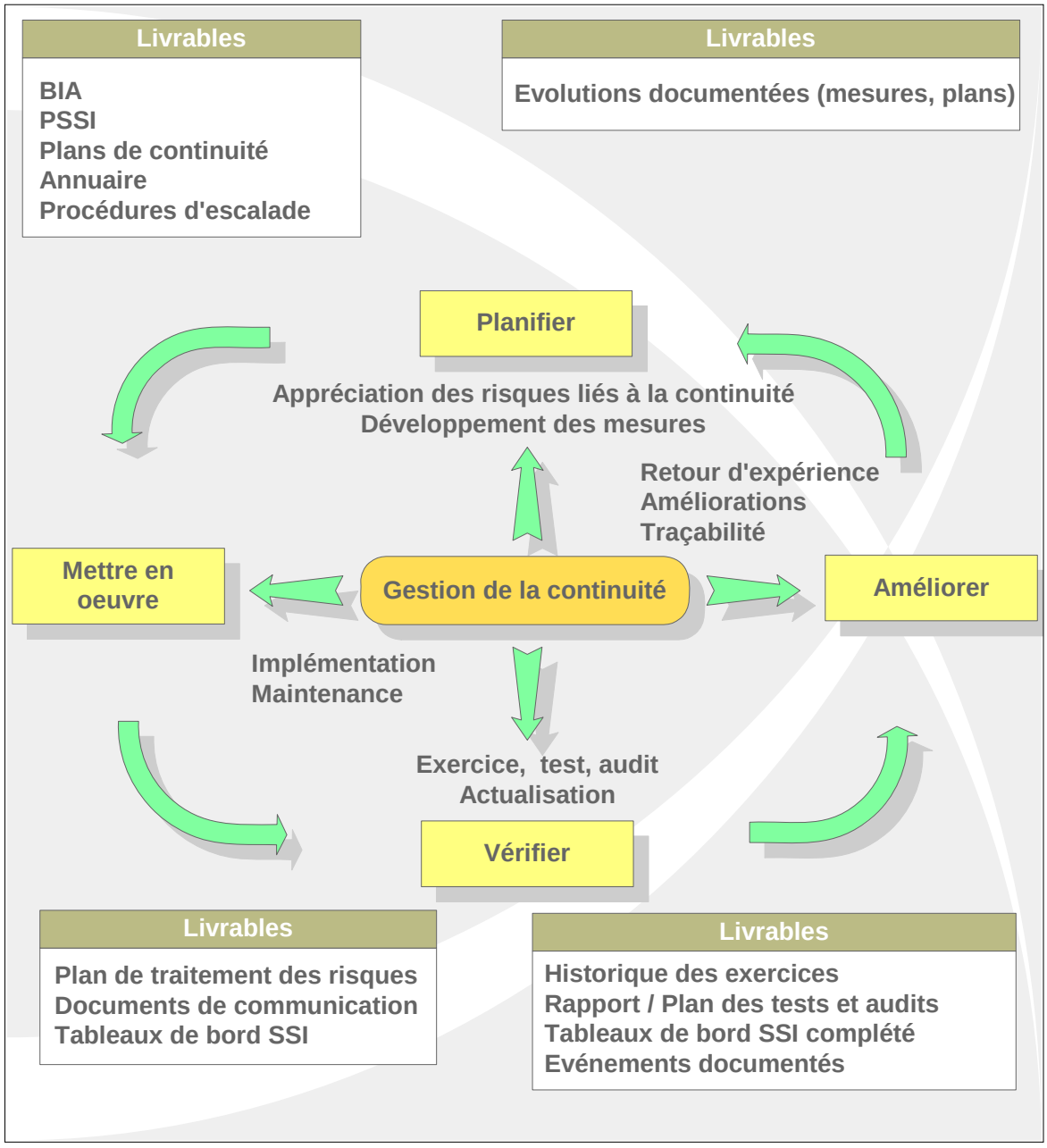
La norme internationale ISO 27001 définit comment mettre en place au sein de son organisme un système de gestion de la sécurité des systèmes d'information (SGSSI ou ISMS *Information Security Management System*). Ce SGSSI est structuré en quatre étapes cycliques (planifier, mettre en œuvre, vérifier, améliorer), afin de respecter le principe de la roue de Deming issue du monde de la qualité.

3 La gestion de la continuité des activités en 4 phases itératives

La gestion de la continuité des activités consiste en un pilotage des processus visant à identifier les impacts potentiels des menaces sur un organisme et à fournir à l'organisation une structure, des moyens et des procédures pour lui permettre de maintenir ses activités essentielles à un niveau acceptable en cas d'incident ou de crise.

Les processus de la gestion de la continuité sont cycliques et s'inscrivent dans les étapes du système de gestion de la sécurité des systèmes d'information (SGSSI).

Le schéma ci-dessous définit les processus et les livrables de la gestion de la continuité à travers les étapes du SGSSI[1].



[1] Le Plan de traitement des risques couvre les mesures en amont et en aval.

Le tableau ci-dessous présente les activités de la gestion de la continuité dans un processus continu de gestion de la SSI. Ces différentes activités sont décrites en Annexe 4.

Étapes SGSSI	Gestion de la continuité des activités
Planifier	Définir le périmètre de gestion de la continuité Définir les besoins en continuité des activités Analyser et apprécier les risques liés à la continuité des activités Identifier et évaluer les options pour traiter les risques SSI Identifier les mesures de sécurité pour traiter les risques
Mettre en œuvre	Mettre en œuvre les différentes mesures de la PSSI, plans de continuité Gérer les ressources techniques et organisationnelles Identifier les indicateurs de mise en œuvre des plans et d'efficacité du système de gestion de la continuité des acticités (SGCA) Suivre la mise en œuvre des mesures de sécurité et des plans
Vérifier	Exécuter les procédures de vérification et autres mesures Vérifier régulièrement la performance du SGCA Mesurer l'efficacité du SGCA Vérifier régulièrement l'appréciation des risques, ainsi que le niveau de risque résiduel et du risque acceptable Mener des audits internes réguliers du SGCA Mettre à jour les plans de sécurité pour prendre en compte les résultats des actions précédents Enregistrer les actions et évènements pouvant impacter la performance du SGCA
Améliorer	Mettre en œuvre les améliorations identifiées pour le SGSSI Prendre les mesures correctives et préventives appropriées Communiquer les résultats et actions, consulter les parties prenantes S'assurer que les révisions réalisent leurs objectifs prévus

4 Le référentiel de la continuité des activités

4.1 La politique de sécurité du système d'information (PSSI)

La politique de sécurité référence l'ensemble des mesures organisationnelles et techniques (prévention, protection, détection, réaction) permettant de couvrir les risques du système que l'organisme souhaite réduire.

La PSSI référence notamment les risques liés à la continuité de l'organisme et les mesures de sécurité associées. Les plans de continuité, qui constituent des mesures de réaction, sont référencés dans un chapitre spécifique appelé plan de continuité des activités (PCA) décrit ci-dessous.

La section 3 du guide d'élaboration de politiques de sécurité des systèmes d'information de la DCSSI liste un ensemble de mesures de sécurité. Le *chapitre 2 (Principes de mise en œuvre*) liste un ensemble de mesures de sécurité sur la Planification de la continuité des activités.

4.2 Le plan de continuité des activités (PCA)

Le PCA référence les instructions, les procédures, l'organisation et les ressources permettant le maintien des éléments essentiels – nécessaires et suffisants – à la continuité des activités de l'entreprise avant, pendant et après un incident ou une crise.

Il référence l'appréciation des risques liés à la continuité des activités (*Business Impact Analysis* – BIA), la stratégie de traitement, les plans de continuité (associés à un risque et classés par activité), les procédures d'escalade et l'annuaire.

Le PCA doit être accessible quel que soit l'état dans lequel se trouve l'organisme. Le PCA doit dont être disponible sur plusieurs type de média : ressources en ligne, sauvegardes sur bandes, support papier mis au coffre…

4.3 L'appréciation des risques liés à la continuité des activités (BIA)

L'appréciation des risques liés à la continuité des activités (*Business Impact Analysis* - BIA) permet dans un premier temps de déterminer les éléments essentiels pouvant causer l'interruption d'une activité économique critique et leurs impacts sur l'organisme.

Une appréciation des risques permet ensuite d'identifier l'ensemble des évènements (incident ou crise) susceptibles de porter atteinte à la continuité des activités de l'organisme.

Cette activité est réalisée par le comité de gestion de la continuité. Ce dernier est chargé, à l'issue de la rédaction du BIA de définir, pour chacun des risques, la stratégie de recouvrement et les décisions de planification de la continuité pour l'organisation.

Le BIA doit être réalisé en collaboration avec le comité de crise ayant la responsabilité en cas de crise de déclencher les différents plans de continuité (ou leurs différentes phases ou actions) en fonction du contexte.

Un guide de meilleures pratiques de la DCSSI explique les étapes à réaliser afin de rédiger un BIA à l'aide de la méthode [EBIOS].

4.4 Les plans de continuité

Le plan de continuité des activités (PCA) référence les plans de continuité (terme global intermédiaire et didactique) classés par secteur d'activité et niveau de continuité. Ces plans couvrent un ou plusieurs risques identifiés dans le BIA et sont activés en cas d'incident ou de crise. Les plans de continuité des activités doivent être connus par l'ensemble des acteurs concerné et sont référencés comme des mesures de réaction, sous la forme de procédures d'exploitation de sécurité (PES), dans la PSSI.

Les différents types de procédures, le contenu d'un plan de continuité et une liste d'exemples sont présentés en Annexe 5.

4.5 Le tableau de bord

Le tableau de bord permet une remontée des informations au niveau opérationnel (cellule de veille, équipe opérationnelle), pilotage (responsable des plans de continuité, comité de crise) et stratégique (comité de gestion de la continuité, direction). C'est un outil de coordination et de supervision.

Dans un premier temps, il permet à la voie fonctionnelle SSI de suivre l'évolution de la mise en œuvre des mesures amont (mesures de prévention, de protection et de détection) et des plans de continuité.

En second lieu, il permet de suivre l'efficacité du SGCA (historique des incidents ou crise, rapidité d'exécution des plans, limitation des impacts…).

Par ailleurs, il permet à l'ensemble des acteurs de suivre l'évolution du niveau de continuité des activités de l'organisme. Il apparaît cependant difficile en période de crise de mettre à jour les tableaux de bord en temps réel, alors que l'ensemble des acteurs est sollicité et que le système d'information n'a pas un niveau de continuité acceptable. Les acteurs préfèrent utiliser dans ce cadre la main courante qui retranscrit chacun des évènements et les actions en cours. Une fois que le système d'information fonctionne à un niveau de continuité acceptable, il est envisageable d'utiliser un tableau de bord afin de superviser les actions de retour à la normale (procédures de restauration) et le niveau de continuité par activité.

Le rôle du tableau de bord dans la gestion de la continuité des activités est précisé en Annexe 7.

Le chapitre *Identifier les indicateurs de mise en œuvre des plans et d'efficacité du SGCA* de l'Annexe 4 décrit les différents types d'indicateurs.

4.6 La main courante

La cellule de veille (cf. *chapitre 5.1.7. La cellule de veille*) doit recenser au sein d'une main courante pour chaque incident ou crise :

- le(s) événement(s) en cours (incident ou crise),
- le(s) risque(s) associé(s) (mettre notamment en évidence les activités touchées et l'impact sur l'organisme),
- le(s) plan(s) de continuité d'activé, les acteurs chargés du traitement et le(s) procédure(s) en cours,
- leur(s) état(s) : non traité / traitement en cours / terminé.

