V.1.0

Réponse à incident

Séquence 3 : Plan de continuité et reprise d'activité

OIDANEOS

ISO 22301 et SMCA

Présentation de l'ISO

ISO 22300:2021 – Sécurité et résilience - Vocabulaire

ISO 22301:2019 – Sécurité et résilience – Système de management de la continuité d'activité – Exigences

ISO 22313:2020 – Sécurité et résilience – Système de management de la continuité d'activité – Lignes directrices sur l'utilisation de l'ISO 22301

ISO 22317:2021 – Sécurité et résilience – Système de management de la continuité d'activité – Lignes directrices pour le bilan d'impact sur l'activité

ISO 22318:2021 – Sécurité et résilience – Système de management de la continuité d'activité – Lignes directrices pour le management de la continuité de la chaîne d'approvisionnement

ISO/TS 22330:2018 – Sécurité et résilience – Système de management de la continuité d'activité – Lignes directrices concernant les aspects humains de la poursuite de l'activité

ISO/TS 22331:2018 – Sécurité et résilience – Système de management de la continuité d'activité – Lignes directrices relative à la stratégie de la continuité d'activité

ISO/TS 22332:2021 – Sécurité et résilience – Système de management de la continuité d'activité – Lignes directrices pour le développement des plans et des procédures de continuité d'activité

Le principe d'un système de management

Un système de management est un ensemble d'éléments corrélés ou interactifs d'un organisme visant à établir des politiques, des objectifs et des processus permettant d'atteindre ces objectifs

ISO/IEC 27000, article 3.41

Situation actuelle « *As-is* »

- Qualité
- Sécurité de l'information
- Management environnemental
- …

Mise en œuvre d'un système de management

Politiques

Objectifs

Processus

- Prise en compte de la structure, des rôles et responsabilités, de la planification et des opérations de l'organisme
- Le domaine du S.M. peut être une partie de l'organisme ou son intégralité

Situation à atteindre

- Qualité
- Sécurité de l'information
- Management environnemental
- …

Le principe d'un système de management

Les caractéristiques clés d'un système de management :

- Accountability
- Répétabilité des processus
- Documentation
- Ressources
- Mesure des performances et mécanismes de revues
- Gestion de la compétence
- Changement culturel

Le principe d'un système de management

Les composants d'un système de management :

- Politique et autre documentation
- Implication de la direction
- Prise en compte du contexte et des obligations
- Gestion des ressources
- Gestion de la communication
- Formation et sensibilisation
- Evaluation de la performance et audit
- Actions correctives des non-conformités
- Revue de la direction
- Amélioration continue

Le système de management de la continuité d'activité

L'ISO 22301 « Sécurité et résilience – Systèmes de management de la continuité d'activité – Exigences » permet de :

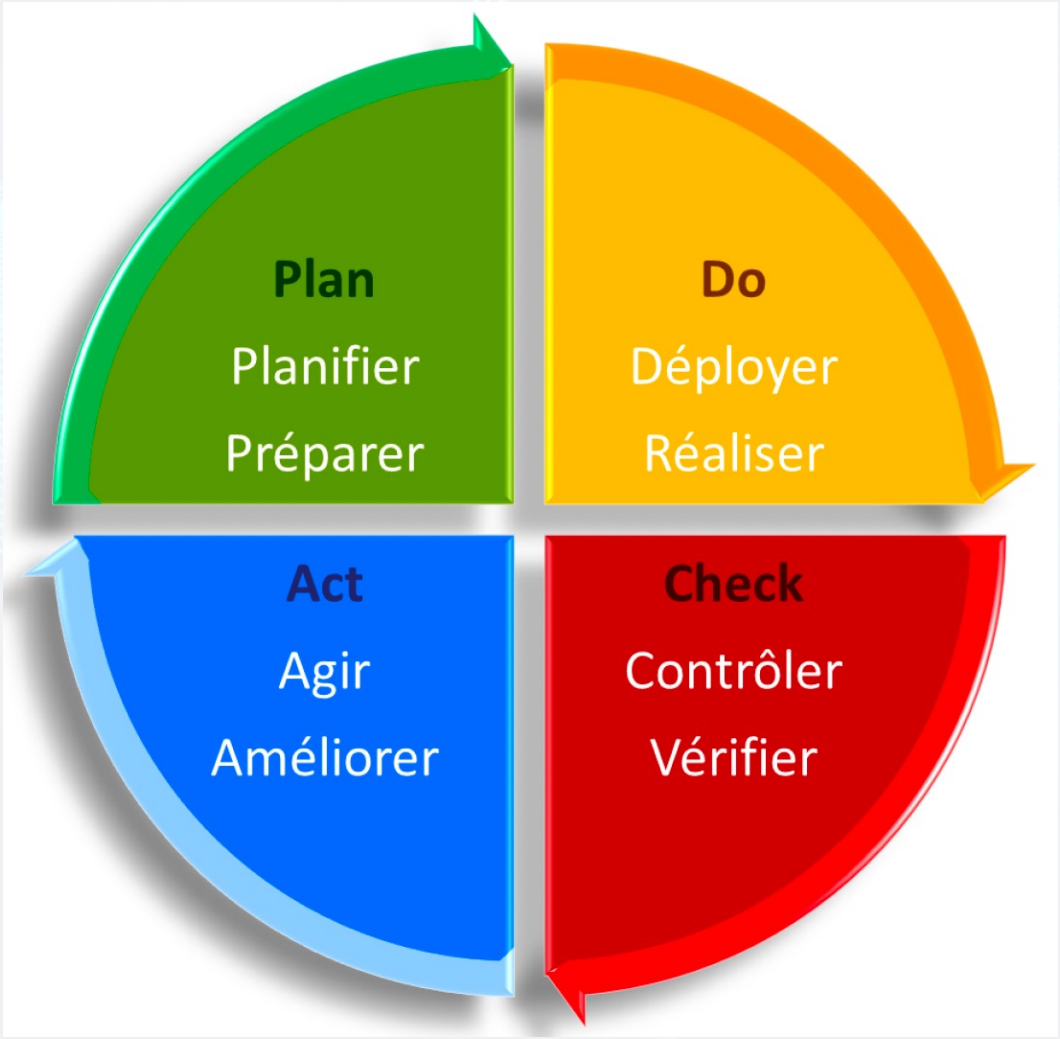
- Clarifier les attendus concernant la continuité d'activité
- Aligner la continuité d'activité sur la stratégie d'entreprise
- Obtenir l'engagement de la direction
- Simplifier la complexité d'un PCA
- S'intégrer dans la démarche de gestion des risques de l'entreprise
- Adresser de multiples sources de besoins et d'obligations
- Adopter une vision « programme » et pas simplement « projet »

Les chapitres de la norme

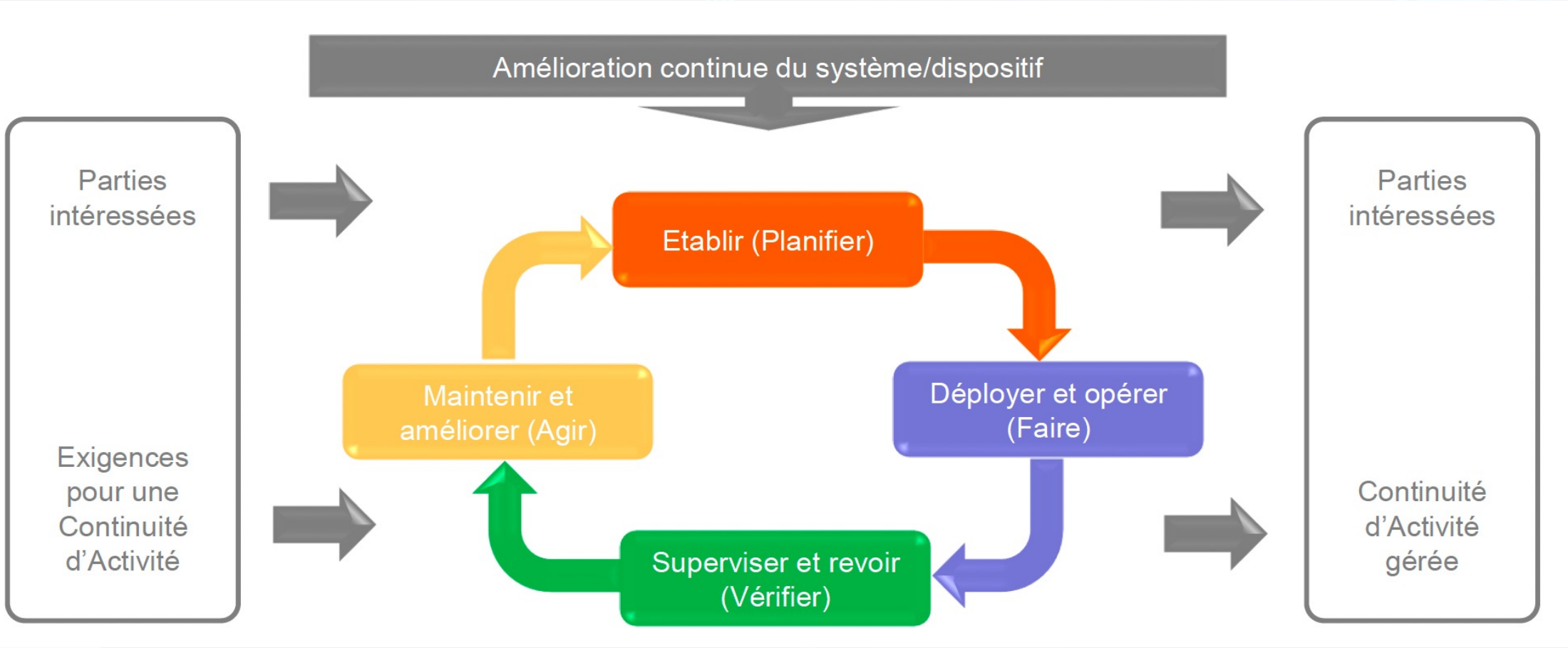
1. Domaine d'application
2. Références normatives
3. Termes et définitions
4. Contexte de l'organisation
5. Leadership
6. Planification
7. Support
8. Fonctionnement
9. Evaluation de la performance
10. Amélioration

EXIGENCES

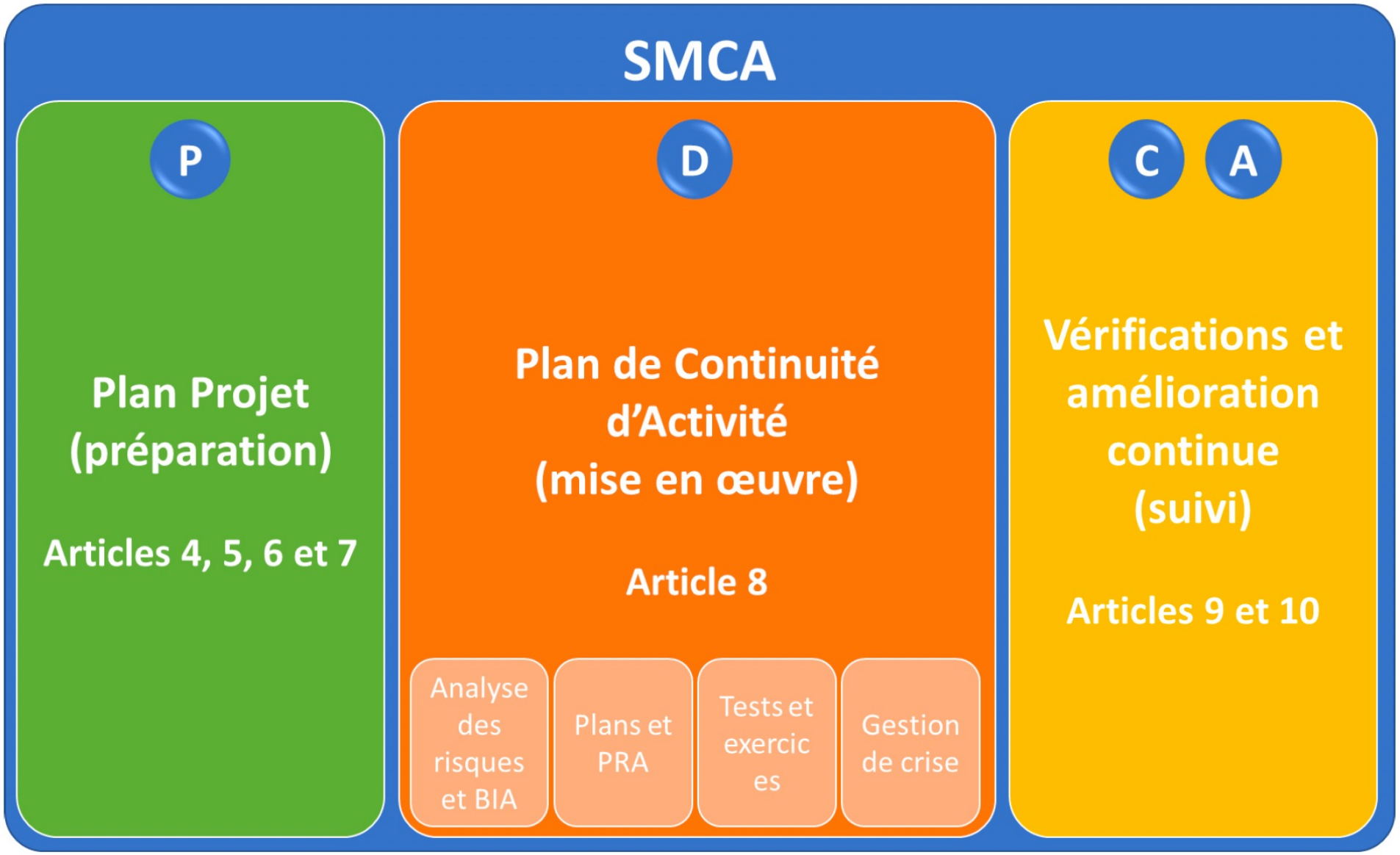
La démarche PDCA



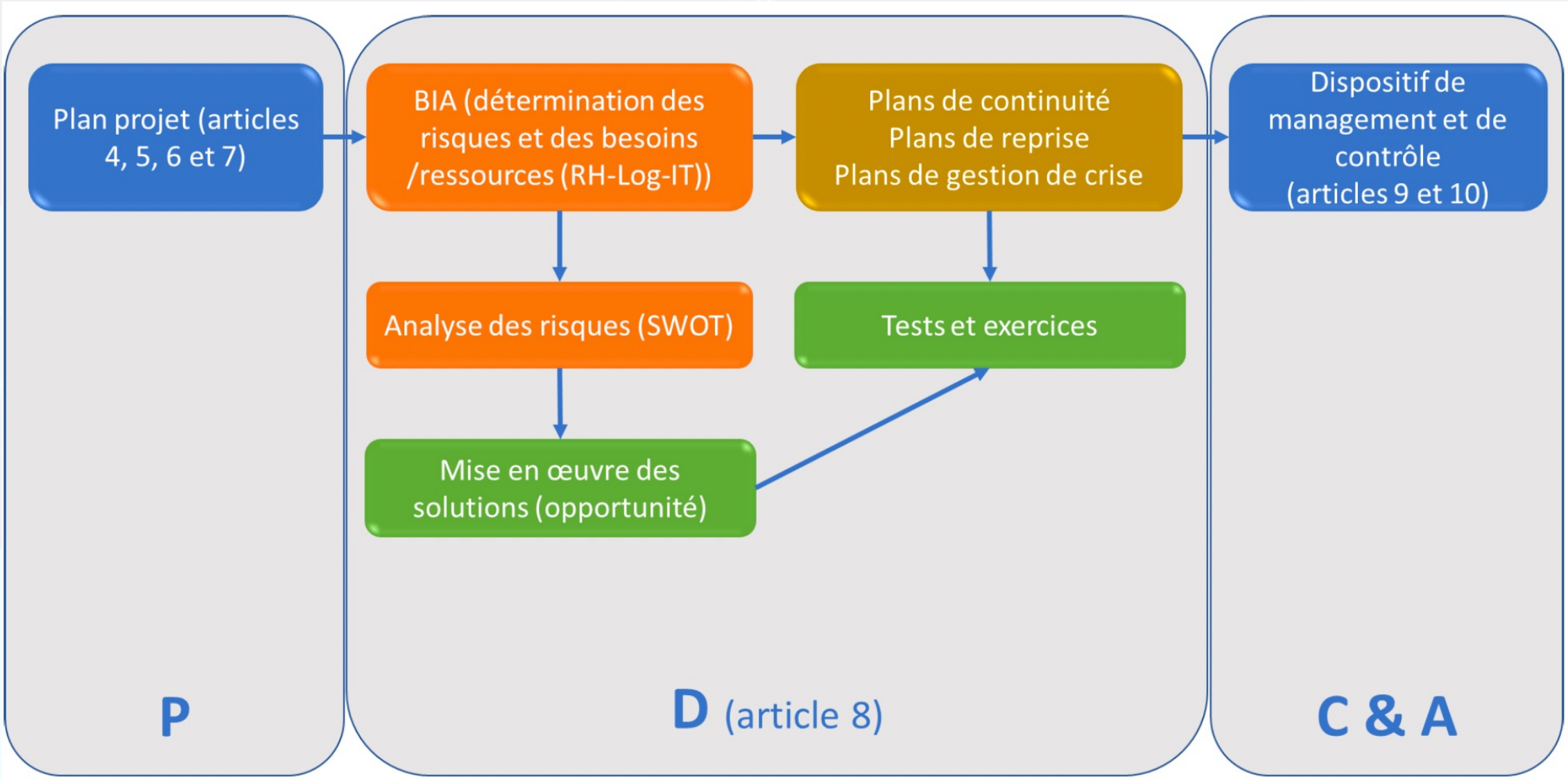
La démarche PDCA



La démarche PDCA



La démarche PDCA



1. Domaine d'application

- Exigences pour **mettre en œuvre, maintenir et améliorer** un système de management afin de se **protéger contre les perturbations**, réduire la vraisemblance de leur survenance, s'y préparer et répondre et se rétablir lorsqu'elles se produisent

- Norme applicable à **tous les types et toutes les tailles d'organismes** qui :
  - *Mettent en œuvre, maintiennent et améliorent un SMCA ;*
  - *Cherchent à assurer la conformité à la politique de continuité d'activité déclarée ;*
  - *Ont besoin d'être aptes à poursuivre la livraison de produits et la fourniture de services à un niveau de capacité acceptable et préalablement défini durant une perturbation*
  - *Cherchent à améliorer leur résilience à travers l'application efficace du SMCA*

- Norme utilisable pour **apprécier l'aptitude** d'un organisme à satisfaire ses propres besoins et obligations en matière de continuité d'activité

3. Termes et définitions

Associez le bon terme à la bonne définition

3. Termes et définitions

1. Continuité d'activité	A. Incident, anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la livraison de produits et à la fourniture de services prévues selon les objectifs d'un organisme
2. Organisme (ou organisation)	B. Résultat à atteindre
3. Produit et service	C. Élément de sortie ou résultat fourni par un organisme au bénéfice des parties intéressées
4. Perturbation	D. Informations documentées servant de guide à un organisme pour répondre à une perturbation et reprendre, rétablir et restaurer la livraison de produits et la fourniture de services en cohérence avec ses objectifs de continuité d'activité
5. Incident	E. Événement qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise
6. Plan de Continuité d'Activité	F. Processus d'analyse de l'impact dans le temps d'une perturbation sur l'organisme
7. Impact	G. Capacité d'un organisme à poursuivre la livraison de produits et la fourniture de services dans des délais acceptables à une capacité prédéfinie durant une perturbation
8. Objectif	H. Personne ou groupe de personnes ayant ses propres fonctions, avec des responsabilités, des autorités et des relations lui permettant d'atteindre ses objectifs
9. Bilan d'impact sur l'activité	I. Résultat d'une perturbation affectant les objectifs

3. Termes et définitions

Continuité d'activité

Organisme (ou organisation)

Produit et service

Perturbation

Incident

Plan de Continuité d'Activité

Impact

Objectif

Bilan d'impact sur l'activité

Incident, anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la livraison de produits et à la fourniture de services prévues selon les objectifs d'un organisme

Résultat à atteindre

Élément de sortie ou résultat fourni par un organisme au bénéfice des parties intéressées

Informations documentées servant de guide à un organisme pour répondre à une perturbation et reprendre, rétablir et restaurer la livraison de produits et la fourniture de services en cohérence avec ses objectifs de continuité d'activité

Événement qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise

Processus d'analyse de l'impact dans le temps d'une perturbation sur l'organisme

Capacité d'un organisme à poursuivre la livraison de produits et la fourniture de services dans des délais acceptables à une capacité prédéfinie durant une perturbation

Personne ou groupe de personnes ayant ses propres fonctions, avec des responsabilités, des autorités et des relations lui permettant d'atteindre ses objectifs

Résultat d'une perturbation affectant les objectifs

4. Contexte de l'organisme

Ce que dit la norme ISO :

4.1. Compréhension de l'organisme et de son contexte

L'organisme doit déterminer les questions externes et internes pertinentes par rapport à sa finalité, et qui affectent sa capacité à atteindre le ou les résultats attendus de son SMCA.

4.2. Compréhension des besoins et attentes des parties intéressées

4.2.1. Généralités

Lors de l'établissement de son SMCA, l'organisme doit déterminer :

a) Les parties intéressées qui sont pertinentes pour le SMCA ;
b) Les exigences de ces parties intéressées

4.2.2. Exigences règlementaires et juridiques

L'organisme doit:

a) mettre en œuvre et maintenir un processus lui permettant d'identifier les exigences réglementaires et juridiques concernant la continuité de ses produits et services, activités et ressources, d'y avoir accès et de les évaluer ;
b) s'assurer que les exigences réglementaires et juridiques ou autres, applicables, sont prises en compte lorsqu'il met en œuvre et maintient son SMCA ;
c) documenter ces informations et les tenir à jour.

4. Contexte de l'organisme

Ce que dit la norme ISO :

4.3. Détermination du domaine d'application du SMCA

4.3.1. Généralités

Pour établir le domaine d'application du SMCA, l'organisme doit en déterminer les limites et l'applicabilité. Lorsqu'il établit ce domaine d'application, il doit prendre en compte :

a) *les questions externes auxquelles il est fait référence en 4.1 ;*
b) *les exigences auxquelles il est fait référence en 4.2 ;*
c) *sa mission, ses buts et ses obligations internes et externes.*

Le domaine d'application doit être disponible sous forme documentée

4.3.2. Domaine d'application du SMCA

L'organisme doit:

a) *établir les parties de l'organisme à inclure dans le SMCA, en prenant en compte leurs emplacements, taille, nature et complexité ;*
b) *Identifier les produits et services à inclure dans le SMCA*

Lors de la définition du domaine d'application, l'organisme doit documenter et expliquer les exclusions. Elles ne doivent pas affecter l'aptitude et la responsabilité de l'organisme à assurer la continuité de l'activité, tel que déterminé par le bilan d'impact sur l'activité ou l'appréciation du risque et par les exigences réglementaires ou juridiques applicables

4. Contexte de l'organisme

Ce que dit la norme ISO :

4.4. Système de management de la continuité d'activité

L'organisme doit établir, mettre en œuvre, maintenir et continuellement améliorer un SMCA, incluant les processus nécessaires et leurs interactions, en accord avec les exigences du présent document.

4. Contexte de l'organisation

- Un SMCA doit prendre en compte :
  - Les exigences légales, règlementaires et contractuelles
  - Les parties prenantes internes et externes qui ont un intérêt dans les efforts de CA
  - Les objectifs stratégiques, les politiques, priorités et appétits du risque de l'entreprise
- Cette partie permet d'avoir les informations fondamentales nécessaires pour établir un périmètre approprié et définir les objectifs
- Il faut :
  - Passer en revue la documentation
  - Discuter avec la direction
  - Identifier les produits et services
  - Définir l'appétit du risque

5. Leadership

Ce que dit la norme ISO :

5.1. Leadership et engagement

La Direction générale doit démontrer son leadership et son engagement en faveur du SMCA en :

a) s'assurant que la politique et les objectifs de continuité d'activité sont établis et qu'ils sont compatibles avec l'orientation stratégique de l'organisme ;
b) s'assurant que les exigences du SMCA sont intégrées aux processus métier de l'organisme ;
c) s'assurant que les ressources nécessaires pour le SMCA sont disponibles;
d) communiquant sur l'importance d'une continuité d'activité efficace et de se conformer aux exigences du SMCA;
e) s'assurant que le SMCA atteint le ou les résultats escomptés;
f) orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du SMCA;
g) Promouvant l'amélioration continue;
h) aidant les autres managers concernés à démontrer leur leadership et leur engagement dès lors que cela s'applique à leurs domaines de responsabilité

NOTE : Dans le présent document, il est possible d'interpréter le terme «activité» de façon large, c'est-à-dire comme se référant aux activités qui sont au cœur des finalités de l'existence de l'organisme

5. Leadership

Ce que dit la norme ISO :

5.2. Politique

5.2.1. Établissement de la politique de continuité d'activité

La Direction générale doit établir une politique de continuité d'activité qui :

a) est appropriée à la mission de l'organisme;
b) fournit un cadre pour l'établissement d'objectifs de continuité d'activité;
c) inclut l'engagement de satisfaire aux exigences applicables;
d) inclut l'engagement d'amélioration continue du SMCA.