La main courante doit être disponible à l'ensemble des acteurs.

4.7 L'annuaire de gestion de la continuité

L'annuaire liste les correspondants à contacter en cas d'incident ou de crise. Il revêt une importance primordiale et conditionne la réactivité et l'efficacité des actions.

L'annuaire répertorie par l'ensemble des acteurs jouant un rôle dans un plan de continuité.

Il doit également publier l'organigramme de l'entité, la chaîne fonctionnelle SSI et notamment la cellule de veille, le service informatique ainsi que le comité de crise.

La création des annuaires passe donc par l'identification de tous les acteurs impliqués dans l'exécution des plans, que leurs responsabilités soient fonctionnelles ou opérationnelles. Régulièrement, les acteurs identifiés doivent être sensibilisés à leur responsabilité. Ils doivent être formés et participer aux exercices liés au déclenchement des plans.

Le contenu de l'annuaire est développé en Annexe 6.

4.8 Les procédures d'escalade

4.8.1 Description

Ce document répertorie séquentiellement, par activité, les différents types de risques (incidents ou crises) par niveaux de gravité (hiérarchisation à partir des besoins en continuité des activités touchées, des impacts sur l'organisme et de l'opportunité du risque). Pour chacun des risques, il convient de lister les indicateurs, les responsables et les plans de continuité associés ainsi que les conditions d'escalade.

La procédure d'escalade permet d'activer les procédures relatives à *l'échelon supérieur* quand l'évènement échappe au contrôle de l'organisme.

La procédure d'escalade pointe sur l'annuaire de plan de continuité et devrait être à disposition de la cellule de veille.

4.8.2 Têtes de déclenchement

Au sein de l'organisme, la cellule de veille évalue les dégâts et, en fonction du risque et des plans de continuité à mettre en œuvre, alerte les têtes de déclenchement. Selon le niveau de continuité associé au risque, la cellule de veille alerte le responsable du plan de continuité concerné (en cas d'incident) ou le comité de crise. Ces derniers sont alors responsables du déclenchement et de la coordination des plans. Habituellement, ces acteurs font partie de la chaîne fonctionnelle SSI (Haut fonctionnaire de défense – Fonctionnaire de sécurité des systèmes d'information – Responsables de sécurité des systèmes d'information…). Ils ont la charge d'alerter l'ensemble des équipes opérationnelles concernées et les responsables des plans de continuité dépendants.

5 Organisation dans la gestion de la continuité

La gestion de la continuité permet aux décideurs et aux utilisateurs de prendre conscience de la gravité des évènements liés à la continuité de l'organisme. La remontée des alertes, la communication des informations doivent être réalisées le plus rapidement possible. Il convient pour cela de définir une organisation adaptée de gestion de la continuité.

5.1 Les acteurs de la gestion de la continuité, rôles et responsabilités

L'identification des acteurs pour chacun des plans de continuité permet une gestion courante des incidents. Même si son envergure est plus limitée, l'organisation mise en place est identique celle prévue pour la gestion de crise.

Un événement peut survenir à tout moment. En fonction du besoin en continuité de l'organisme, un système d'astreinte ou de service de garde peut être mis en place. Il faut également s'assurer que ces acteurs aient accès au bâtiment en dehors des heures ouvrées.

Le rôle de chaque acteur est défini aux chapitres suivants.

Les interactions entre acteurs sont présentées en Annexe 8.

5.1.1 Le comité de gestion de continuité

Le comité de gestion de continuité est chargé d'apprécier les impacts sur l'organisme en cas de perte de la continuité des activités. Il définit la stratégie de recouvrement des risques et l'organisation à mettre en œuvre en cas d'incident ou de crise.

Il est composé du comité de direction, des responsables économiques, de la chaîne fonctionnelle SSI et d'experts techniques.

Il est chargé de coordonner les actions de construction de l'ensemble des plans de continuité.

En cas de crise, le comité de gestion de continuité doit prendre toutes les mesures nécessaires pour s'assurer de la bonne exécution des plans déclenchés au sein de son organisme. Des moyens de communications avec le comité de crise doivent être prédéfinis et garantis.

5.1.2 Le gestionnaire des plans de continuité

Le gestionnaire des plans de continuité est le responsable organisationnel du comité de gestion de continuité. Il n'est ni le propriétaire ni le grand décideur du ou des plans.

Dans un environnement complexe, il peut arriver que l'on nomme plusieurs gestionnaires. Chaque gestionnaire est dans ce cas responsable de la construction, de l'implémentation, du test et de l'évolution d'un ou plusieurs plans.

5.1.3 La cellule de veille

La cellule de veille centralise toutes les remontées d'évènements. Elle peut être alertée par le bureau informatique, un utilisateur, le gardien ou le responsable des moyens généraux. Par ailleurs, des outils automatiques (signaux d'alarme par exemple) ou informatiques (base SNMP, sonde réseau, supervision des journaux systèmes, sniffer…) peuvent être utilisés pour automatiser la remontée des informations.

Comme l'indique l'[ISO 17799], les procédures de remontées d'alertes doivent être formalisées afin de réduire les temps de réaction. Lors d'un évènement la cellule de veille doit :

- évaluer les dégâts,
- classifier l'événement,
- remonter l'information aux personnes concernées.

En fonction du niveau de l'évènement, la cellule de veille contacte le gestionnaire d'incidents ou le comité de crise.

Dans le cas d'une crise, la réactivité prime et l'objectif est d'informer sans délai les têtes de déclenchement. Tous les moyens disponibles référencés dans l'annuaire sont alors utilisés pour informer le comité de gestion de crise de la situation le plus rapidement possible.

5.1.4 Le gestionnaire d'incidents

Le gestionnaire d'incidents gère la continuité des activités lorsque l'organisme fonctionne de manière nominale. Sur la base des informations communiquées par la cellule de veille, le gestionnaire d'incidents réalise les actions suivantes :

- identifier la procédure d'escalade correspondante,
- identifier le ou les plans de continuités concernés,
- alerter le ou les responsables des plans,
- suivre la mise en œuvre des plans.

Les activités du gestionnaire d'incidents peuvent être assurées par la cellule de veille.

5.1.5 Le comité de crise

Le comité de crise constitue la structure organisationnelle de gestion de crise. Il assiste le comité de gestion de continuité à la rédaction des plans de continuité relatifs à la gestion de crise.

Pour être efficace, le comité de crise doit être restreint. Il est composé d'un représentant du comité de direction, des responsables économiques, de la chaîne fonctionnelle SSI et d'experts techniques. Ses membres doivent être assujettis à des astreintes ou au moins être disponibles à tout moment et en tout lieu.

Le comité de crise se réunit dans le centre de gestion de crise situé à proximité du site touché pour remplir son rôle dans les meilleures conditions.

En cas de crise, il a la responsabilité de déclencher les différents plans de continuité (ou leurs différentes phases ou actions) en fonction du contexte et de coordonner leur mise en application. Il alerte les responsables des plans de continuité à activer.

Durant toute la crise, il assure la liaison avec la direction générale et/ou le comité de gestion de continuité.

Le comité de crise doit maintenir un canal de communication permanent avec les services internes et externes de l'organisme. Une personne peut être chargée de réaliser des communiqués sur la crise à destination des clients, fournisseurs et partenaires. Les remontées d'informations des équipes opérationnelles permettent au comité de crise d'avoir une vision de l'état réel de la situation permettant une prise de décision avertie.

En cas de nécessité, le comité de crise a la charge d'activer un site alternatif, situé à distance raisonnable de l'organisme, permettant d'assurer une continuité des activités pendant la phase de restauration.

Le comité de crise est mis en place lorsque l'organisme est en phase de crise. Lors de gestion d'incidents, c'est le gestionnaire d'incidents (ou directement la cellule de veille) qui assure la gestion de la continuité des activités.

5.1.6 Le responsable d'un plan de continuité

Le responsable d'un plan de continuité est chargé de construire le plan de continuité visant à réduire les impacts d'un risque sur une activité essentielle, à assurer une continuité de service tout au long de l'événement à un niveau dégradé acceptable et à restaurer le service au niveau nominal.

En amont, il s'assure de l'efficacité des procédures définies dans le plan :

- maintenir le plan à jour à chaque changement du contexte,
- tester une partie ou la totalité du plan,
- mettre à jour le plan après un retour d'expérience.

En cas d'incident, le responsable du plan de continuité est alerté par le gestionnaire d'incidents (ou directement la cellule de veille).

En cas de crise, le plan de continuité est activé à la demande du comité de crise en fonction des évènements.

Le responsable prend alors la responsabilité de mettre en œuvre les plans à activer dont il a la charge.

Un ensemble d'étapes est nécessaire avant l'activation d'un plan :

- analyser la situation sur la base des informations récoltées par la cellule de veille,
- vérifier les points de contrôles.

Lorsque le plan est activé, le responsable du plan de continuité procède aux actions suivantes :

- vérifier les conditions de mise en œuvre du plan,
- estimer les procédures du plan à mettre en œuvre et les acteurs à alerter,
- lancer les procédures,
- activer la cellule de coordination éventuelle et les équipes opérationnelles,
  - Alerter les acteurs
  - Transmettre des actions à réaliser adaptée au contexte
  - Indiquer éventuellement des postures spécifiques à adopter
  - Demander d'un accusé réception
- coordonner et superviser l'application du plan,
  - Demander régulièrement un état courant de la situation
  - Vérifier régulièrement l'état d'avancement du traitement de la situation
  - S'assurer de la bonne communication entre les acteurs
    - en interne,
    - avec l'extérieur.
- rendre compte à la hiérarchie, à la chaine fonctionnelle SSI, à travers la cellule de veille ou le comité de crise, de l'évolution des travaux,
- alerter les responsables des plans de continuité dépendants.

Le responsable du plan de continuité peut être assisté par une cellule de coordination afin de piloter les différentes actions réalisées par les équipes opérationnelles.

Il est conseillé de désigner un responsable d'un plan de continuité par activité essentielle de l'organisme. Cela permet de regrouper les différents plans de continuité propre à une activité essentielle sous une responsabilité unique (et son remplaçant). Il peut en effet être nécessaire d'activer plusieurs plans de continuité sollicitant des équipes opérationnelles support ou métier (informatique, télécommunication, logistique, ressources humaines…) afin d'assurer la continuité d'un service essentiel.

5.1.7 La cellule de coordination

Le pilotage des opérations de continuité peut être confié à une cellule de coordination, dirigée par le responsable du plan de continuité concerné. Cette cellule décharge le gestionnaire d'incidents et le comité de crise des tâches de coordination avec les équipes opérationnelles chargées de la mise en œuvre des procédures.

Certaines décisions peuvent lui être déléguées par le comité de crise comme l'anticipation du déclenchement de certains dispositifs ou plans d'action.

La cellule est constituée à la demande du comité de crise en fonction des évènements, mais également dans le cas d'un incident, en fonction d'un processus d'escalade. Le responsable du plan de continuité, alerté par la cellule de veille, est en charge de la création de la cellule de coordination dont il prend la direction et du déclenchement de son plan de continuité.