5.2.2. Communication de la politique de continuité d'activité

La politique de continuité d'activité doit :

a) être disponible sous forme d'information documentée;
b) être communiquée au sein de l'organisme;
c) être à la disposition des parties intéressées, comme approprié

5.3. Rôles, responsabilités et autorités

La Direction générale doit s'assurer que les responsabilités et autorités pour les rôles pertinents sont attribuées et communiquées au sein de l'organisme. La Direction générale doit désigner qui a la responsabilité et l'autorité de:

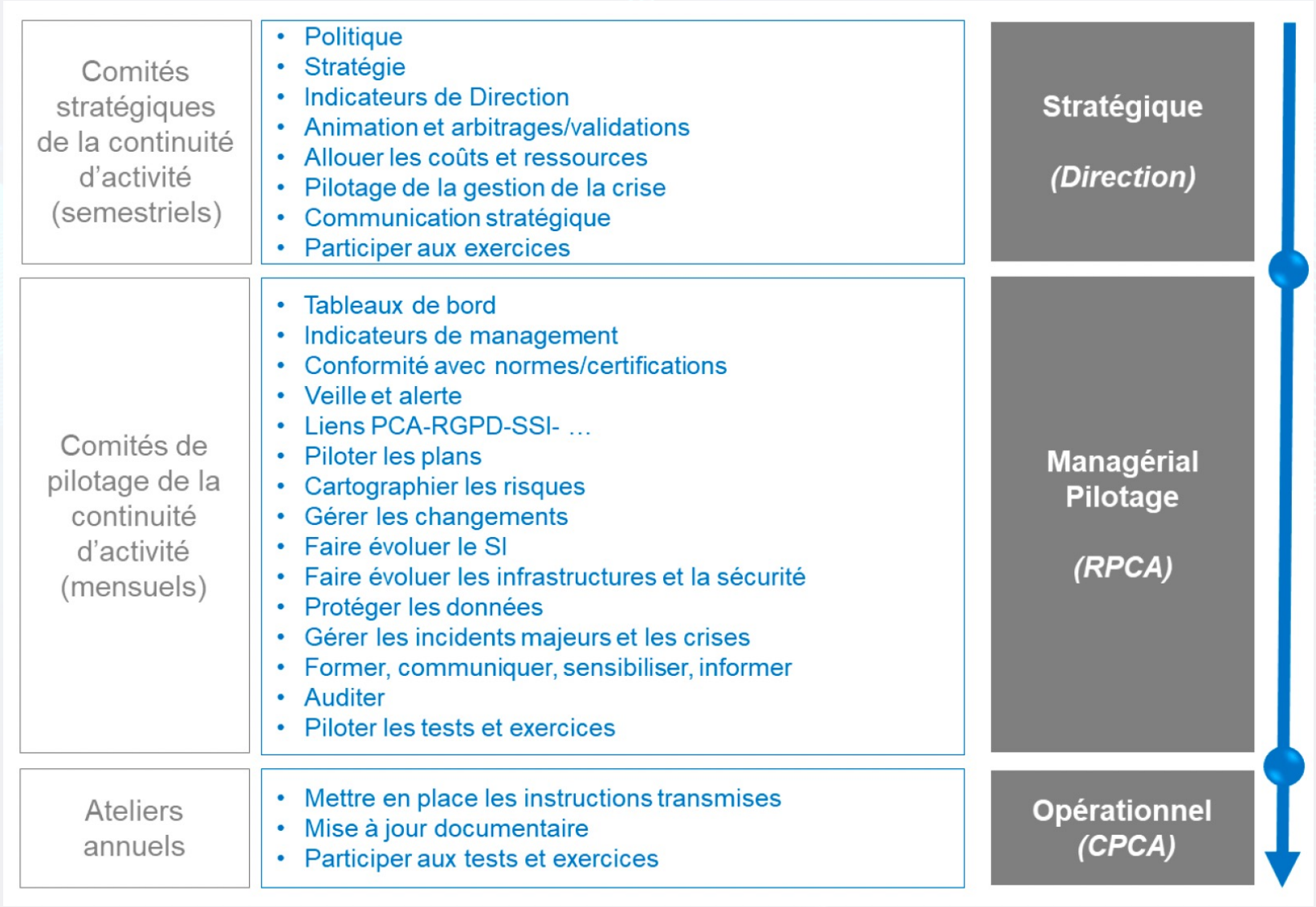
a) s'assurer que le SMCA est conforme aux exigences du présent document;
b) rendre compte à la Direction générale de la performance du SMCA

5. Leadership

- Un SMCA doit inclure :
  - Une politique de continuité d'activité
  - Une définition des rôles, responsabilités et autorités

- Il faut :
  - Etablir un comité de pilotage de la continuité d'activité
  - Créer la politique de continuité d'activité
  - Définir les rôles et responsabilités avec notamment un sponsor, un coordinateur

5. Leadership



6. Planification

Ce que dit la norme ISO :

6.1. Actions faces aux risques et opportunités

6.1.1. Détermination des risques et opportunités

Lorsqu'il conçoit son SMCA, l'organisme doit prendre en considération les questions auxquelles il est fait référence en 4.1 et les exigences auxquelles il est fait référence en 4.2 et déterminer les risques et opportunités auxquels il faut faire face pour:

a) *fournir l'assurance que le SMCA peut atteindre le ou les résultats escomptés;*
b) *empêcher ou limiter les effets indésirables; et*
c) *obtenir une démarche d'amélioration continue*

6.1.2. Gestion des risques et opportunités

L'organisme doit planifier:

a) *les actions à mener face aux risques et opportunités;*
b) *la manière: 1) d'intégrer et de mettre en œuvre ces actions au sein des processus du SMCA (voir 8.1); et 2) d'évaluer l'efficacité de ces actions (voir 9.1*).

NOTE Les risques et opportunités se rapportent à l'efficacité du système de management. Les risques liés à une perturbation de l'activité relèvent du 8.2

6. Planification

Ce que dit la norme ISO :

6.2. Objectifs de continuité d'activité et planification pour les atteindre

6.2.1. Établissement des objectifs de continuité d'activité

L'organisme doit établir les objectifs de continuité d'activité aux fonctions et niveaux pertinents. Les objectifs de continuité d'activité doivent:

a) être cohérents avec la politique de continuité d'activité;
b) être mesurables (si possible);
c) prendre en compte les exigences applicables (voir 4.1 et 4.2);
d) être surveillés;
e) être communiqués;
f) être mis à jour comme approprié.

L'organisme doit conserver des informations documentées sur les objectifs de continuité d'activité.

6.2.2. Détermination des objectifs de continuité d'activité

Lorsque l'organisme planifie la façon d'atteindre ses objectifs de continuité d'activité, l'organisme doit déterminer:

a) ce qui sera fait;
b) quelles ressources seront requises
c) qui sera responsable;
d) à quelle échéance;
e) comment les résultats seront évalués.

6. Planification

Ce que dit la norme ISO :

6.3. Planification des modifications du SMCA

Lorsque l'organisme détermine le besoin d'apporter des modifications au SMCA, y compris celles identifiées à l'Article 10, les modifications doivent être réalisées de façon planifiée. L'organisme doit prendre en considération:

a) *l'objet des modifications et leurs conséquences potentielles;*
b) *l'intégrité du SMCA;*
c) *la disponibilité des ressources;*
d) *l'attribution ou la réattribution des responsabilités et autorités*

6. Planification

- Définir des objectifs de continuité d'activité
  - Exemple :
    - Assurer la sécurité des employés et des visiteurs de la société ABC
    - Gérer les menaces et les impacts associés à une interruption des opérations critiques
    - Réduire les risques en matière de continuité d'activité en mettant en place des contrôles appropriés et proactifs pour diminuer la probabilité d'un événement perturbateur, une stratégie de gestion de crise, des plans pour avoir une résilience des métiers critiques selon les attentes des parties prenantes et la capacité à maintenir une communication avec le personnel et les clients
- Avoir un alignement avec :
  - Les autres disciplines de gestion des risques
  - La culture d'entreprise

7. Support

Ce que dit la norme ISO :

7.1. Ressources

L'organisme doit déterminer et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la maintenance et l'amélioration continue du SMCA.

7.2. Compétences

L'organisme doit :

a) *déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui affecte ses performances de continuité d'activité;*
b) *s'assurer que ces personnes sont compétentes sur la base d'une formation initiale, d'une formation professionnelle ou d'une expérience appropriée;*
c) *le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité des actions entreprises;*
d) *conserver des informations documentées appropriées comme preuves de ces compétences.*

NOTE Les actions envisageables peuvent par exemple inclure la formation, l'encadrement ou la réaffectation du personnel actuellement en activité ou le recrutement, direct ou en sous-traitance, de personnes compétentes.

7. Support

Ce que dit la norme ISO :

7.3. Sensibilisation

Les personnes effectuant un travail sous le contrôle de l'organisme doivent avoir conscience:

a) de la politique de continuité d'activité;
b) de leur contribution à l'efficacité du SMCA, y compris les bénéfices d'une amélioration des performances de la continuité d'activité;
c) des implications de la non-conformité aux exigences du SMCA;
d) de leurs propres rôle et responsabilités, durant et après des perturbations

7.4. Communication

L'organisme doit déterminer les éléments de communication interne et externe pertinents pour le SMCA, et notamment:

a) sur quoi communiquer;
b) quand communiquer;
c) avec qui communiquer;
d) comment communiquer;
e) qui communiquera

7. Support

Ce que dit la norme ISO :

7.5. Informations documentées

7.5.1. Généralités

Le SMCA de l'organisme doit inclure:

a) les informations documentées exigées par le présent document;

b) les informations documentées que l'organisme juge nécessaires à l'efficacité du SMCA.

NOTE L'étendue des informations documentées dans le cadre d'un SMCA peut différer selon l'organisme en fonction de: — la taille de l'organisme, ses domaines d'activité, ses processus, produits et services, et ses ressources; — la complexité des processus et de leurs interactions; — les compétences des personnes.

7.5.2. Création et mise à jour

Quand il crée et met à jour ses informations documentées, l'organisme doit s'assurer que sont appropriés:

a) l'identification et la description (par exemple titre, date, auteur, numéro de référence);

b) le format (par exemple langue, version logicielle, graphiques) et le support (par exemple papier, électronique);

c) la revue et l'approbation du caractère adapté et adéquat des informations

7. Support

Ce que dit la norme ISO :

7.5. Informations documentées

7.5.3. Maîtrise des informations documentées

7.5.3.1. Les informations documentées exigées par le SMCA et par le présent document doivent être maîtrisées pour s'assurer:

a) *qu'elles soient disponibles et propres à être utilisées, où et quand c'est nécessaire;*
b) *qu'elles sont convenablement protégées (par exemple contre la perte de confidentialité, l'utilisation inappropriée ou la perte d'intégrité)*

7.5.3.2 Pour maîtriser les informations documentées, l'organisme doit s'occuper des activités suivantes, quand elles lui sont applicables:

a) *distribution, accès, récupération et utilisation*
b) *stockage et préservation, y compris préservation de la lisibilité;*
c) *maîtrise des modifications (par exemple maîtrise des versions);*
d) *conservation et élimination des informations.*

Les informations documentées d'origine externe que l'organisme juge nécessaires à la planification et au fonctionnement du SMCA doivent être identifiées, le cas échéant, et maîtrisées.

NOTE L'accès peut impliquer une décision concernant l'autorisation de consulter les informations documentées uniquement, ou l'autorisation et l'autorité de consulter et modifier les informations documentées

7. Support

- Détailler les procédures opérationnelles standards (SOP)
- Créer un programme d'évaluation et de développement des compétences
- Développer un plan de communication
- Créer un plan de sensibilisation
- Implémenter la gestion documentaire

8. Gestion des opérations

Ce que dit la norme ISO :

8.1. Planification opérationnelle et maîtrise

L'organisme doit planifier, mettre en œuvre et maîtriser les processus nécessaires pour satisfaire aux exigences et réaliser les actions déterminées en 6.1, en:

a) *établissant les critères pour ces processus;*
b) *mettant en œuvre la maîtrise de ces processus en accord avec ces critères;*
c) *conservant des informations documentées pour être en mesure de montrer que les processus ont été menés comme prévu.*

L'organisme doit maîtriser les modifications prévues et passer en revue les conséquences des modifications non intentionnelles, si nécessaire en menant des actions pour limiter tout effet adverse. L'organisme doit s'assurer que les processus externalisés et la chaîne d'approvisionnement sont maîtrisés

8. Gestion des opérations

Ce que dit la norme ISO :

8.2. Bilan d'impact sur l'activité et appréciation du risque

8.2.1 Généralités

L'organisme doit:

a) mettre en œuvre et maintenir des processus systématiques pour le bilan d'impact sur l'activité et l'appréciation des risques de perturbation;

b) passer en revue le bilan d'impact sur l'activité et l'appréciation du risque à des intervalles planifiés et lorsque des changements significatifs interviennent au sein de l'organisme ou dans le contexte dans lequel il opère.

NOTE L'organisme détermine l'ordre dans lequel le bilan d'impact sur l'activité et l'appréciation du risque sont effectués.