5.1.8 Les équipes opérationnelles

Les équipes opérationnelles ont deux rôles principaux :

- évaluer les dégâts,
- appliquer les procédures du plan de continuité sur le plan technique :
  - les procédures d'urgences permettant de contenir, lutter et stopper l'événement,
  - les procédures alternatives permettant aux activités de se poursuivre en mode dégradé,
  - les procédures de restauration permettant de réactiver le SI dans un état nominal.

D'une manière générale, les acteurs doivent suivre la démarche suivante :

1. accuser réception du message d'activation ou d'action et rendre compte des actions effectuées au responsable du plan ou la cellule de coordination,
2. analyser et mettre en œuvre les mesures et les ressources associés,
3. tenir informer le responsable du plan de continuité ou la cellule de coordination de l'avancement des travaux,
4. rester en attente de nouvelles mesures en fonction du niveau d'alerte.

Les équipes opérationnelles peuvent-être issue des services support ou métier de l'organisme :

- des différents services métiers de l'entreprise,
- du service informatique,
- du service sécurité du bâtiment,
- du service médical,
- du service d'hygiène,
- du service comptabilité,
- du service des ressources humaines,
- du service logistique,
- de l'ensemble des utilisateurs de l'entreprise,
- …

5.1.9 Le responsable des moyens généraux

Le responsable des moyens généraux gère les moyens de soutien communs à l'ensemble des activités métier de l'organisme tels que l'électricité, le chauffage, le système de climatisation, la disponibilité des locaux…. Il est souvent responsable du contrôle d'accès physique.

Le responsable des moyens généraux peut-être chargé de la gestion et du maintien en condition opérationnel des ressources nécessaires à la mise en œuvre des mesures et plans de continuité des activités.

En cas d'incident ou de crise, il a à charge l'évaluation des dégâts relatifs aux moyens sous sa responsabilité et l'alerte de la cellule de veille.

En fonction de la procédure d'escalade et de l'annuaire des plans de continuité, le responsable des moyens généraux peut être sollicité par la cellule de coordination afin de réaliser un ensemble d'actions relatives à un ou plusieurs plans de continuité.

5.1.10 Le personnel utilisateur

Selon la mesure *Journalisation des faiblesses de sécurité* du chapitre 13 de l'[ISO 17799], les utilisateurs sont chargés d'alerter la cellule de veille en cas d'incident ou de crise.

Les procédures de remontées d'alerte doivent être connues de tous et l'annuaire doit être accessible facilement.

En fonction de la procédure d'escalade et de l'annuaire des plans de continuité, les utilisateurs peuvent être sollicités par la cellule de coordination afin de réaliser un ensemble d'actions relatives à un ou plusieurs plans de continuité, par exemple :

- organisation du redémarrage (normal ou dégradé),
- mise en place de procédures de contournement éventuelles,
- organisation de travaux exceptionnels,
- tâches d'attente du secours.

Les utilisateurs doivent être sensibilisés aux plans de continuité qui les concernent, ainsi que sur la procédure d'alerte (les coordonnées de la cellule de veille, les indicateurs les concernant…).

5.2 Les moyens et outils de gestion de la continuité

L'annuaire, les procédures d'escalade, le PCA répertoriant l'ensemble de plans de continuité, les tableaux de bord et la main courante permettent à l'ensemble des acteurs de gérer la continuité des activités au sein de l'organisme.

Il doit être mis à la disposition des acteurs un jeu papier de l'ensemble de ces moyens. Une sauvegarde dans un bâtiment extérieur doit également être effectuée qui constitue généralement le lieu d'où la cellule de crise contrôlera les évènements.

Lors du déclenchement des plans, les différents acteurs doivent pouvoir communiquer entre eux rapidement. On doit s'assurer de l'existence de moyens de communication fiables, redondants, diversifiés et immédiatement accessibles par l'ensemble des acteurs.

Il peut être important, selon le niveau de sensibilité des informations, de disposer de moyens de communication sécurisés, en cas de besoins en confidentialité, en intégrité et en imputabilité sur les informations échangées.

5.3 Les moyens et outils spécifiques à la gestion de crise

5.3.1 Le centre de gestion de crise

Le centre de gestion de crise est un site où le comité de crise se réunit afin coordonner la gestion de la crise.

Il est situé dans un périmètre suffisamment proche de l'environnement ciblé afin de faciliter la communication avec les responsables des plans de continuité activés et faciliter les déplacements, mais ne doit pas être adjacent à celui-ci pour ne pas être sujet aux mêmes évènements. En cas de sensibilité de l'organisme, sa localisation peut être tenue secrète.

Il doit être muni des équipements de communication adéquats permettant la coordination et la mise en place des plans de continuité. Les moyens de communication doivent être maintenus vers les clients, les fournisseurs et les partenaires.

5.3.2 Le site alternatif

Le site alternatif est un site opérationnel permettant d'assurer la continuité des activités essentielles de l'entreprise en cas de crise. Il est constitué des serveurs de secours et d'une infrastructure permettant d'assurer les activités critiques de l'entreprise à un niveau de dégradation défini dans le plan de continuité.

La direction, au cours de la rédaction du BIA doit identifier et hiérarchiser les activités devant être assurées en toute circonstance. Il convient d'identifier la liste des moyens techniques à mettre en œuvre en fonction des activités identifiées comme essentielles au sein des plans de continuité relatif à l'activation du site alternatif.

Le site alternatif doit être suffisamment éloigné de l'organisme pour ne pas être sujet aux mêmes évènements et suffisamment près pour limiter les inconvénients liés aux déplacements et aux échangent de données. Par ailleurs, sa localisation doit rester secrète, notamment en cas de grève.

Il doit être muni des équipements de communication adéquats permettant le maintien des activités économiques de l'organisme et de sa communication.

Les possibilités de renforcement du personnel, les moyens de mobilisation du personnel, la possibilité de faire du télétravail et les extensions de délégation de signature doivent être recensés en cas d'activation du site alternatif.

5.3.3 La « mallette » de gestion de crise

Il doit exister une mallette au format papier et électronique regroupant tous les documents nécessaires à l'armement du comité de crise et du site alternatif.

Annexes

Annexe 1 – Glossaire

Acceptation du risque (*risk acceptance*)	Décision d'accepter un risque traité selon les critères de risque. [EBIOS]
Activité essentielle (*Mission Critical Activity* – MCA)	Fonction participant à la finalité (la raison d'être) de l'entreprise. La perte d'une fonction critique trahit l'essence du système : il devient impossible d'appréhender sa finalité.
Alerte	Notification qu'un risque existe potentiellement ou a eu lieu.
Analyse du risque (*risk analysis*)	Utilisation systématique de données pour l'identification des origines des attaques et l'estimation du risque. [EBIOS]
Annuaire d'alerte et de gestion de la continuité	Document présentant, par activité économique, selon les procédures d'escalade, le responsable du plan de continuité à appeler en cas d'incident ou de crise.
Appréciation du risque (*risk assessment*)	Ensemble du processus d'analyse du risque et d'évaluation du risque. [ISO Guide 73]
Appréciation des risques liés à la continuité (*Business Impact Analysis* – BIA)	Détermination des éléments essentiels pouvant causer l'interruption d'une activité économique critique de l'organisme suivi d'une analyse des impacts déterminant les impacts d'une interruption en terme de niveau de dégradation (RSO), de délai reprise (RTO) et de point de reprise (RPO). [ISO 17799]
Cellule de coordination	Le pilotage des opérations de continuité peut être confié à une cellule de coordination, dirigée par le responsable du plan de continuité concerné. Cette cellule déchargera le comité de crise des tâches de coordination entre les équipes opérationnelles déclenchées.
Cellule de veille	La cellule de veille est en charge de surveiller les indicateurs critiques aux systèmes définis dans les tableaux de bord SSI, d'évaluer les dégâts, de classifier les évènements et d'avertir en fonction de la procédure d'escalade, le gestionnaire d'incidents ou le comité de crise.
Équipe opérationnelle	L'équipe opérationnelle est en charge d'évaluer les dégâts et de réaliser le plan de continuité sur le plan technique (mesures de réaction, mesures alternatives, mesures de réparations…).
Centre de gestion de crise	Site où le comité de crise se réunit afin de gérer la crise.
Comité de crise (*crisis team*)	En cas de crise, le comité de crise a la responsabilité de déclencher les différents plans de continuité (ou leurs différentes phases ou actions) en fonction du contexte. Ses membres doivent être assujettis à des astreintes (service de garde) ou au moins être disponibles à tout moment et en tout lieu.

	Le comité de crise contient un représentant de chacune des composantes du comité de gestion de continuité et assure la liaison avec la direction générale et/ou le comité de gestion de continuité.
Comité de gestion de continuité	Maîtrise d'ouvrage chargée d'apprécier les impacts d'activité de l'organisme, de définir la stratégie de recouvrement et les décisions de planification de la continuité pour l'organisation en cas d'incident ou de crise. Il est composé du comité de direction, des responsables économiques et des experts techniques. Des moyens de communications avec le comité de crise doivent être prédéfinis et garantis en cas de crise.
Confidentialité (*confidentiality*)	Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés. [EBIOS]
Crise (*disaster*)	Évènement soudain causant des pertes et des dommages importants, entraînant une interruption d'une ou plusieurs activités critique ou un arrêt de l'organisme, ayant des impacts à long terme et nécessitant le recours à un comité de crise et, le cas échéant, à un site alternatif. Une crise peut avoir des conséquences sur la survie même de l'entreprise.
Critère de sécurité (*security criteria*)	Caractéristique d'un élément essentiel permettant d'apprécier ses différents besoins de sécurité. [EBIOS] *Exemples :* *disponibilité ;* *intégrité ;* *confidentialité* …
Délai de reprise (*Recovery Time Objective* – RTO)	Période maximale de temps acceptable d'un arrêt d'une activité économique de l'entreprise, avant le retour en mode nominal.
Disponibilité (*availability*)	Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés. [EBIOS]
Élément essentiel (*essential element*)	Information ou fonction ayant au moins un besoin de sécurité non nul. [EBIOS] *Exemples :* *une liste de noms ;* *une requête de certification ;* *gérer la facturation ;*

un algorithme de chiffrement ;

…

Élément menaçant

(*threat agent*)

Action humaine, élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Elle peut être caractérisée par son type (naturel, humain, ou environnemental) et par sa cause (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, elle est aussi caractérisée par une exposition et des ressources disponibles. Dans le cas d'une cause délibérée, elle est aussi caractérisée par une expertise, des ressources disponibles et une motivation. [EBIOS]

Exemples :

ancien membre du personnel ayant peu de compétences techniques et de temps mais susceptible d'avoir une forte motivation ;

pirate avec de fortes compétences techniques, bien équipé et une forte motivation liée à l'argent qu'il peut gagner ;

climat très fortement pluvieux pendant trois mois par an ;

virus ;

utilisateurs ;

développeurs ;

…

Entité

(*entity*)

Il s'agit d'un bien qui peut être de type organisation, site, personnel, matériel, réseau, logiciel, système. [EBIOS]

Exemples :

société d'infogérance ;

locaux de l'organisme ;

administrateur système ;

micro-ordinateur portable ;

Ethernet ;

système d'exploitation ;

portail de téléprocédure ;

…

Évaluation des dégâts

(*damage assessment*)

Le rassemblement des informations pertinentes et valides lors d'un incident ou d'une crise, est primordial afin d'aider le comité de crise dans la décision de déclenchement des différents plans de continuité en fonction du contexte.