8. Gestion des opérations

Ce que dit la norme ISO :

8.2. Bilan d'impact sur l'activité et appréciation du risque

8.2.2 Bilan d'impact sur l'activité de l'organisme

L'organisme doit utiliser le processus de bilan d'impact sur l'activité afin de déterminer les priorités et les exigences de continuité d'activité. Le processus doit:

a) définir les types d'impacts et les critères pertinents pour le contexte de l'organisme;

b) identifier les activités qui supportent la livraison des produits et la fourniture des services;

c) utiliser les types d'impacts et les critères pour apprécier les impacts dans le temps découlant de la perturbation de ces activités

d) identifier la durée au-delà de laquelle les impacts d'une non-reprise de ces activités deviendraient inacceptables pour l'organisme;

NOTE 1 Ce délai peut être appelé «durée maximale tolérable de perturbation (DMTP)».

e) déterminer les délais par ordre de priorité à l'intérieur de la durée identifiée en

d) pour reprendre les activités perturbées avec une capacité minimale acceptable spécifiée;

NOTE 2 Ce délai peut être désigné comme «objectif de délai de rétablissement (RTO)».

f) utiliser ce bilan pour identifier les activités prioritaires;

g) déterminer quelles ressources sont nécessaires pour soutenir les activités prioritaires;

h) déterminer les dépendances, y compris les partenaires et fournisseurs, et interdépendances des activités prioritaires

8. Gestion des opérations

Ce que dit la norme ISO :

8.2. Bilan d'impact sur l'activité et appréciation du risque

8.2.3. Appréciation du risque

L'organisme doit mettre en œuvre et maintenir un processus d'appréciation du risque. L'organisme doit:

a) identifier les risques de perturbation pour les activités prioritaires de l'organisme, ainsi que pour les ressources requises;
b) analyser et évaluer les risques identifiés;
c) déterminer quels risques exigent un traitement.

NOTE 2 Les risques dans ce paragraphe se rapportent à la perturbation des activités métier. Les risques et opportunités liés à l'efficacité du système de management relèvent du 6.1

8.3. Stratégies et solutions de continuité d'activité

8.3.1 Généralités

En se basant sur les éléments de sortie du bilan d'impact sur l'activité et de l'appréciation du risque, l'organisme doit identifier et sélectionner des stratégies de continuité d'activité qui prennent en compte des options pour avant, pendant et après une perturbation. Les stratégies de continuité d'activité doivent comprendre une ou plusieurs solutions.

8. Gestion des opérations

Ce que dit la norme ISO :

8.3. Stratégies et solutions de continuité d'activité

8.3.2 Identification des stratégies et solutions

L'identification doit prendre en considération dans quelle mesure les stratégies et solutions:

a) *satisfont aux exigences pour poursuivre et rétablir les activités prioritaires dans les délais identifiés et au niveau de capacité convenu;*
b) *protègent les activités prioritaires de l'organisme;*
c) *réduisent la vraisemblance des perturbations;*
d) *raccourcissent la période de perturbation;*
e) *limitent l'impact de la perturbation sur les produits et services de l'organisme;*
f) *assurent la disponibilité des ressources adéquates*

8.3.3. Sélection des stratégies et solutions

La sélection doit prendre en considération dans quelle mesure les stratégies et solutions:

a) *satisfont aux exigences pour poursuivre et rétablir les activités prioritaires dans les délais identifiés et au niveau de capacité convenu;*
b) *prennent en compte la quantité et le type de risque que l'organisme peut prendre ou non;*
c) *prennent en compte les coûts et bénéfices associés.*

8. Gestion des opérations

Ce que dit la norme ISO :

8.3. Stratégies et solutions de continuité d'activité

8.3.4 Exigences de ressources

L'organisme doit déterminer les exigences de ressources pour mettre en œuvre les solutions de continuité d'activité sélectionnées. Les types de ressources considérés doivent comprendre, sans toutefois s'y limiter:

a) les personnes;
b) les informations et les données;
c) l'infrastructure physique telle que les bâtiments, les lieux de travail ou d'autres installations et les utilités associées;
d) les équipements et les consommables;
e) les systèmes de technologies de l'information et de la communication (TIC);
f) le transport et la logistique;
g) le financement;
h) les partenaires et fournisseurs.

8.3.5 Mise en œuvre des solutions

L'organisme doit mettre en œuvre et maintenir les solutions de continuité d'activité afin qu'elles puissent être activées quand c'est nécessaire

8. Gestion des opérations

Ce que dit la norme ISO :

8.4. Plans et procédures de continuité d'activité

8.4.1. Généralités

L'organisme doit mettre en œuvre et maintenir une structure de réponse qui permettra d'avertir les parties intéressées pertinentes et de communiquer avec elles en temps opportun. Il doit fournir des plans et procédures pour gérer l'organisme durant une perturbation. Les plans et procédures doivent être utilisés quand c'est nécessaire pour activer les solutions de continuité d'activité.

NOTE Il existe différents types de procédures qui constituent les plans de continuité d'activité

L'organisme doit identifier et documenter les plans et procédures de continuité d'activité en se basant sur les éléments de sortie des stratégies et solutions retenues. Les procédures doivent:

a) être précises concernant les mesures immédiates devant être prises durant une perturbation;
b) être souples pour répondre aux changements de conditions internes et externes d'une perturbation;
c) se concentrer sur l'impact d'incidents menant potentiellement à une perturbation;
d) être efficaces pour réduire l'impact au minimum par la mise en œuvre de solutions appropriées
e) attribuer des rôles et responsabilités pour les tâches qu'elles présentent.

8. Gestion des opérations

Ce que dit la norme ISO :

8.4. Plans et procédures de continuité d'activité

8.4.2. Structure de réponse

8.4.2.1 L'organisme doit mettre en œuvre et maintenir une structure identifiant une ou plusieurs équipes chargées de répondre aux perturbations.

8.4.2.2 Les rôles et responsabilités de chaque équipe et les relations entre les équipes doivent être clairement établis.

8.4.2.3.Les équipes doivent être collectivement compétentes pour:

a) apprécier la nature et l'étendue d'une perturbation ainsi que son impact potentiel;
b) apprécier l'impact par rapport aux seuils prédéfinis justifiant le lancement initial d'une réponse formelle;
c) activer une réponse appropriée pour la continuité d'activité;
d) planifier les actions à entreprendre;
e) établir des priorités (en considérant la sécurité de la vie des personnes comme la première priorité);
f) surveiller les effets de la perturbation et la réponse de l'organisme;
g) activer les solutions de continuité d'activité;
h) communiquer avec les parties intéressées pertinentes, les autorités et les médias.

8.4.2.4 Chaque équipe doit avoir:

a) un personnel identifié et ses suppléants, avec la responsabilité, l'autorité et la compétence nécessaires pour exercer le rôle qui leur est attribué;

b) des procédures documentées afin de guider ses actions (voir 8.4.4), y compris celles destinées à l'activation, au fonctionnement, à la coordination et à la communication de la réponse

8. Gestion des opérations

Ce que dit la norme ISO :

8.4. Plans et procédures de continuité d'activité

8.4.3. Avertissement et communication

8.4.3.1 L'organisme doit documenter et maintenir des procédures pour:
a) communiquer en interne et en externe avec les parties intéressées pertinentes, y compris quoi, quand, avec qui et comment communiquer;

NOTE L'organisme peut documenter et maintenir des procédures concernant la manière et les circonstances dans lesquelles l'organisme communique avec les employés et les personnes à contacter en cas d'urgence

b) gérer la réception, la documentation et la réponse aux communications provenant des parties intéressées, y compris un système de conseil national ou régional sur les risques ou un système équivalent;
c) assurer la disponibilité des moyens de communication durant une perturbation;
d) faciliter une communication structurée avec les services d'urgence;
e) fournir les détails de la réponse de l'organisme aux médias à la suite d'un incident, y compris une stratégie de communications;
f) effectuer l'enregistrement des détails de la perturbation, des actions réalisées et des décisions prises.

8. Gestion des opérations

Ce que dit la norme ISO :

8.4. Plans et procédures de continuité d'activité

8.4.3. Avertissement et communication

8.4.3.2 Le cas échéant, les éléments suivants doivent également être considérés et mis en œuvre:
a) alerter les parties intéressées potentiellement impactées par une perturbation réelle ou imminente;
b) assurer une coordination et une communication appropriées entre de multiples organismes participant à la réponse.

Les procédures d'avertissement et de communication doivent faire l'objet d'exercices dans le cadre du programme d'exercice de l'organisme décrit en 8.5

8.4.4. Plans de continuité d'activité

8.4.4.1 L'organisme doit documenter et maintenir ses plans et procédures de continuité d'activité.
Les plans de continuité d'activité doivent fournir des recommandations et des informations qui aideront les équipes à répondre à une perturbation et aideront l'organisme à répondre et à se rétablir.

8. Gestion des opérations

Ce que dit la norme ISO :

8.4. Plans et procédures de continuité d'activité

8.4.4. Plans de continuité d'activité

8.4.4.2 Les plans de continuité d'activité doivent globalement contenir:

a) les détails des actions que les équipes accompliront afin de:
   1) continuer ou rétablir les activités prioritaires dans des délais prédéterminés;
   2) surveiller l'impact de la perturbation et la réponse de l'organisme à celle-ci;

b) la référence au(x) seuil(s) prédéfini(s) et au processus visant à activer la réponse;

c) les procédures permettant la livraison des produits et la fourniture des services au niveau de capacité convenu;

d) les détails permettant de gérer les conséquences immédiates d'une perturbation en tenant dûment compte:
   1) du bien-être des individus;
   2) de la prévention d'une perte ou indisponibilité supplémentaire d'activités prioritaires;
   3) de l'impact sur l'environnement

8. Gestion des opérations

Ce que dit la norme ISO :

8.4. Plans et procédures de continuité d'activité

8.4.4. Plans de continuité d'activité

8.4.4.3 Chaque plan doit inclure:

a) le but, le domaine d'application et les objectifs;
b) les rôles et les responsabilités de l'équipe qui mettra en œuvre le plan;
c) les actions pour mettre en œuvre les solutions;
d) les informations d'appui nécessaires pour activer (y compris les critères d'activation), mettre en œuvre, coordonner et communiquer les actions de l'équipe;
e) les interdépendances internes et externes;
f) les exigences de ressources;
g) les exigences de compte rendu;
h) un processus de sortie.

Chaque plan doit être utilisable et disponible au moment et à l'endroit auxquels il est requis

8.4.5. Rétablissement

L'organisme doit disposer de processus documentés pour restaurer et revenir à ses activités métier à partir des mesures temporaires adoptées pendant et après une perturbation

8. Gestion des opérations

Ce que dit la norme ISO :

8.5. Programme d'exercices

L'organisme doit mettre en œuvre et maintenir un programme d'exercices et de tests afin de valider dans le temps l'efficacité de ses stratégies et solutions de continuité d'activité. L'organisme doit mener des exercices et des tests qui:

a) sont cohérents avec ses objectifs de continuité d'activité;
b) sont basés sur des scénarios appropriés qui sont bien planifiés avec des buts et des objectifs clairement définis;
c) développent le travail d'équipe, les compétences, la confiance et les connaissances des personnes qui ont des rôles à jouer en lien avec les perturbations;
d) cumulés au fil du temps, valident ses stratégies et solutions de continuité d'activité;
e) permettent de produire des rapports post-exercices formalisés contenant les résultats, les recommandations et les actions pour mettre en œuvre des améliorations;
f) sont passés en revue dans le contexte de l'effort d'amélioration continue;
g) sont menés à des intervalles planifiés et lorsque des changements significatifs interviennent au sein de l'organisme ou dans le contexte dans lequel il opère.
h) L'organisme doit agir en fonction des résultats de ses exercices et tests pour mettre en œuvre des modifications et améliorations

8. Gestion des opérations

Ce que dit la norme ISO :

8.6. Évaluation de la documentation et des capacités de continuité d'activité

L'organisme doit:

a) évaluer l'adaptation, l'adéquation et l'efficacité de son bilan d'impact sur l'activité, son appréciation des risques, ses stratégies, ses solutions, ses plans et ses procédures;
b) réaliser ses évaluations par le biais de revues, d'analyses, d'exercices, de tests, de rapports post incident et d'évaluations des performances;
c) soumettre à évaluation les capacités de continuité d'activité des partenaires et fournisseurs appropriés;
d) évaluer la conformité aux exigences réglementaires et juridiques applicables, aux meilleures pratiques de son secteur ainsi que la conformité à sa propre politique de continuité d'activité et aux objectifs associés;
e) mettre à jour la documentation et les procédures en temps opportun.

Ces évaluations doivent être réalisées à des intervalles planifiés, après un incident ou une activation, et lorsque des changements significatifs interviennent

8. Gestion des opérations

9. Évaluation de la performance

Ce que dit la norme ISO :

9.1. Surveillance, mesurage, analyse et évaluation

L'organisme doit déterminer:

a) ce qu'il est nécessaire de surveiller et mesurer;
b) les méthodes de surveillance, de mesurage, d'analyse et d'évaluation, selon les cas, pour assurer la validité des résultats;
c) quand et par qui la surveillance et le mesurage doivent être effectués;
d) quand et par qui les résultats de la surveillance et du mesurage doivent être analysés et évalués.