Évaluation du risque (*risk evaluation*)	Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque. [ISO Guide 73]
Fonction (*function*)	Traitement ou ensemble de traitements contribuant au fonctionnement d'une activité d'un organisme, qui crée, modifie, détruit ou transporte des informations. [EBIOS] *Exemples :* - *créer des plans techniques ;* - *établir les devis ;* - *gérer la facturation ;* - *un algorithme de chiffrement ;* - *générer un certificat ;* - *…*
Gestion de la continuité des activités (*Business Continuity Management* – BCM)	Gestion des processus visant à identifier les impacts potentiels des menaces sur un organisme et à fournir à l'organisation une structure, des moyens et des procédures pour lui permettre de maintenir ses activités essentielles en cas d'incident ou de crise à un niveau acceptable.
Gestionnaire des plans de continuité	Maîtrise d'ouvrage étant responsable organisationnel du comité de gestion de continuité chargée de coordonner les actions de construction des différents plans de continuité. Il n'est ni le propriétaire ni le grand décideur du ou des plans.
Gestionnaire d'incidents	Le gestionnaire d'incidents gère la continuité des activités lorsque l'organisme fonctionne de manière nominale sur la base des informations communiquées par la cellule de veille. Les activités du gestionnaire d'incidents peuvent être assurées par la cellule de veille.
Gestion du risque (*risk management*)	Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque. [ISO Guide 73]
Incident (*incident*)	Évènement, anticipé ou non, qui perturbe le cours normal des activités économiques de l'organisation, ayant un faible impact sur l'organisme et des conséquences potentielles à court et moyen termes sur la continuité des activités essentielles de l'organisme. Un incident s'il n'est pas maîtrisé peut entraîner une crise. On rencontre des incidents tous les jours.
Indicateur (*preventive control*)	Donnée statistique combinant la mesure d'un ou plusieurs points-clés et utilisée en comparaison avec un historique, une (des) valeur(s) cible(s) et/ou une (des) valeur(s) seuil(s). [TDBSSI]
Information essentielle (*critical information*)	Renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement. [IGI 900] [REC 901]

Impact

(*impact*)

Conséquence sur l'organisme de la réalisation d'une menace. [EBIOS]

Exemples :

perte d'image de marque vis-à-vis de la clientèle ;

perte financière à hauteur de 10% du chiffre d'affaires ;

infraction aux lois et aux règlements donnant lieu à des poursuites judiciaires à l'encontre du Directeur ;

…

Information

(*information*)

Renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement. [IGI 900] [REC 901]

Exemples :

- *un message ;*
- *une liste de noms ;*
- *une requête de certification ;*
- *liste de révocation ;*
- *…*

Intégrité

(*integrity*)

Propriété d'exactitude et de complétude des éléments essentiels. [EBIOS]

Menace

(*threat*)

Attaque possible d'un élément menaçant sur des biens. [EBIOS]

Exemples :

un ancien membre du personnel, ayant peu de compétences techniques mais susceptible d'avoir une forte motivation, altère volontairement les logiciels du système par un virus, profitant de la facilité d'introduire des logiciels à effets malicieux sur le réseau bureautique de l'organisme ; ceci pouvant notamment affecter la fonction d'établissement de devis et la génération de certificats de signature ;

un pirate avec une bonne expertise, un matériel standard et payé pour le faire, vole des fichiers confidentiels en accédant à distance au réseau de la société ;

un développeur, membre du personnel, avec une très bonne expertise des codes sources mais peu de connaissances SSI, modifie volontairement le code source ;

un visiteur vole un matériel contenant des informations confidentielles ;

…

Mesure de sécurité

Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en œuvre pour la satisfaire. Il peut s'agir

(*security measure*)	de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de "lutte", de récupération, de restauration, de compensation… [EBIOS]
Méthode d'attaque (*attack method*)	Moyen type (action ou événement) pour un élément menaçant de réaliser une attaque. [EBIOS] *Exemples :* *vol de supports ou de documents ;* *piégeage du logiciel ;* *atteinte à la disponibilité du personnel ;* *écoute passive ;* *crue ;* *…*
Niveau de reprise (*Recovery Scope Objective* – RSO)	Niveau acceptable du service fourni lors ou après une remise en service après une crise. Il constitue une dégradation du niveau accepté de service (SLA).
Personnel utilisateur	En cas d'incident ou de crise, les utilisateurs ont en charge l'évaluation des dégâts et l'alerte de la cellule de veille.
Plan de continuité (*Continuity Plan* – CP)	Le plan de continuité des activités (PCA) englobe un ensemble de plan de continuité (terme global intermédiaire et didactique) classé par secteur d'activité couvrant un ou plusieurs risques identifiés dans le BIA, activé en cas d'incident ou de crise.
Plan de continuité des activités - PCA (*Business Continuity Plan* – BCP)	Documentation référençant les instructions, les procédures, l'organisation et les ressources permettant le maintient des éléments essentiels nécessaires à la continuité des activités de l'entreprise avant, pendant et après un incident ou une crise. Le PCA est constitué de l'analyse des impacts d'activité (BIA) et de leur stratégie de recouvrement, comprenant les plans de continuité (associés à un risque et classés par activité), la procédure d'escalade et l'annuaire des plans de continuité.
Point de reprise (*Recovery Point Objective* – RPO)	Point dans le cycle de vie des données qu'il convient de restaurer. Il aide à définir la politique de back up, le degré de « perte d'informations » que l'organisme considère comme acceptable.
Politique de sécurité de système d'information (*information systems security policy*)	Ensemble, formalisé dans un document applicable, des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. [PSSI]
Prise de risque (*risk retention*)	Acceptation de la charge de la perte d'un risque particulier. [EBIOS]

Procédure d'escalade (*escalation procedure*)	Document répertoriant séquentiellement, par activité, les différents types d'incidents et de crises par niveaux de gravité, les conditions d'escalade, ainsi que les indicateurs, les responsables et les plans de continuité associés. La procédure d'escalade pointe sur l'annuaire de plan de continuité. Il devrait être à disposition de la cellule de veille.
Responsable des moyens généraux	Personne ayant à charge la gestion des moyens de soutien communs à l'ensemble des activités métier de l'organisme.
Responsable du plan de continuité	Maîtrise d'œuvre réalisant le plan de continuité et qui dirige la cellule de coordination relative à son plan de continuité.
Site alternatif	Site opérationnel permettant la continuité des activités de l'entreprise en cas de crise. Il est constitué des serveurs de secours, et d'une infrastructure permettant d'assurer les activités critiques de l'entreprise à un niveau de dégradation défini dans le plan de continuité.
Réduction du risque (*risk reduction*)	Processus visant à minimiser les conséquences négatives et les opportunités d'une menace. [EBIOS]
Risque (*risk*)	Combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque et de l'impact sur les éléments essentiels et sur l'organisme. [EBIOS] *Exemples :* *un ancien membre du personnel, ayant peu de compétences techniques mais susceptible d'avoir une forte motivation, altère volontairement les logiciels du système par un virus, profitant de la facilité d'introduire des logiciels à effets malicieux sur le réseau bureautique de l'organisme ; ceci pouvant notamment affecter la disponibilité et l'intégrité de la fonction d'établissement de devis et de la génération de certificats de signature, ce qui pourrait engendrer une incapacité à fournir un service, une impossibilité de remplir des obligations contractuelles et de graves conséquences en termes d'image de marque ;* *un pirate avec une bonne expertise, un matériel standard et payé pour le faire, vole des fichiers confidentiels en accédant à distance au réseau de la société, entraînant de ce fait l'échec d'une transaction avec un partenaire et une perte d'image de marque ;* *…*
Sécurité des systèmes d'information (SSI) (*information security*)	Protection des systèmes d'information, et en particulier des éléments essentiels, contre toute atteinte des critères de sécurité non autorisée, qu'elle soit accidentelle ou délibérée. [EBIOS]
Système d'information (SI)	Ensemble d'entités organisé pour accomplir des fonctions de traitement d'information. [EBIOS]

(*information system*)

Tableau de bord SSI

Ensemble cohérent d'indicateurs mis en forme et agencés de manière à présenter une image synthétique de la situation de la sécurité du système d'information considéré. [TDBSSI]

Traitement du risque

(*risk treatment*)

Processus de sélection et de mise en œuvre des mesures visant à modifier le risque, ce qui signifie une réduction du risque, un transfert du risque ou une prise de risque. [EBIOS]

Transfert du risque

(*risk transfer*)

Partage avec une autre partie de la charge de la perte d'un risque particulier. [EBIOS]

Exemples :

souscription d'une assurance ;

…

Vulnérabilité

(*vulnerability*)

Caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information. [EBIOS]

Exemples :

absence d'organisation sécurité incendie pour une entité de type Organisation ;

peu de sensibilisation aux problèmes de sécurité pour une entité de type Personnel ;

facilité de pénétrer sur le site pour une entité de type Site ;

possibilité de créer ou modifier des commandes systèmes pour une entité de type Réseau ;

…

Annexe 2 – Acronymes

BCM	*Business Continuity Management*
BCP	*Business Continuity Plan*
BIA	*Business Impact Analysis*
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
MCA	*Mission Critical Activity* – Activité critique de l'organisme
PCA	Plan de Continuité des Activités
PES	Procédures d'Exploitation de Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
RPO	*Recovery Point Objective* – Point de reprise
RSO	*Recovery Scope Objective* – Niveau de dégradation
RTO	*Recovery Time Objective* – Délai de reprise
SGCA	Système de Gestion de la Continuité des Activités
SGSSI	Système de Gestion de la Sécurité des Systèmes d'Information
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
TDBSSI	Tableau De Bord SSI

Annexe 3 – Références bibliographiques

[EBIOS] *Expression des Besoins et Identification des Objectifs de Sécurité* – SGDN – version 2 (2004).

[PSSI] *Guide d'élaboration de politique de sécurité de système d'information* – DCSSI (2004).

[TDBSSI] *Guide d'élaboration de tableaux de bord de sécurité de système d'information pour les administrations* – DCSSI (2004).

[ISO 17799] *Information technology – Security Techniques – Code of practice for information security management* – International Organization for Standardization (ISO) (2005).

[ISO 27001] *Information technology – Security Techniques – Information security management systems – Requirements* – International Organization for Standardization (ISO) (2005).

Annexe 4 – Description des activités de la gestion de la continuité au sein du SGSSI

L'ensemble des processus de la gestion de la continuité est présenté par la suite en fonction des étapes du SGSSI relatives à l'ISO 27001.

Phase 1 : Planifier

La mesure *Inclure la sécurité du système d'information dans les processus de gestion de la continuité* du chapitre 14 de l'[ISO 17799] liste les différents processus nécessaires à la mise en place d'une gestion de la continuité dans l'organisme. L'ensemble de ces concepts est repris ci-dessous.

Définir le périmètre de gestion de la continuité

Dans un premier temps, il s'agit d'identifier les caractéristiques de l'organisme et du système étudié ainsi que le périmètre de l'étude afin de mettre en évidence les activités critiques de l'organisme et d'adopter à terme une gestion de risques adaptée. L'étape 1, *Étude du contexte,* de la méthode [EBIOS] permet de réaliser cette activité.

Définir les besoins en continuité des activités

La direction doit ensuite exprimer un besoin en continuité pour chaque activité critique identifiée, selon son niveau de criticité. Il existe différentes approches pour exprimer un besoin de continuité.

Il est possible d'utiliser une échelle spécifique à la continuité définissant un niveau de dégradation (*Recovery Status Objective*, RSO), un délai reprise (*Recovery Time Objective*, RTO) et un point de reprise (*Recovery Point Objective*, RPO) acceptables pour l'organisme.

Une autre approche consiste à exprimer un niveau de sécurité acceptable en fonction des 3 critères de sécurité les plus usités pour la gestion de risques (disponibilité, intégrité, confidentialité) vis-à-vis d'impacts liés à la continuité de l'organisme. En effet, la gestion de la continuité n'est pas limitée à un besoin en disponibilité des activités. Une infraction aux lois et règlement par exemple porte atteinte à la continuité de l'organisme mais ne constitue pas un problème en disponibilité. Il existe au sein de la méthode [EBIOS] une liste d'impacts sur la continuité tels que l'incapacité à fournir le service, perturbation du fonctionnement interne, impossibilité à fournir les obligations contractuelles...

Cette activité permet aux décideurs d'identifier les impacts sur l'organisme en cas d'incident ou de crise et les niveaux de service acceptables et se traduit par un livrable appelé *Business Impact Analysis* (BIA).

L'étape 2, *Expression des besoins de sécurité*, de la méthode [EBIOS] permet d'exprimer des besoins en continuité sur la base d'une échelle adaptée en fonction d'impacts liés à la continuité.

Étude des menaces

Les menaces sur le système sont identifiées avec leurs niveaux d'opportunité. L'étape 3, *Étude des menaces*, de la méthode [EBIOS] permet de réaliser cette activité.

Une fois l'ensemble des menaces sur le système identifiées, l'appréciation permet d'identifier les véritables risques sur la continuité des activités de l'organisme. Cette activité se déroule en 2 étapes successives, l'analyses et l'évaluation des risques.

Analyse des risques liés à la continuité des activités

L'analyse des risques permet dans un premier temps de faire apparaître les risques portant atteinte à la continuité de l'organisme. Pour cela, les menaces sur le système sont confrontées aux besoins en continuité exprimés pour chaque activité critique. Il convient donc de rédiger les risques en précisant leurs atteintes sur la continuité des activités critiques, leurs impacts potentiels sur l'organisme.

Évaluer les risques liés à la continuité des activités

Le risque est un évènement qui, selon sa nature (incidents ou crise) peut entraîner un impact plus ou moins grand sur la continuité de l'organisme.

La méthode de gestion des risques [EBIOS] permet de mettre en œuvre la mesure Continuité des activités et évaluation des risques du chapitre 14 de l'[ISO 17799]. En effet, la méthode [EBIOS] permet d'évaluer les risques liés à la continuité. Les risques peuvent être hiérarchisés en fonction de leurs atteintes sur la continuité des activités, leurs impacts sur l'organisme ainsi que sur le niveau d'opportunité des menaces. Des priorités peuvent ainsi être spécifiées par risque.

Identifier et évaluer les options pour traiter les risques SSI

La politique de traitement des risques est facilitée par l'évaluation des risques qui présente permet de hiérarchiser les risques selon leurs opportunités, leurs atteintes sur la continuité des activités et l'impact sur l'organisme. Les décideurs ont ainsi l'ensemble des informations nécessaires à la prise de décision. Une définition claire de la politique de traitement de chacun des risques et des plans de continuité associés est alors réalisée :

1. refus du risque,
2. optimisation du risque,
3. transfert du risque,
4. prise de risque.

Un plan de traitement des risques doit être validé par les décideurs.

Les risques ayant un impact majeur sur la continuité de l'organisme et ayant un niveau d'opportunité élevé sont traitées en en premier.

Les risques acceptés constituent des risques résiduels. Les décideurs prennent la responsabilité de ne pas couvrir ces risques, au vu de leurs impacts sur la continuité de l'organisme et de leur opportunité.

Identifier les mesures de sécurité pour traiter les risques

Il convient à cette étape de définir pour chacun des risques retenus un ensemble de mesures.

Ces mesures peuvent être issues de différents référentiels SSI comme [PSSI], l'[ISO 17799]….

Les différents types de mesures

La couverture du risque permet d'intervenir sur toutes les composantes du risque par le biais de mesures de sécurité mises en œuvre avant, pendant et après l'événement.

Avant l'événement :

- Mesures de prévention (réduction des impacts) :
  - Mise en place d'une organisation de gestion d'incident et de crise
  - Sensibilisation de l'ensemble des acteurs
  - Formation aux outils informatiques
- Mesures de protection (réduction des vulnérabilités)

Au cours de l'événement :

- Mesures de réaction (réduction des impacts) :
  - Procédures d'urgences,
  - Solutions alternatives,
  - Plan de communication

Après l'incident (réduction des impacts) :

- Mesures de réaction :
  - Procédures de réparation et de restauration
  - Procédures de retour à la vie normale

Nous constatons donc que les mesures peuvent être de différents types et couvrent l'ensemble des composantes du risque.

Les mesures de prévention et de protection sont employées dans la gestion de risques SSI.

Par contre, les mesures de réaction sont spécifiques à la gestion de la continuité des activités et constituent les plans de continuité.

L'ensemble des mesures est référencé dans la Politique de Sécurité des Systèmes d'Information (PSSI) de l'organisme. Les plans de continuité ne constituent qu'un chapitre de la PSSI.

Dans la suite du document, nous allons nous intéresser plus particulièrement aux activités liées à l'élaboration des plans de continuité.

Élaboration des plans de continuité, mesures de réaction spécifiques à la continuité

Le Plan de Continuité des Activités (PCA) est un document « chapeau » qui référence l'ensemble des documents permettant la gestion de la continuité au sein de l'organisme. Il référence ainsi l'ensemble des plans de continuité (cf. *chapitre 4 Le référentiel de la gestion de la continuité*).

Un risque peut être couvert par un ou plusieurs plan de continuité et un plan de continuité peut couvrir un ou plusieurs risques. Le plan de continuité constitue une mesure de réaction à activer lorsque le ou les risques auxquels il est rattaché surviennent (cf. *chapitre 6.5. Les plans de continuité*).

Le contenu et le niveau de détail de chacun des plans dépendent de la nature, du besoin et de la complexité de chaque organisme. Il convient de séparer les plans de continuité par domaines d'activité et de les référencer par niveau de continuité dans le PCA et dans les procédures d'escalade.

En effet, les procédures d'escalade référencent l'ensemble des risques (incident ou crise) par niveau de continuité, les plans de continuité associés et les conditions de déclenchement (cf. *chapitre 4.8 Les procédures d'escalade*).

Obtenir la validation des risques résiduels

Le traitement des risques liés à la continuité par la méthode [EBIOS] prévoit une démonstration de couverture. Les risques sont couverts par un ensemble de mesures et de plans de continuité. En cas de couverture partielle, les risques résiduels sont alors mis en évidence. Le décideur, au vu des composantes du risque non couvert, possède l'ensemble des informations nécessaires à la prise de décision.

Cette démarche de planification se rapproche du rapport du député M. LASORDES qui définit qu' *après avoir défini, sans se préoccuper des moyens associés et du système d'information, les activités qu'il considère comme sensible, l'organisme identifie toutes les composantes qui y contribuent (ressources humaines, produits, ressources informatiques, etc.). Puis il définit des modes opératoires permettant de contourner la difficulté rencontrée.*

Phase 2 : Mettre en œuvre

Mettre en œuvre les différentes mesures de la PSSI

Les mesures de prévention et de protection

Les mesures de sécurité définies dans la PSSI sont mises en œuvre et sont maintenues à jour en prenant en compte les moyens et l'organisation définis dans la stratégie de l'organisme.

La formation et la sensibilisation des acteurs est une mesure de prévention de la PSSI jugée importante dans la gestion de la continuité.

Le développement d'une culture de gestion de la continuité des activités est primordial et peut être déterminant en cas d'incident ou de crise, pour permettre une optimisation des réactions des personnes concernées.

L'ensemble du personnel doit être sensibilisé à la gestion de la continuité et doit connaître son rôle et les ressources à mettre en œuvre dans chacun des plans auxquels il est impliqué. Les acteurs doivent être formés aux outils déployés pour la gestion de la continuité, tels que l'annuaire, les procédures d'escalade, l'outil de veille et/ou le tableau de bord SSI, les outils de pilotages…

La rédaction de la PSSI et des plans de continuité permet d'impliquer et de sensibiliser les acteurs, de mettre en place une organisation de gestion de la continuité.

Les tests et les audits participent également au développement de la culture continuité. Ils doivent être réalisés avec l'ensemble des personnes concernées (Responsable du plan, cellule de coordination et équipe opérationnelle).

Les mesures de réaction, les plans de continuité

Les plans de continuité des activités, les ressources et l'organisation définies dans la stratégie sont mises en œuvre afin de gérer la continuité des activités de l'organisme.

L'annexe 9 décrit les interactions entre acteurs en cas d'incident ou de crise.

Gérer les ressources

Définition d'une stratégie technique relative aux ressources

Une fois les mesures et les plans de continuité permettant la réduction des risques définis, il convient d'identifier et de déployer les ressources nécessaires à leur mise en œuvre.

Une stratégie relative aux ressources nécessaires à la gestion de la continuité est notamment mise en place afin de s'assurer qu'en cas d'incident ou de crise, les différents moyens mis en œuvre dans les plans sont directement opérationnels.

Définition d'une stratégie organisationnelle

Au-delà d'une structure classique de gestion de risques SSI, une structure organisationnelle, des ressources et un centre opérationnel sont mis en place pour assurer la continuité des activités de l'organisme à un niveau minimum acceptable en cas d'un incident ou de crise. (cf. *chapitre 5 Organisation dans la gestion de la continuité*).

Les responsabilités des acteurs doivent être communiquées.

L'organisation déployée pour gérer la continuité de l'organisme varie en fonction du niveau de continuité. En cas de crise par exemple un comité de crise et un site alternatif peuvent être activés.

Pour chaque plan de continuité, une structure organisationnelle sur trois niveaux est mise en place :

- niveau stratégique,
  - Comité de gestion de la continuité des activités
  - Comité de gestion de crise
- niveau coordination,
  - Responsables du plan de continuité (Représentant de l'activité de l'organisme)
  - Cellule de coordination
- niveau opérationnel.
  - Équipe opérationnelle

Identifier les indicateurs de mise en œuvre des plans et d'efficacité du SGCA

Dans cette activité, il convient d'identifier différents types d'indicateurs.

Dans un premier temps, un ensemble d'indicateurs doit être défini pour suivre la mise en œuvre des mesures amont (mesures de prévention, de protection et de détection) et l'élaboration des plans liés à la continuité des activités.

En second lieu, des indicateurs doivent être identifier afin de suivre l'efficacité du SGCA (historique des incidents ou crise, rapidité d'exécution des plans, limitation des impacts…).

Par ailleurs, des indicateurs peuvent être définis sur la base des risques (incident, crise) afin :

- de détecter la survenance d'un risque en amont et d'identifier le ou les plans associés à déclencher,
- de suivre la mise en œuvre des procédures de restauration et le niveau de continuité des activités de l'organisme à tous les niveaux de la hiérarchie.