L'organisme doit conserver des informations documentées appropriées comme preuves des résultats. L'organisme doit évaluer la performance et l'efficacité du SMCA

9. Évaluation de la performance

Ce que dit la norme ISO :

9.2. Audit interne

9.2.1. Généralités

L'organisme doit réaliser des audits internes à des intervalles planifiés afin de fournir des informations permettant de déterminer si le SMCA:

a) est conforme:
   1) aux exigences propres de l'organisme concernant son SMCA;
   2) aux exigences du présent document;

b) est efficacement mis en œuvre et maintenu.

9.2.2. Programmes d'audit

L'organisme doit :

a) planifier, établir, mettre en œuvre et maintenir un programme d'audit, couvrant notamment la fréquence, les méthodes, les responsabilités, les exigences de planification et le compte rendu. Le programme d'audit doit tenir compte de l'importance des processus concernés et des résultats des audits précédents;
b) définir les critères d'audit et le périmètre de chaque audit;
c) sélectionner des auditeurs et réaliser des audits pour assurer l'objectivité et l'impartialité du processus d'audit;
d) s'assurer qu'il est rendu compte des résultats des audits aux managers pertinents;
e) conserver des informations documentées comme preuves de la mise en œuvre du ou des programmes d'audit et des résultats d'audit;
f) s'assurer que toutes les actions correctives nécessaires sont prises sans délai indu pour éliminer les non-conformités détectées ainsi que leurs causes;
g) s'assurer que les actions de suivi incluent la vérification des actions entreprises et le compte rendu des résultats de cette vérification

9. Évaluation de la performance

Ce que dit la norme ISO :

9.3. Revue de direction

9.3.1. Généralités

La Direction générale doit passer en revue le SMCA de l'organisme, à des intervalles planifiés, afin de s'assurer qu'il est toujours adapté, adéquat et efficace.

9.3.2. Éléments d'entrée de la revue de direction

La revue de direction doit prendre en considération:

a) l'état d'avancement des actions décidées lors des revues de direction précédentes;
b) les modifications des questions externes et internes pertinentes pour le SMCA;
c) les informations sur les performances du SMCA, y compris les tendances concernant:
1) les non-conformités et les actions correctives;
2) les résultats de l'évaluation de la surveillance et du mesurage;
3) les résultats des audits;
d) les retours d'information des parties intéressées;
e) le besoin d'apporter des modifications au SMCA, y compris en ce qui concerne la politique et les objectifs;
f) les procédures et les ressources qui pourraient être utilisées dans l'organisme pour améliorer la performance et l'efficacité du SMCA;
g) les informations issues du bilan d'impact sur l'activité et de l'appréciation du risque;
h) les éléments de sortie de l'évaluation de la documentation et des capacités de continuité d'activité (voir 8.6);
i) les risques ou les questions qui n'ont pas été traités de manière appropriée lors d'une précédente appréciation du risque;
j) les leçons tirées et les actions découlant d'incidents évités de justesse et de perturbations;
k) les opportunités pour l'amélioration continue

9. Évaluation de la performance

Ce que dit la norme ISO :

9.3. Revue de direction

9.3.3. Éléments de sortie de la revue de direction

9.3.3.1 Les éléments de sortie de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et à tout besoin d'apporter des modifications au SMCA pour améliorer son efficience et son efficacité, y compris les éléments suivants:

a) les variations apportées au domaine d'application du SMCA;

b) la mise à jour du bilan d'impact sur l'activité, de l'appréciation du risque, des stratégies et solutions de continuité d'activité et des plans de continuité d'activité;

c) la modification des procédures et des moyens de maîtrise pour répondre aux questions internes ou externes qui peuvent impacter le SMCA;

d) la manière dont l'efficacité des moyens de maîtrise sera mesurée

9.3.3.2 L'organisme doit conserver des informations documentées comme preuve des résultats des revues de direction. Il doit:

a) communiquer les résultats de la revue de direction aux parties intéressées pertinentes;

b) entreprendre l'action appropriée en fonction de ces résultats

9. Evaluation de la performance

- Définir des métriques, indicateurs, et tableaux de bords
- Implémenter un processus d'audit interne
- Réaliser des revues de performance
- Identifier et tracer les actions correctives

9. Evaluation de la performance

Moye

Support pour un comité de suivi mensuel

Suivi des risques pouvant amener un crise

Tableau de bord

- Suivi des livrables (étapes, délais, retards, relances, …)
- Suivi de la charge pour les contributeurs de l'organisme
- En tirer des tendances et des points de risques

Indicateurs

- De management : suivi du PCA dans les métiers (trimestriels)
- De gouvernance : suivi des risques par nature (mensuels)
  - *IT (disponibilité, résolution des incidents-problèmes, SSI, …)*
  - *Bâtiments (utilisation capacitaires, résolution incidents-problèmes, …)*
  - *Sécurité (intrusions, résolution incidents-problèmes)*
  - *RH (turnover, …)*
  - *Métiers (réclamations clients, résolution incidents-problèmes, …)*
  - *…*

10. Amélioration

Ce que dit la norme ISO :

10.1. Non-conformité et actions correctives

10.1.1 L'organisation doit déterminer les opportunités d'amélioration et mettre en oeuvre les actions nécessaires pour atteindre les résultats attendus de son SMCA.

10.1.2 Lorsqu'une non-conformité se produit, l'organisme doit:
a) réagir à la non-conformité, et le cas échéant:
1) agir pour la maîtriser et la corriger;
2) faire face aux conséquences;
b) évaluer le besoin d'agir pour éliminer la ou les causes de la non-conformité, de sorte qu'elle ne se reproduise pas ni ne se reproduise ailleurs, en:
1) passant en revue la non-conformité;
2) déterminant les causes de la non-conformité;
3) déterminant si des non-conformités similaires existent ou pourraient potentiellement se produire;
c) mettre en œuvre toute action nécessaire;
d) passer en revue l'efficacité de toute action corrective mise en œuvre;
e) modifier le SMCA si nécessaire.

Les actions correctives doivent être à la mesure des effets des non-conformités rencontrées.

10.1.3 L'organisme doit conserver des informations documentées comme preuves:
a) de la nature des non-conformités et de toutes les actions menées ultérieurement;
b) des résultats de toute action corrective

10. Amélioration

Ce que dit la norme ISO :

10.2. Amélioration continue

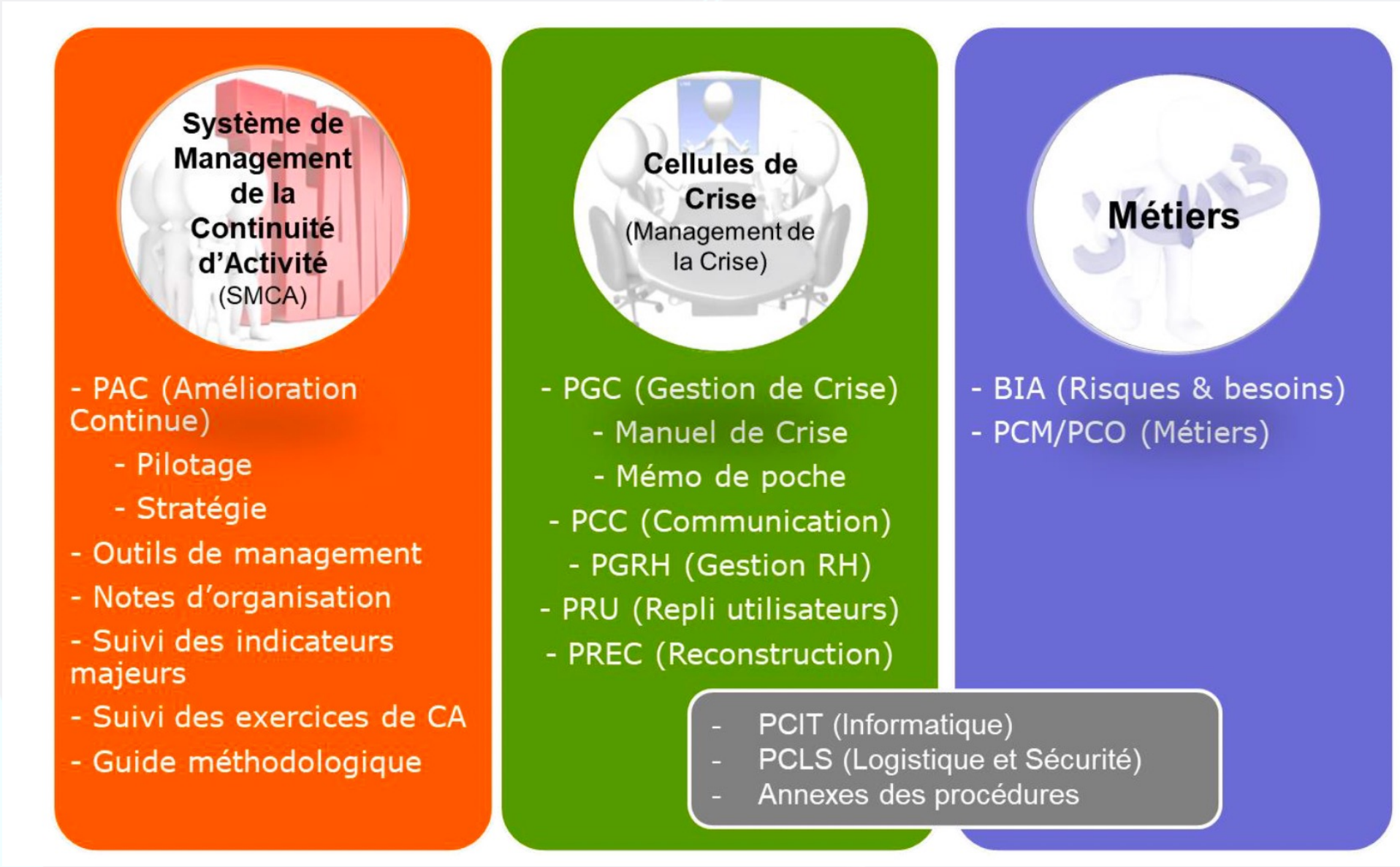
L'organisme doit continuellement améliorer l'adaptation, l'adéquation et l'efficacité du SMCA sur la base de mesures qualitatives et quantitatives. L'organisme doit prendre en considération les résultats de l'analyse et de l'évaluation, ainsi que les éléments de sortie de la revue de direction pour déterminer s'il existe des besoins ou des opportunités, en lien avec l'activité ou avec le SMCA, à considérer dans le cadre de l'amélioration continue.

NOTE L'organisme peut utiliser les processus du SMCA tels que le leadership, la planification et l'évaluation de la performance, afin d'aboutir à une amélioration

10. Amélioration

- Documenter les actions correctives
- Analyser les causes racines
- Réaliser des reporting

Documentation d'un SMCA



Synthèse

Plan (Planifier)

- **Contexte de l'organisation**
  - Enjeux pertinents pour atteindre l'objectif / qui affectent la capacité de l'organisation à atteindre les résultats escomptés de son SMCA
- **Leadership**
  - Leadership Assuré
  - Fait preuve d'un engagement continu envers le système de gestion de continuité de l'activité
  - Synergie avec les objectifs de l'organisation
- **Planification et objectifs**
  - Etablissement d'objectifs stratégiques et des principes directeurs du SMCA
  - Les objectifs d'un système de gestion de la continuité de l'activité sont l'expression de l'intention de l'organisation de traiter les risques identifiés et / ou de se conformer aux exigences des besoins organisationnels
- **Soutien**
  - La gestion au jour le jour d'un système de management de la continuité efficace repose sur l'utilisation des ressources

➔ Créer le plan de réalisation du dispositif de gestion de crise et de continuité d'activité
➔ Mettre en place un environnement durablement favorable

Do (Déployer)

- **Activité**
  - Après avoir planifié le SMCA, une organisation doit le mettre en opération

➔ Mettre en place le PCA et l'organisation de gestion de crise

Check (Contrôler)

- **Evaluation**
  - Un suivi permanent ainsi que des réexamens périodiques destinés à améliorer son fonctionnement sont planifiés et mis en œuvre

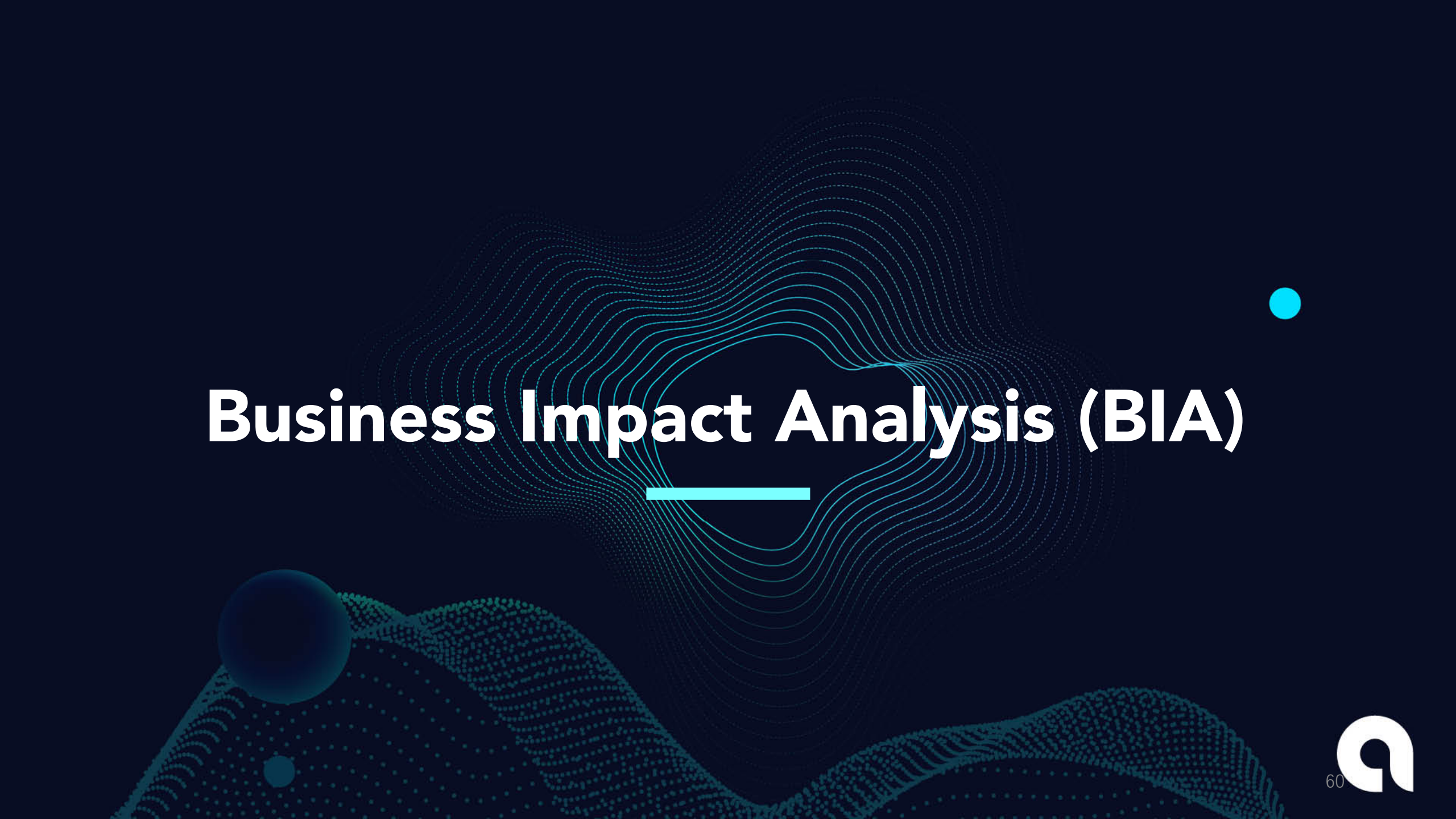
➔ Mettre en place le suivi permanent

Act (Agir)

- **Amélioration**
  - Ensemble des mesures prises dans toute l'organisation pour accroître l'efficacité (atteinte des objectifs) et de l'efficience (un rapport optimal de coût / bénéfice) des processus et des mesures afin d'apporter des avantages accrus pour l'organisation et ses parties prenantes

➔ Faire évoluer le PCA et l'organisation avec l'entreprise et améliorer le dispositif

Business Impact Analysis (BIA)



Business Impact Analysis (BIA)

Objectifs de la démarche de BIA

Comprendre **les produits et les services clés de l'entreprise**, et les activités qui permettent de les traiter

Déterminer **les priorités et les délais** de reprise des activités

Identifier **les ressources / moyens et les dépendances** nécessaires à la continuité d'activité

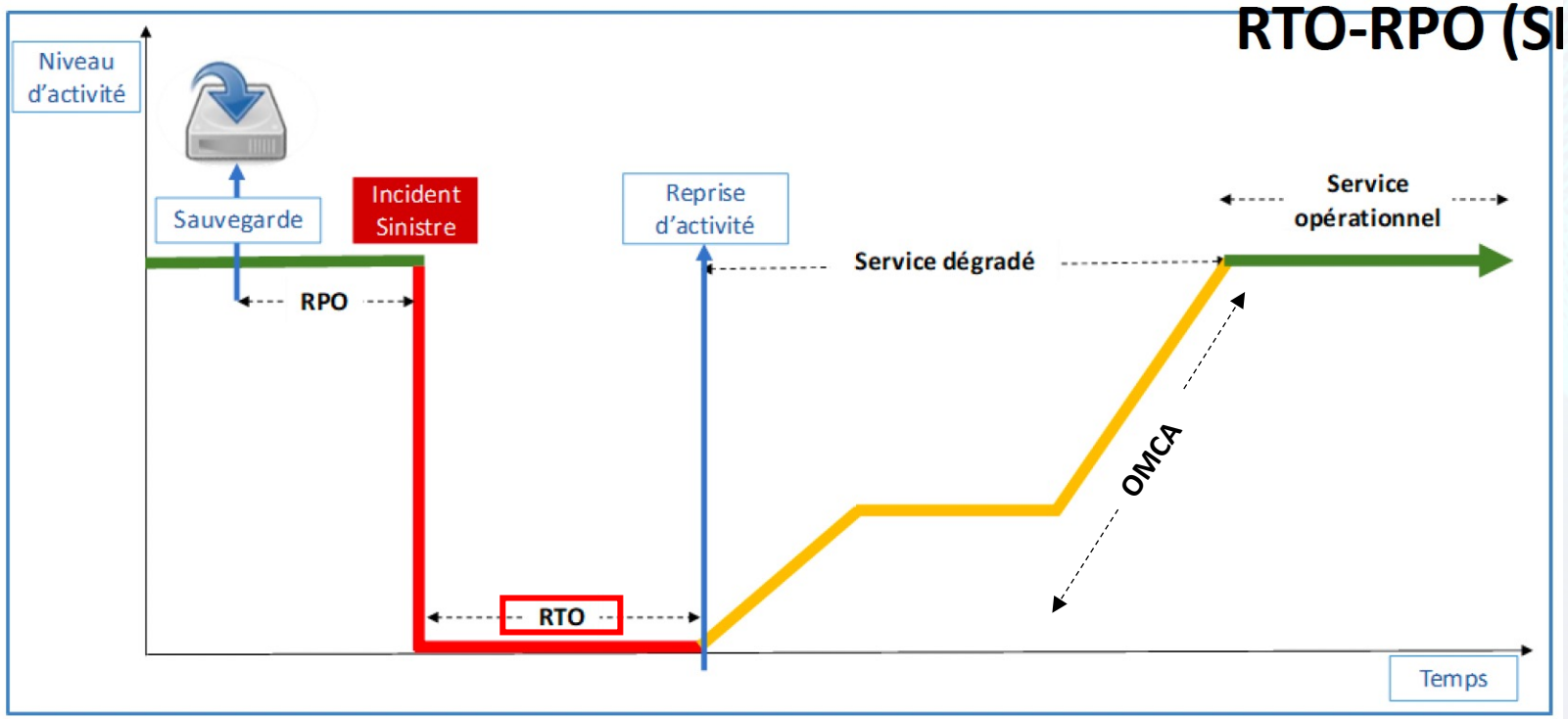
Identifier les **dépendances nécessaires** à la continuité et à la reprise des activités

La démarche de BIA

Les paramètres à identifier pendant un BIA

Délai maximum d'interruption admissible (DMIA) / Recovery time objective (RTO)

- Temps maximum acceptable durant lequel une ressource peut être indisponible pendant un incident majeur.
- Période de temps maximale après le sinistre sous laquelle chacune des ressources nécessaires à l'accomplissement d'un processus métier pour être opérationnel doivent être recouvertes.
- Généralement exprimé en heure, jour ou en semaine. L'heure de début et de fin de DMIA doit être bien identifiée
- Le délai d'interruption de service doit être inférieur au DMIA/RTO. Ce délai comprend:
  - la détection de l'incident ;
  - la décision de passage en secours
  - la mise en œuvre des procédures de secours
  - le contrôle et la relance des services et des applications

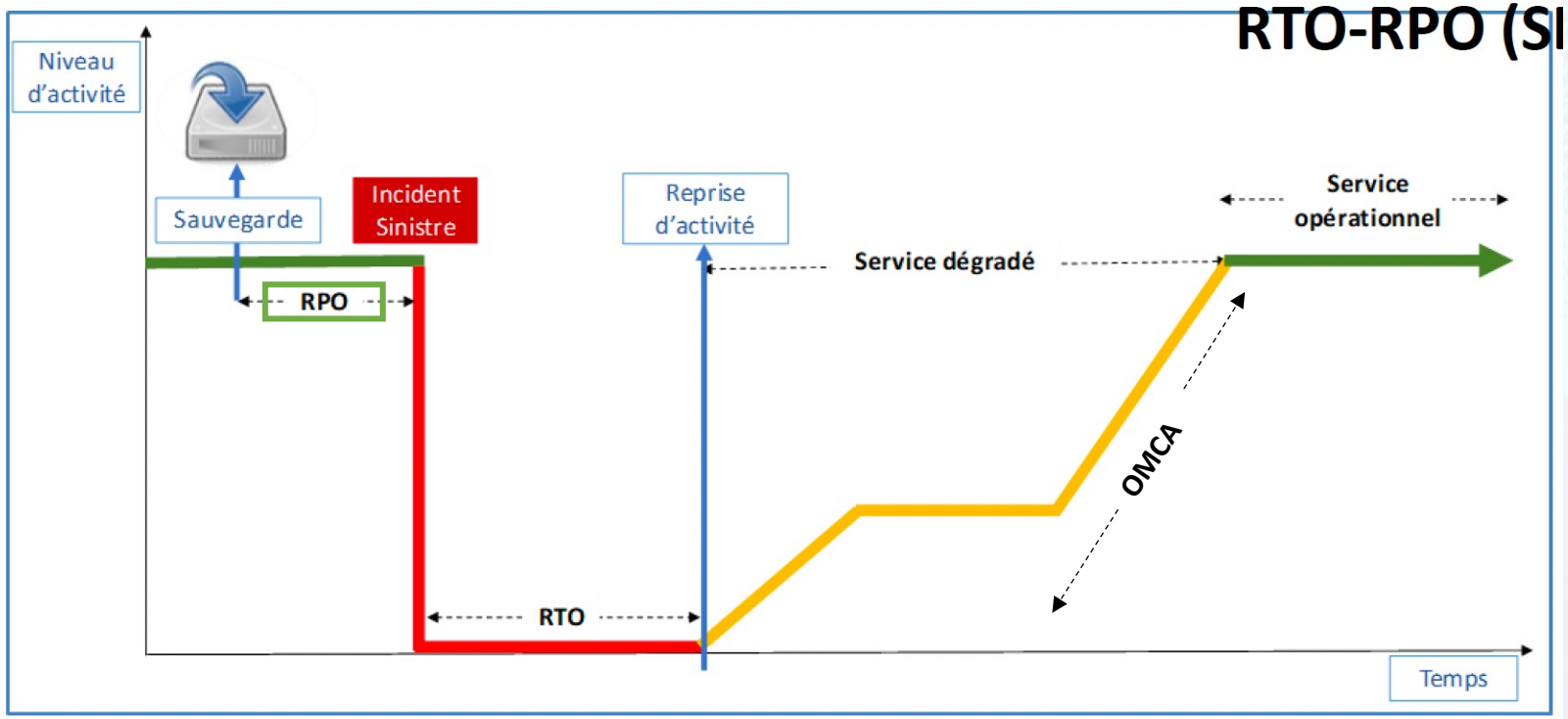


La démarche de BIA

Les paramètres à identifier pendant un BIA

Perte de données maximale admissible (PDMA) / Recovery point objective (RTO)

- Fraicheur des données à restaurer pour reprendre l'activité
- Quantifie les données que le SI peut être amené à perdre suite à un incident
- Durée entre l'incident à l'origine de la perte de données et la date la plus récente des données qui pourront être utilisées en remplacement lors de leur restauration
- Déterminé par le type et la fréquence des sauvegardes (ou réplications) effectuées sur les ressources informatiques.
- Les données perdues ne sont pas toujours restaurées à partir d'un backup. Elles peuvent être également issues d'un processus de réplication ou encore reconstruites à partir de journaux de transaction et/ou de réparation.