Il apparaît toutefois difficile d'alimenter ce type d'indicateur pendant une crise dans la mesure ou l'ensemble des ressources disponibles est sollicité et que le système d'information est atteint. La mise en œuvre des procédures d'urgences et alternatives ne peut se faire que par la main courante. La supervision des mesures et du niveau de continuité des activités par le biais de tableau de bord ne peut se faire qu'une fois le niveau de continuité acceptable des activités essentielles assuré (procédures d'urgence, procédure alternative

Les indicateurs peuvent être regroupés par domaine, activité, niveau, afin de constituer des tableaux de bord (cf. *chapitre 4.5 Le tableau de bord*).

Suivre la mise en œuvre des mesures de sécurité et des plans

Des tableaux de bords (cf. *chapitre 4.5 Le tableau de bord*) de niveaux opérationnels, pilotages et stratégiques sont mis en place sur la base des indicateurs définis à l'activité précédente.

Ces tableaux de bords permettent de suivre à tous les échelons de l'organisation la mise en œuvre des mesures et l'élaboration des plans.

Phase 3 : Vérifier

Exécuter les procédures de vérification et autres mesures

Les tests doivent être réalisés régulièrement pour vérifier l'efficacité des mesures et plans de continuité. Ils peuvent couvrir une partie ou l'ensemble du plan.

Le suivi des tests est réalisé par le responsable du plan de continuité. Ce dernier doit notamment s'assurer de la validité des informations contenues dans le plan. En effet certaines informations peuvent évoluer au cours du temps (informations personnelles, téléphone, adresse, ressources, réglementation, sous-traitant, fournisseurs…).

Par ailleurs, il doit gérer la maintenance des ressources nécessaires au déploiement des plans de continuité.

Par ailleurs, des exercices impliquant différents plans de continuité doivent être réalisés régulièrement afin de parfaire le dispositif, sensibiliser l'organisme et valider les procédures.

Ils impliquent l'ensemble des acteurs sur la base de scénarios prédéfinis afin de tester la réactivité de l'organisme sur l'ensemble des processus de gestion de la continuité :

- activation et de suivi des plans de continuité,
- mise en place d'une organisation de crise,
- basculement sur le site alternatif,
- …

Les exercices doivent d'abord permettre de réduire les délais de réaction et de déploiement des plans de continuité et de sensibiliser l'ensemble des acteurs aux processus nécessaires à la gestion

d'incident ou de crise. L'objectif des exercices est de roder l'ensemble des procédures, tant opérationnelles que techniques. Ils permettent de tester la réactivité et le bon comportement des personnes concernées face à une alerte.

La réalisation et le suivi des exercices sont sous la responsabilité du comité de gestion de la continuité.

A l'issue, un ensemble d'améliorations doit être identifié.

Différents types de tests sont notamment définis par l'[ISO 17799] :

a. vérification de l'efficacité des mesures face à différents scénarios,
b. simulations, formation des acteurs à la gestion d'un incident ou d'une crise,
c. tests techniques pour s'assurer de l'efficacité des moyens mis en œuvre dans les plans,
d. test de basculement sur un site alternatif,
e. essai des équipements et des services fournisseurs,
f. exercice grandeur nature permettant de tester l'organisation, les équipements, les services et les processus permettant de faire face à une interruption de service.

Vérifier régulièrement la performance du SGCA

Il est très important de promouvoir une culture d'évaluation et de retour d'expérience au sein de l'organisme.

Après chaque événement critique, une fois que l'organisme est revenu à un fonctionnement normal, il convient de réunir l'ensemble des intervenants pour identifier des axes d'amélioration. Un retour d'expérience des acteurs concerné permet de mettre à jour les plans de continuité, les ressources et l'organisation. Il peut être judicieux de faire une sensibilisation autour de l'événement au sein de l'organisme, qui serait plus parlant qu'un discours théorique dans la mesure où il a été vécu par le personnel.

Après chaque audit, test et exercice, une mise à jour des mesures et des plans de continuité doit être réalisée.

Mesurer l'efficacité du SGCA

Des tableaux de bord (cf. 4.4 Le tableau de bord) de niveaux opérationnels, pilotages et stratégiques sont mis en place sur la base des indicateurs définis au préalable.

Ces tableaux de bords permettent de mesurer à tous les échelons de l'organisation le niveau de continuité des activités de l'organisme.

Vérifier régulièrement l'appréciation des risques, ainsi que le niveau de risque résiduel et du risque acceptable

Il convient de réévaluer les risques à chaque changement de contexte (changement d'organisation, évolution de la menace, mise à jour du système…) afin de s'assurer de la pertinence des mesures et des plans de continuité.

Si des risques résiduels apparaissent, il convient d'identifier leurs atteintes sur la continuité des activités afin d'apprécier s'ils sont acceptables pour l'organisme.

Mener des audits internes réguliers du SGCA

Par ailleurs, il est conseillé qu'une entité indépendante réalise régulièrement un audit SSI de l'organisme en prenant en compte les aspects continuité. L'audit permet dans un premier temps de vérifier que les risques identifiés dans le BIA sont pertinents et que les mesures et plans de continuité planifiés sont adaptés. Ensuite, l'audit consiste à vérifier si les mesures organisationnelles et techniques sont effectivement mises en place.

Dans le cadre d'une homologation d'un système, l'autorité responsable s'appuie sur le résultat de l'audit pour juger du niveau de risque.

Mettre à jour les plans de sécurité pour prendre en compte les résultats des actions précédents

Les mesures et plans de sécurité sont mis à jour par rapport aux audits, aux tests et exercices, aux retours d'expérience ainsi que la réévaluation des risques.

Enregistrer les actions et évènements pouvant impacter la performance du SGCA

La réalisation du référentiel de gestion de la continuité via la méthode [EBIOS] facilite l'enregistrement des biens, des risques, des mesures et des plans susceptibles d'impacter les performances du SGCA.

La cellule de veille recense l'ensemble des évènements (incident, crise) subis par l'organisme et les procédures ayant été mises en œuvre.

Phase 4 : Améliorer

Mettre en œuvre les améliorations identifiées pour le SGSSI

Les améliorations identifiées à l'étape précédente sont implémentées.

Prendre les mesures correctives et préventives appropriées

Le recensement des événements (incident, crise), les retours d'expériences et la réévaluation des risques permettent d'identifier les axes d'améliorations.

Communiquer les résultats et actions, consulter les parties prenantes

La rédaction des risques en mettant en avant les activités critiques concernées et l'impact sur la continuité de l'organisme permet de sensibiliser les acteurs.

S'assurer que les révisions réalisent leurs objectifs prévus

Il convient de définir des indicateurs permettant de s'assurer que les objectifs ont été mis en œuvre.

Annexe 5 – Contenu d'un plan de continuité type et exemples

Le déclenchement de plans de continuité permet de mettre en place des procédures métier ou support (informatique, logistique, télécommunication) pour assurer un niveau de service acceptable pour l'organisme.

Le PCA référence l'ensemble des plans de continuité.

Les différents types de procédures mise en œuvre par le plan de continuité

Un plan de continuité permet de déclencher un ensemble de procédures ayant pour objectif réduire l'impact d'un événement.

Un plan de continuité peut comporter 3 types de procédures :

- Les procédures d'urgences (ou fiches réflexes)

Procédures à mettre en œuvre immédiatement après l'alerte d'incident ou de crise permettant de stabiliser la situation afin de réduire les impacts du risque.

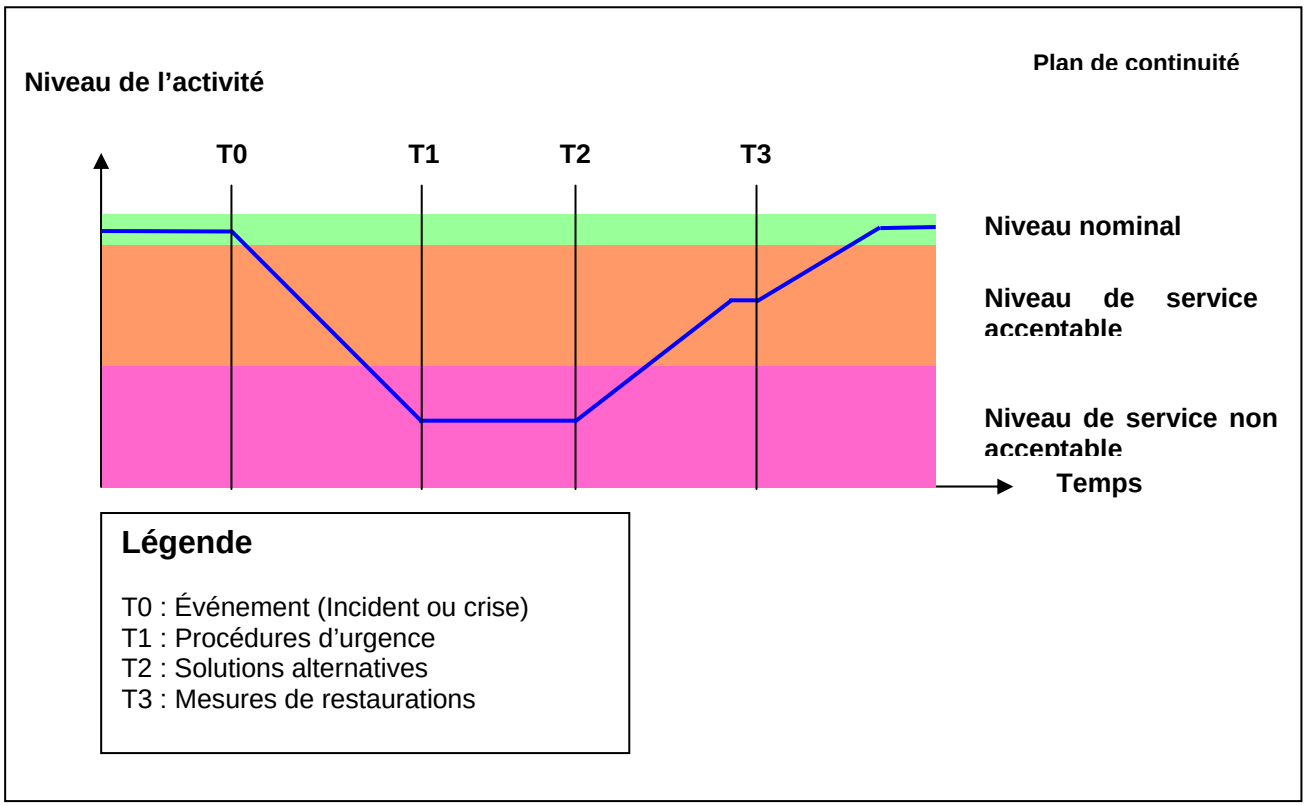
- Les solutions alternatives

Procédures permettant, une fois la situation stabilisée par d'assurer la continuité de l'activité une solution alternative à un niveau de reprise acceptable (RSO), préalablement défini dans l'analyse des impacts d'activité (BIA).

- Les procédures de restauration

Ces procédures réalisées après l'incident ou la crise, permettent de revenir au niveau normal de fonctionnement de l'activité. Ces actions doivent être mises à jour régulièrement en fonction des tests, audits, et dans le cas où la cible changerait au cours du temps et que le BIA est redéfini.

Le schéma suivant décrit le déclenchement des différents types de procédures relatives à un plan de continuité au cours du temps.