Besoins des métiers
- Redémarrage service
- Redémarrage de l'IT
- Perte de données

Confrontation
- Continuité du service IT
- Reprise d'activité IT

Offre de l'informatique
- Redémarrage de l'IT
- Perte de données

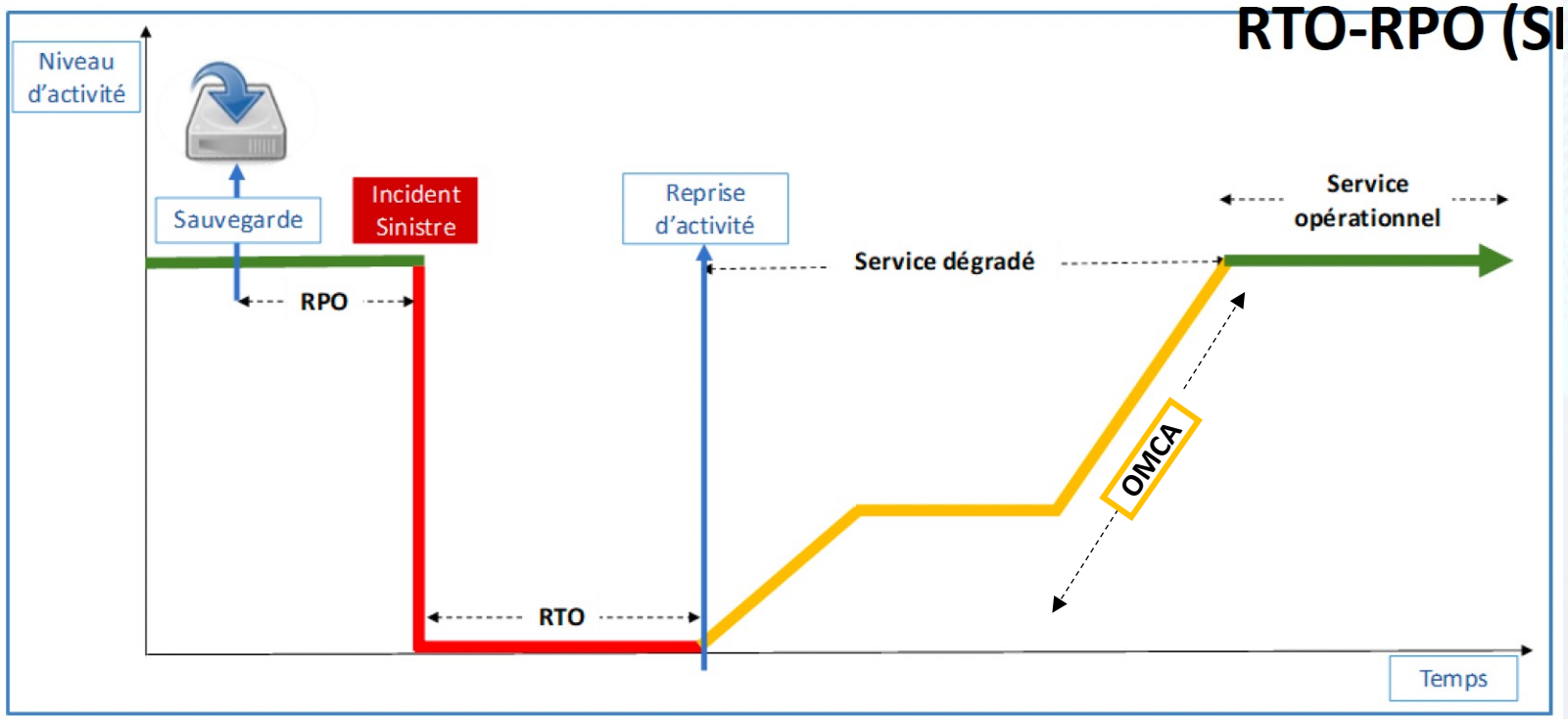
La démarche de BIA

Les paramètres à identifier pendant un BIA

Objectif minimal de continuité d'activité (OMCA)

- Niveau d'activité au-dessous duquel les conséquences sur le fonctionnement, l'accessibilité, la performance ou le service sont considérées comme inacceptable.

- Valeurs fixés par les métiers
- Objectifs fixés pour le PCA sont validés par le management



Besoins des métiers
- Redémarrage service
- Redémarrage de l'IT
- Perte de données

Confrontation
- Continuité du service IT
- Reprise d'activité IT

Offre de l'informatique
- Redémarrage de l'IT
- Perte de données

La démarche de BIA

Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessai**res pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessai**res pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

La cartographie et priorisation des activités et processus de l'entreprise

PROCESSUS	CRITERES				TOTAL
	QUALITE DE SERVICE	RESPECT DES DELAIS	CHIFFRE D'AFFAIRE	LÉGISLATION / LOIS	
	Coef : 3	Coef : 2	Coef : 1	Coef : 5	
Prospecter de nouveaux clients	2	3	5	2	27
Traiter les commandes	2	3	5	1	22
Assurer la facturation	1	2	5	1	17
Développer de nouveaux produits	5	3	3	5	49
Gérer les achats	3	4	2	3	34
Gérer la logistique	2	5	3	3	34
Gérer les finance	1	1	1	2	16
Gérer les RH	4	2	2	2	28
Manager les risques	5	5	3	5	53

La démarche de BIA

Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessai**res pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

L'identification des impacts

Impacts à analyser 1

RISQUES COMMERCIAUX ET SUR LES MARCHES

- Perte d'affaire en cours
- Perte d'opportunité commerciale
- Perte d'avantage compétitif
- Dégradation du service client
- Qualité des approvisionnements
- Non-règlement par un client
- Documents incomplets
- Assurance inadéquate
- Performance de tiers
- Retard de livraison
- Changement des coûts
- Systèmes juridiques
- Fabrication
- Manque de connaissance des marchés
- Politique
- Grèves
- Boycottage ou embargo
- Saisie, dommage ou destruction
- Transfert
- Perte de clients
- Perte de partenaires
- Perte de fournisseurs
- Livraison matières premières non assurée
- Stock externalisé détruit
- Service client non assuré (call center)
- Service métier non assuré (back-office – prise de commande - …)
- Service opérationnel non assuré (production)
- Service informatique non assuré (hébergement, …)
- Flux informatiques non assurés
- Flux documentaires non assurés

RISQUES SUR LES ACTIFS

- Immos corporelles-bureaux
- Immos corporelles-système d'information
- Immos corporelles-immobilier
- Immos incorporelles
- Stocks
- Ressources Humaines
- Vol ou dégradation de données
- Perte ou dégradation de programmes IT

RISQUES SUR L'ENVIRONNEMENT

- Destruction de l'environnement
- Non-respect des règles environnementales (RSE)
- Accident industriel
- Aléa climatique – tempête
- Aléa climatique – canicule
- Aléa climatique – tsunami
- Aléa climatique – inondation
- Aléa climatique – autre

RISQUES JURIDIQUES

- Engagement client
- Engagement partenaire
- Engagement fournisseur
- Loi
- Règlementation
- Recommandation d'audit
- Mise à jour de licences
- RGPD
- Règes de sécurité

La démarche de BIA

L'identification des impacts

Impacts à analyser 2

RISQUES SANTE ET SURETE

- Perte d'informations sensibles ou critiques
- Intrusion physique
- Intrusion logique (cyber)
- Attentat
- Epidémie/pandémie
- Intoxication
- Mise en danger du personnel (santé)
- Non-respect des règles d'hygiène et de sécurité
- Manque de moyens de sécurité

RISQUES FINANCIERS

- Perte de CA
- Déficit de trésorerie
- Surplus de trésorerie
- Pénalités de retard
- Pertes de commissions
- Pénalités pour non-exécution d'une opération
- Pénalités fiscales
- Frais spécifiques liés à la crise
- Risques liés à la forclusion
- Paiement d'intérêts divers
- Paiement de sinistres non-assurés
- Remboursement agios des clients
- Non-recouvrement des indus
- Paiement de prestations en doublon ou à tort
- Change

RISQUES OPERATIONNELS

- Rupture du processus de Direction / management
- Rupture de processus opérationnels
- Rupture de processus supports - RH
- Rupture de processus supports - communication
- Rupture de processus supports - juridique
- Rupture de processus supports - finances
- Rupture de processus supports - reporting
- Rupture de processus supports – sécurité des personnes et des biens
- Rupture de processus supports – logistique et moyens généraux
- Dépassement des dates critiques
- Perte de visibilité stratégique
- Rupture de la confiance du personnel
- SPOF (unicité de profil)

RISQUES DE REPUTATION

- Réputation clients
- Réputation partenaires
- Réputation fournisseurs
- Réputation autorités
- Réputation groupe
- Confiance interne

La démarche de BIA

L'identification des impacts

Impacts humains : L'interruption de l'activité peut-elle avoir un impact inacceptable sur la motivation, le bien-être, la santé, la sécurité des employés, des clients et/ou du public?

Impacts financiers : L'interruption de l'activité peut-elle avoir des impacts inacceptables sur les finances de l'entreprise, comme…

- interruption de flux de trésorerie / interruption de revenus?
- perte de revenus?
- pénalités, amendes, dépenses additionnelles…?

Impacts juridiques/réglementaires : L'interruption de l'activité peut-elle mener à une incapacité inacceptable de remplir des obligations réglementaires, légales ou contractuelles? Est-ce qu'il y a des risques inhérents de pénalités importantes et de poursuites?

Impacts sur la réputation et l'image : L'interruption de l'activité peut-elle entraîner des impacts inacceptables sur la confiance des parties prenantes de l'entreprise ou du public? Peut-elle engendrer de la perte de parts de marché?

Impacts opérationnels : L'interruption de l'activité peut-elle avoir des impacts inacceptables sur les opérations de l'entreprise, comme…

- qualité et livraison des produits et/ou des services essentiels à la survie de l'entreprise?
- environnement?
- approvisionnement?
- chaîne de production?
- rémunération?

La démarche de BIA

L'évaluation des impacts

Impacts	Faible	Moyen	Élevé	Critique
Financiers directs	< 10K€	10K€ à 100K€	100K€ à 1M€	> 1 M€
Financiers indirects	< 10K€	10K€ à 100K€	100K€ à 1M€	> 1 M€
Image et réputation	Diffusion dans un cercle réduit de clients ou partenaire, mécontentement de certains clients	Diffusion dans les médias spécialisés sans persistance dans le temps, fort mécontentement d'une majorité de clients ou de certains clients clés	Diffusions multiples et répétées dans les médias spécialisés internationaux, médias grand public, plaintes ou perte de nombreux clients et ou certains clients clés	Importante médiatisation internationale touchant un grand public et pouvant persister dans la durée, perte de nombreux clients y compris clients clés

87

La démarche de BIA

Identification des impacts

Impacts	Faible	Moyen	Élevé	Critique
Juridiques et réglementaires	Pas d'incapacité à répondre aux légales, contractuelles. Avertissement sans publication ou sans sanction	Non-respect d'obligations contractuelles jugées essentielles, infractions aux obligations légales avec médiatisation. Blâme accompagnés le cas échéant de sanction pécuniaire < 1M€ ou sanction équivalente	Mise en cause de la responsabilité civile, mise en cause de la responsabilité pénale. Suspension temporaire d'un ou plusieurs dirigeants, interdiction temporaire de tout ou partie des services ou opération, avec sanction pécuniaire > 1M€	Responsabilité civile avec effet systémique (chaine de contrats liés, non respect de formalités..), responsabilité pénale. Démission d'office d'un ou plusieurs dirigeants, interdiction définitive d'exercer tout ou partie des services ou opération, avec sanction pécuniaire ou retrait d'agrément
Organisationnels et sociaux	Perturbation des activité sans conséquences à moyen terme, retards non significatifs dans les projets stratégiques (quelques jours), mécontentement du personnel	Perturbation importante des activités, plan d'action spécial, retards importants dans les projets stratégiques (quelques semaines) pouvant impacter d'autres projets non critiques, grève limitée au niveau de l'activité ou entité	Perturbations très importantes nécessitant une action des responsables d'activité et une remonté au niveau des directions du pôle, retards très importants dans les projets, risque de perte d'opportunités ou non- conformité, grève au niveau de la ligne métier ou filiale	Arrêt d'activité nécessitant une cellule de crise pour déterminer les actions à entreprendre, retards très importants dans les projets stratégiques, remise en cause des projets, grèves au niveau du pôle ou du groupe

La démarche de BIA

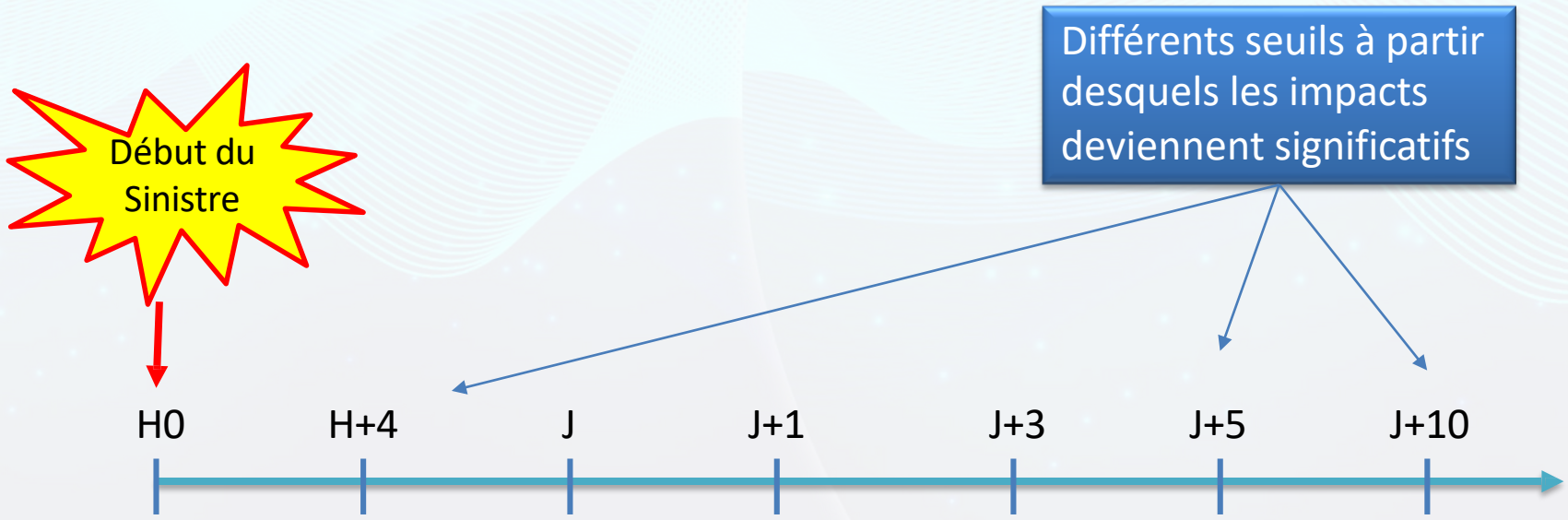
Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessai**res pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

Evaluer les impacts

Définir une échelle de temps adapté aux processus étudiés

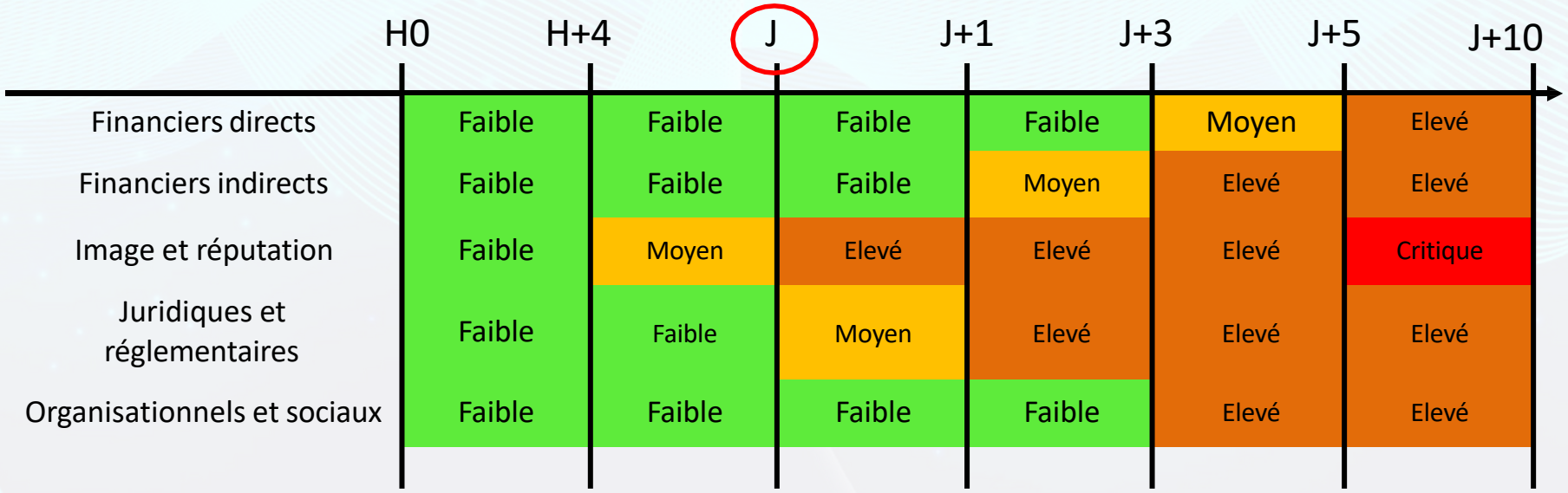


Pour des opérations quotidiennes : durée minimal de quelques heures ou 1 Jour

La démarche de BIA

Evaluer les impacts

Pour chaque impact, étudiez le niveau pour chaque intervalle



DIMA = J = Durée à partir de laquelle le type d'impact le plus important devient élevé 92

La démarche de BIA

Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessai**res pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

La reprise d'activité (OMCA)

Reprise de l'activité

Activité	TMA 4h	TMA 24h	TMA 72h	TMA 1S
Activité 1	50%	75%	75%	100%
Activité 2		40%	50%	75%
Activité 3			25%	50%

Reprise du personnel

Activité	ETP actuels	TMA 4h	TMA 24h	TMA 72h	TMA 1S
Activité 1	20	10	15	15	20
Activité 2	5	0	2	2,5	3,8
Activité 3	40	0	0	10	20
Total fonctions clés		10	17	27,5	43,8
Travail à distance		10	15	15	20
Repli interne autre site		0	2	12,5	23,8

La démarche de BIA

Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessaires** pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

Les étapes de la démarche de BIA

1. **Cartographier les activités / processus** de l'entreprise (et prioriser si nécessaire les plus critiques)
2. **Identifier les types d'impacts** et leur niveau d'évaluation
3. **Evaluer les impacts** pour chacun des processus en estimant la DMIA et la PDMA
4. **Evaluer l'OMCA** en conséquence pour chacune des activités
5. **Identifier les ressources et moyens nécessaires** pour les activités (et les moyens de contournement)
6. **Valider le BIA** par les responsables métiers / direction générale

La démarche de BIA

Validation par la Direction : présentation possible

DMIA	Activité	Impact				entité
		Image	Finance	Reglemer	Productivité	
H+4	Gérer le portefeuille d'obligations et de parts de FCC détenus en direct		4			Investissements & Placements
H+4	Gérer le portefeuile d'OPCVM actions (et d'OPCVM d'obligations convertibles)		4			Investissements & Placements
H+4	Gérer le portefeuilles d'obligations convertibles détenues en direct		1			Investissements & Placements
H+4						
4						
J+1	Recruter une personne	2	2	1	2	Ressources Humaines
J+1	Gérer la fin du contrat de travail	1	2	2	1	Ressources Humaines
J+1	Assurer la paye du personnel du groupe et le paiement des indemnités des	1	3	3	3	Ressources Humaines
J+1	Assurer les déclarations réglementaires	1	2	2	1	Ressources Humaines
J+1	Assurer le conseil et l'accompagnement des managers	1	1	2	1	Ressources Humaines
J+1	Vendre et mettre en place un crédit	3	2	2	1	Centres d'Appels
J+1						
7						

Analyse de risques

L'analyse de risques

Principes généraux de l'analyse de risques

Principe de l'analyse des risques

Les risques s'analysent selon leur vraisemblance (V) et leur Impact (I) ; Le total (T) est le multiplication des 2 avec ou sans pondération

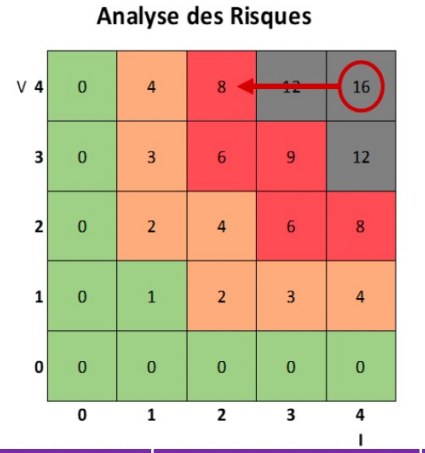
Les risques bruts représentent les risques initiaux sans mesures de réduction

Les risques nets représentent les risques bruts pondérés des mesures de réduction des risques mises en place

Exemple

- Risque de crue pour un immeuble construit dans une zone inondable
  - *Risque brut : V = 4/4 ; I = 4/4 ; T = 16 (le maximum)*
  - *Risque net : plan inondation, salles informatiques en hauteur, … : V = 4/4 ; I = 2/4 ; T = 8 (le risque est donc divisé par 2)*
- Représentation

+ RB
- MR
= RN

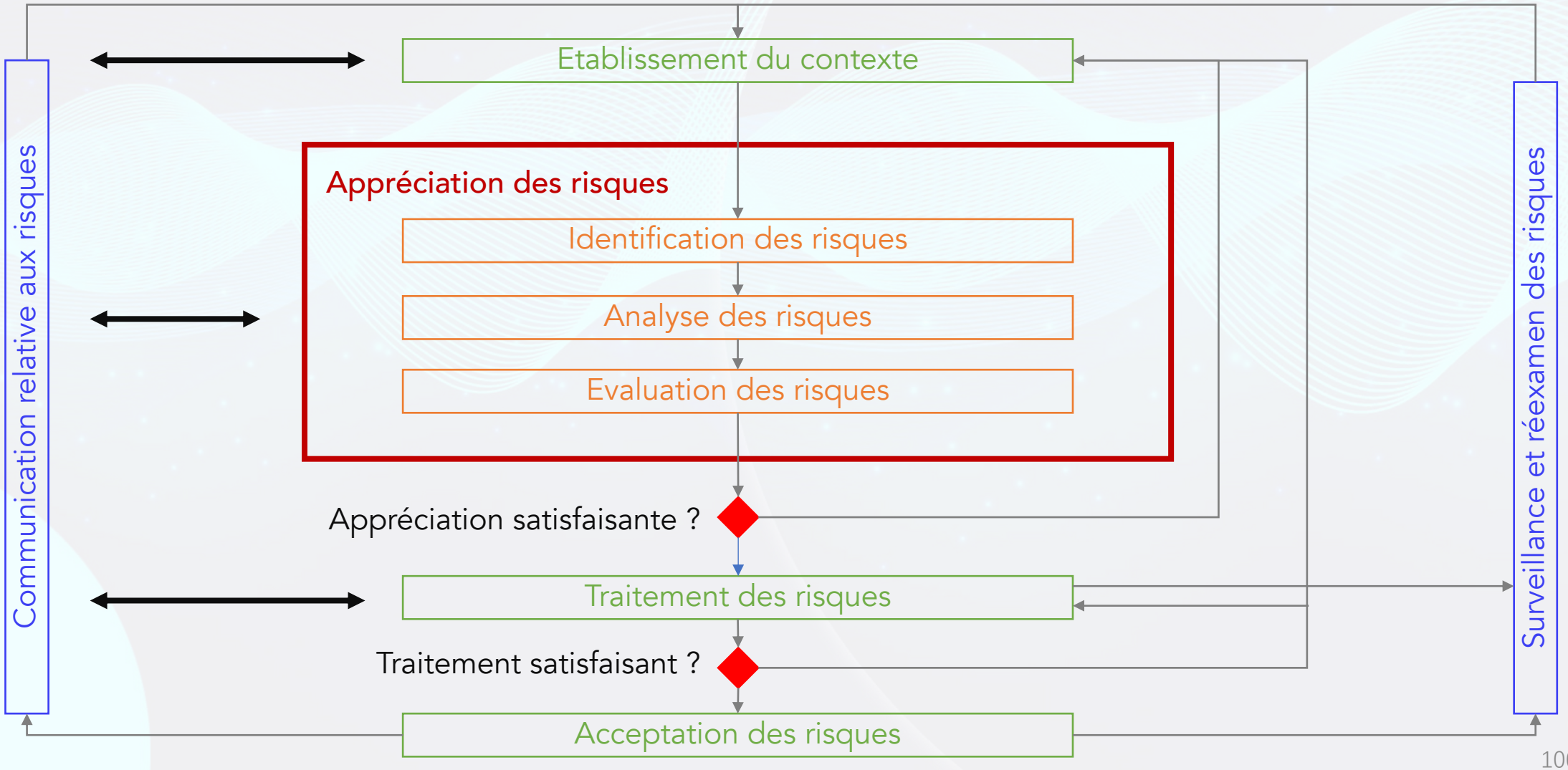


Exemple de méthode d'analyse des risques (EBIOS) →

Vulnérabilité	Menace	Risque	Impact
Construire un édifice en bord de Seine, dans un lieu exposé	Crue de la Seine	Impossibilité d'utiliser le site Intrusions …	Perte de CA Chômage technique Dégradations et vols Perte de données sensibles

L'analyse de risques

Le cadre de la gestion des risques : ISO 27005



Le cadre de la gestion des risques : les grandes étapes

1. Définir le cadre de ma gestion des risques

L'analyse de risques

Exemple de critères de criticité et lien avec le BIA

Niveau	Risque	Impact	