Contenu d'un plan type

Le continu d'un plan de continuité des activités est :

- Le risque (menace et besoins de sécurité des activités critiques concernées)
- Le niveau de continuité
- Les procédures d'escalade (extrait de la procédure d'escalade globale)
  - Les listes des contrôles à effectuer (check-list)
  - Les conditions de mise en œuvre
  - Les indicateurs correspondants
- Les acteurs (extrait de l'annuaire de plan de continuité)
  - Le responsable du plan de continuité
  - Les délégations de responsabilité en cas d'indisponibilité
  - Les personnes impliquées dans :
    - le comite de crise
    - la cellule de coordination
    - les équipes opérationnelles
  - Les contacts externes à l'organisme :
    - police, mairie, pompier…
    - fournisseurs
    - clients
    - presse
- Les procédures d'urgences (ou fiches réflexes) et/ou
- Les solutions alternatives et/ou
- Les procédures de restauration
- Les ressources nécessaires au plan (exemples : documentation technique, références fabricant pour un matériel, sources pour un logiciel, documentation interne, sauvegardes sur bandes, serveur de secours…)
  - Lieu de stockage
  - Procédures de mise en place (installation, configuration, déploiement…)
  - Références fournisseurs
  - Les documents-types
- Les plans de continuité dépendants
  - Autres plans de continuité à activer selon des conditions définies
  - Plan de communication éventuel
  - Plan de sensibilisation et de formation correspondant
  - Le journal de suivi des tests
  - Retour d'expérience, commentaires et date du dernier test
  - Date et personne responsable des prochains tests
- Le journal de suivi des opérations de maintenance
  - Mise à jour du BIA et des plans de continuité à chaque évolution du contexte
    - Retour d'expérience
    - Changement organisationnel
    - Remplacement des ressources du SI
    - Émergence de nouveaux métiers dans l'entreprise
    - Évolution des risques
    - …

***Proformae* de plan de continuité**

Plan de continuité – TITRE			
Niveau de continuité			
Risque			
Entités	Vulnérabilités concernées		
Activités	Besoins en continuité		
Impacts sur l'organisme			
Procédures d'escalade			
Contrôles à effectuer			
Conditions d'activation du plan			
Indicateurs			
Les acteurs			
Responsable du plan de continuité			
Suppléant			
Comité de crise			
Cellule de coordination			
Équipe opérationnelle			
Contacts externes			
Police/Mairie…			
Fournisseurs			
Clients			
Presse			
Procédures			
Procédures d'urgence	Mesures	Ressources	Acteurs
Solutions alternatives	Mesures	Ressources	Acteurs
Procédures de restauration	Mesures	Ressources	Acteurs
Plans de continuité associés			
Journal de suivi des tests			
Derniers tests			
Date	Visa responsable	Portée du test	Compte-rendu
Prochain test			
Date	Visa responsable	Portée du test	Objectif à atteindre
Journal de suivi des opérations de maintenance			
Date	Visa responsable	Éléments modifiés	Compte-rendu

Des exemples de plans de continuité des activités

Dans le domaine de la SSI, les plans de continuité les plus utilisés sont :

- le plan de restauration des activités économiques,

Procédures définissant les restaurations d'activés économiques après un incident ou une crise. Il est également appelé BRP (*Business Recovery Plan*).

- le plan de continuité métier,

Le plan de continuité métier définit les procédures alternatives (par exemple au format papier) à mettre en œuvre pour assurer des fonctions métiers critiques de l'organisme au cours d'un incident ou une crise pendant laquelle le SI n'est plus disponible.

- le plan d'urgence,

Procédures à mettre en œuvre immédiatement après l'alerte d'incident ou de crise permettant de stabiliser la situation afin de réduire les impacts du risque.

- le plan de secours informatique et de télécommunication,

Procédures permettant d'atténuer les impacts sur les systèmes d'information par exemple après un acte de malveillance.

- le plan de communication de crise interne et externe,

Le plan de communication est composé d'une communication interne pour le personnel et d'une communication externe pour le public, les clients, les fournisseurs, les autorités gouvernementales afin de faciliter la circulation des informations en interne et de faire taire les rumeurs. Les procédures du plan de communication de crise doivent être coordonnées avec tous les autres plans. Des trames pour la presse peuvent être rédigées dans le plan.

- le plan de gestion de crise,

Le plan de gestion de crise se concentre sur la restauration des fonctions essentielles de l'organisation à partir du centre de gestion de crise et du site alternatif et exécute ces fonctions jusqu'à 30 jours avant de revenir à une situation normale. Ce plan concerne les missions de l'organisation jugées les plus critiques et ne se concentre pas sur les technologies de l'information. Ce plan prend en compte les procédures nécessaires à la mise en place du centre de gestion de crise et éventuellement du site alternatif.

- le plan de recouvrement de crise.

Le plan de recouvrement de crise se concentre sur les technologies de l'information. Il se limite aux crises majeures nécessitant une relocalisation et ayant des effets à long terme. Ce plan fournit des procédures détaillées pour faciliter le recours à des ressources d'un site alternatif. Il est activé après un incident, le temps de retrouver une situation normale.

Dans d'autres domaines, on peut trouver :

- le plan relatif à la santé du personnel,

Procédures permettant d'assurer la sécurité et l'évacuation du personnel en cas de risque sur leur santé tel qu'un incendie, une inondation, une urgence médicale, une attaque virale…

- le plan relatif à la propriété.

Procédures permettant de couvrir un risque portent atteinte à la propriété du personnel tel qu'une attaque criminelle, un vol, une grève…

Le tableau suivant indique la(les) période(s) lors de laquelle chaque plan est activé :

Plans	Pendant	Après
Plan relatif à la propriété	X	
Plan relatif à la santé et à la sécurité des employés	X	
Plan d'urgence	X	
Plan de restauration des activités économiques		X
Plan de continuité métier	X	
Plan de secours informatiques	X	X
Plan de communication de crise interne et externe	X	X
Plan de gestion de crise	X	X
Plan de recouvrement de crise		X

Annexe 6 – L'annuaire

L'annuaire doit contenir des informations sur les utilisateurs internes à l'organisme mais également sur l'ensemble des acteurs externes susceptibles de jouer un rôle dans la gestion de la continuité des activités comme les prestataires, les fournisseurs, les clients, les pompiers, le SAMU, la police, la mairie, la préfecture pour les ministères, les opérateurs de services publics...

L'annuaire contient des informations sensibles. Cependant, la gestion de la continuité des activités nécessite une publication de l'annuaire à l'ensemble des acteurs. Il est donc recommandé de ne mettre dans l'annuaire que les informations strictement nécessaires.

Informations nécessaires à la gestion de crise

Il peut être intéressant au sein de l'annuaire d'identifier pour chacun des acteurs :

- la proximité de son domicile vis-à-vis de son lieu de travail,
- la disponibilité d'un véhicule personnel,
- la disponibilité prévisible en cas de fermeture des établissements scolaires,
- sa capacité à utiliser le réseau Internet depuis son domicile (télétravail),
- ses compétences au regard des missions et fonctions prioritaires à assurer, notamment en cas d'activation du site alternatif,
- les postes qu'il pourrait occuper dans une situation dégradée.

Mises à jour de l'annuaire

Il est recommandé d'identifier un responsable chargé de mettre à jour l'annuaire à chaque changement organisationnel. Un mécanisme de synchronisation des annuaires, automatique ou manuel doit ainsi être mis en place entre l'annuaire source et l'ensemble des copies de l'annuaire sous format électronique ou papier.

Recherche dans l'annuaire

La cellule de veille est chargée de classifier l'incident, de donner l'alerte et d'identifier les acteurs concernés en cas d'incident ou de crise. Elle aura quelques difficultés en évaluant les dégâts à identifier le scénario complet du risque que l'organisme est en train de subir. Seul une partie du risque sera visible, comme par exemple les entités concernées (serveur, pare-feu, salle machines…), les impacts (perturbation du réseau, incapacité à rendre le service…), cependant, la vulnérabilité exploitée ou l'élément menaçant ne seront peut être pas clairement identifiés. Une recherche multi critères sur l'annuaire, par composante du risque, permettrait d'identifier les risques potentiellement concernés et les plans de continuité susceptibles de correspondre à l'événement subi.

***Proformae* d'annuaire**

Il est important de spécifier pour chaque acteur les rôles au sein de l'organisation de crise, et pour chaque plan de continuité auquel il est rattaché.

La présence d'une ligne téléphonique fixe ou d'un poste de messagerie n'étant pas garantie, les coordonnées doivent indiquer les différents moyens de communication afin de pouvoir joindre efficacement les acteurs en cas d'incident ou de crise.

Les annuaires doivent également renseigner les contacts d'astreintes et de permanences.

Une entrée de l'annuaire peut correspondre parfois non pas à une personne mais à une fonction, notamment dans le monde militaire.

Chaque acteur est décrit par une fiche contenant les informations suivantes :

Fiche personnel				
Civilité	Nom	Prénom	Nom complet	Grade
Téléphonie				
Moyen clair				
Téléphone Fixe	Téléphone mobile	Télécopie		
Moyen chiffrant				
Téléphone Fixe	Téléphone mobile	Télécopie		
Moyens spéciaux				
Téléphone fixe personnel	Téléphone mobile personnel	Téléphone par satellite	Téléphone sur RIM	Visioconférence
Messagerie				
Messagerie Internet	Messagerie Intranet	Messagerie formelle	Adresse télégraphique	
Web				
Site Web sur internet	Site Web sur intranet			
Rôle				
Nom du plan de continuité	Rôles dans le plan de continuité	Suppléant	Domaine d'expertise ou d'intervention	Planning d'astreinte et de permanence
Rôles en temps de crise				
Organisation				
Nom de l'organisme	Nom du service	Secteur d'activité	Fonction dans le service	
Responsable hiérarchique	Adjoint	Adresse	Couverture géographique	

Annexe 7 – Les tableaux de bord

Le guide [TDBSSI] présente la démarche nécessaire à l'élaboration d'indicateurs constitutifs d'un tableau de bord à partir d'objectifs ou d'exigences de sécurité.

Un indicateur est constitué d'un ensemble de données sources sur la base desquelles peuvent être définis un calcul et une représentation graphique. Des valeurs cible et seuil ainsi qu'une plage de tolérance facilitent l'interprétation de l'indicateur par la personne ayant la responsabilité d'activer les plans de continuité associés.

Les indicateurs peuvent être de nature différente. La suite du chapitre présente, par type d'indicateur le rôle de chaque acteur par niveau hiérarchique.

- Suivi de la mise en œuvre d'une mesure amont (mesure de prévention, protection ou de détection) ou d'un plan de continuité des activités

  1. Niveau opérationnel

     Plusieurs équipes opérationnelles peuvent être nécessaires pour mettre en œuvre une mesure amont ou élaborer un plan de continuité. Chaque équipe est alors chargée de tenir informé le niveau pilotage des actions dont ils ont la charge.

  2. Niveau pilotage

     Sur la base des indicateurs de niveau opérationnel, le responsable des mesures PSSI et les responsables des plans de continuité supervisent l'avancement des différentes équipes concernées.

     Les responsables des plans de continuité doivent tenir informé le comité de crise et le gestionnaire des plans de continuité de l'évolution de la construction du PCA en alimentant des indicateurs de niveau pilotage.

  3. Niveau stratégique

     Le gestionnaire des plans de continuité et le comité de crise tiennent informé la direction de l'avancement du SGCA.

- Mesurer l'efficacité du SGCA

  1. Niveau opérationnel

     Les équipes techniques et la cellule de veille alimentent des indicateurs de niveau opérationnel présentant un historique des incidents et crise.

  2. Niveau pilotage

     Les indicateurs de niveau opérationnel permettent au responsable des mesures PSSI d'apprécier l'efficacité des mesures amont (prévention, protection, détection) en fonction des incidents survenus. Ces indicateurs permettent aux responsables des plans de continuités d'estimer les conséquences d'un plan sur un évènement.

     Ils alimentent des indicateurs de niveau de pilotage permettant au gestionnaire des plans de continuité et au comité de crise de percevoir l'efficacité du SGCA en vue d'améliorer les processus, les mesures, les plans… Par exemple, lorsqu'un incident apparait trop fréquent, il peut s'avérer pertinent de mettre en œuvre une mesure de protection plutôt qu'un plan de réaction.

  3. Niveau stratégique

     Le gestionnaire des plans de continuité et le comité de crise tiennent informé la direction de l'efficacité du SGCA.

- Supervision de l'évolution d'un incident ou d'une crise

  1. Niveau opérationnel

  Il est conseillé de définir les indicateurs de niveau opérationnels sur la base d'objectifs exprimant la volonté de couverture d'un risque technique, physique ou organisationnel. Les données sources peuvent être alimentées par des techniciens à partir de remontées de journaux. La cellule de veille en est le destinataire.

  2. Niveau pilotage

  La cellule de veille est en charge de surveiller les indicateurs de niveau pilotage et alerte, en fonction de l'événement, le gestionnaire d'incident ou le comité de crise.

  Les responsables des plans de continuité peuvent alimenter les indicateurs de niveau pilotage pour tenir informé le gestionnaire d'incident ou le comité de crise de l'évolution de la situation. Cependant, il est difficile de suivre une crise sur la base d'un tableau de bord. L'utilisation d'un tableau de bord n'apparaît réaliste qu'une fois le niveau de service acceptable assuré. Il permet dans ce cadre de suivre le niveau de continuité par activité et l'évolution des procédures de restauration.

  3. Niveau stratégique

  Le niveau stratégique permet de visualiser le niveau de sécurité global de l'organisme et de suivre le niveau de fonctionnement de chaque activité essentielle de l'organisme. Au niveau stratégique, les indicateurs sont alimentés par le gestionnaire d'incident et le comité de crise ainsi que par les responsables de chaque activité métier essentielle de l'organisme.

  Au niveau stratégique, un indicateur représentant le niveau de continuité de l'organisme peut se référer à l'échelle du *chapitre 1.4 Les niveaux de continuité : le baromètre de l'organisme*.

Les destinataires du tableau de bord SSI doivent être identifiés en amont afin de leur proposer un tableau de bord adapté. De même, les responsables de l'indicateur et des données sources doivent être impliquées au plus tôt afin de faire vivre l'indicateur.

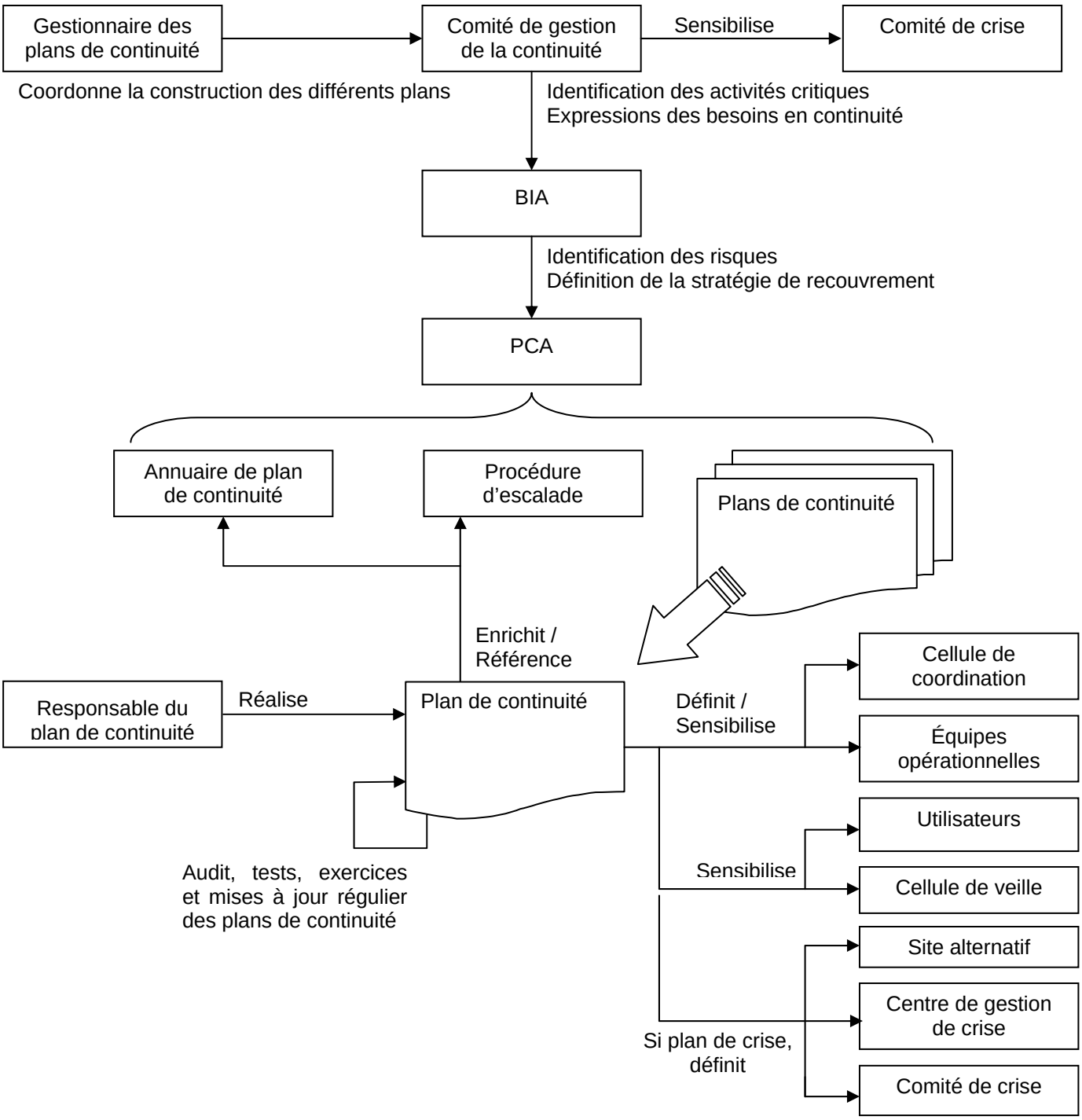
Les indicateurs doivent être documentés et maintenus à jour au niveau des procédures d'escalade du plan de continuité des activités (PCA).

Annexe 8 – Les interactions entre les acteurs de gestion de la continuité des activités

La communication entre acteurs doit être encouragée.

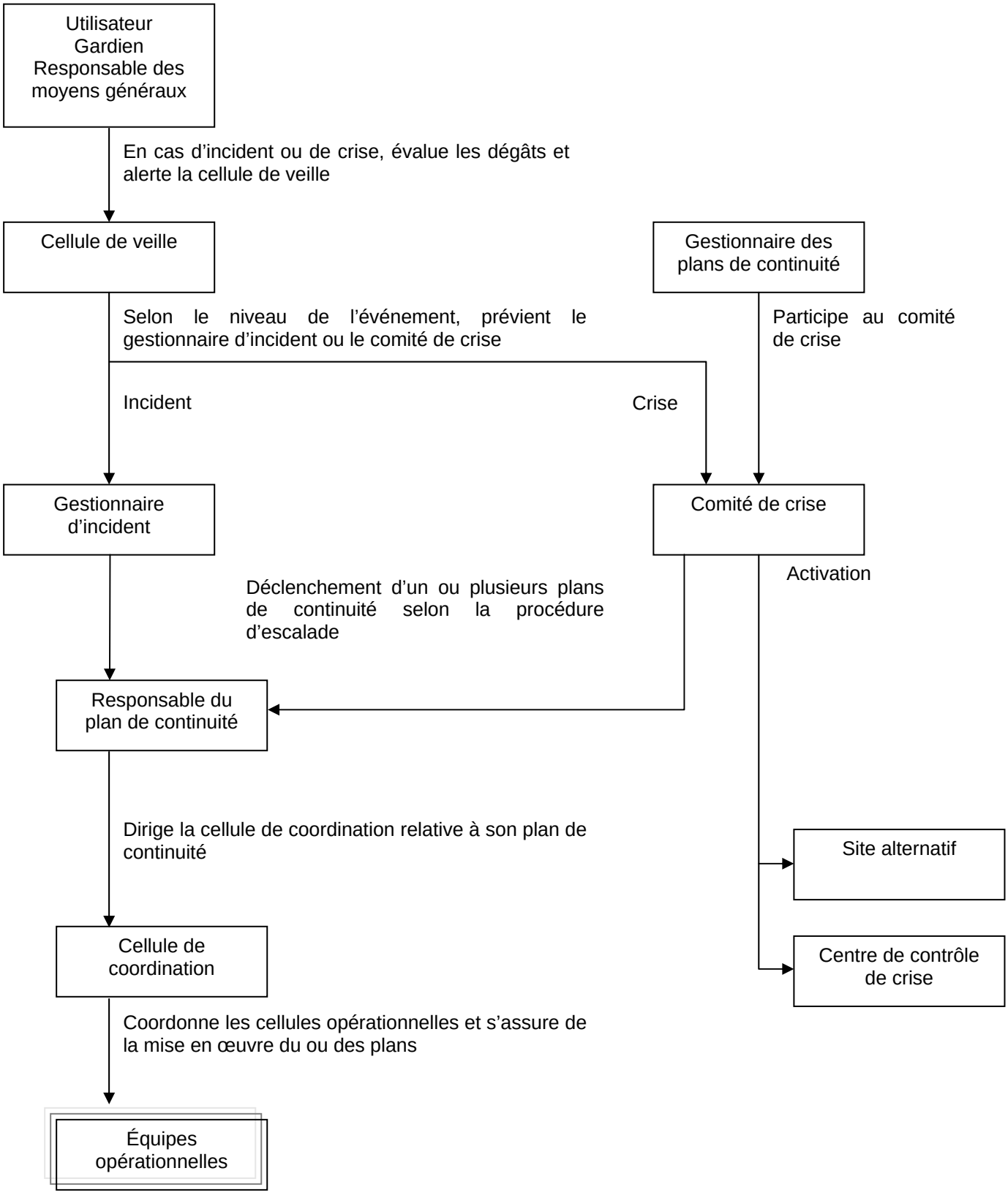
Gestion du PCA

L'élaboration du plan de continuité des activités est une opération complexe nécessitant une charge de travail importante de la part des acteurs concernés. Le schéma suivant présente les interactions entre les différents acteurs nécessaires à la création et au maintient du PCA.



Gestion d'un incident ou d'une crise

Le schéma suivant présente les interactions entre acteurs nécessaires à la gestion d'un incident ou d'une crise au sein d'un organisme.



Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Club EBIOS
72 avenue Gaston Boissier
78220 VIROFLAY
contact[at]club-ebios.org

Identification de la contribution
Nom et organisme (facultatif) :
Adresse électronique :
Date :

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :

Quels autres sujets souhaiteriez-vous voir traiter ?

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution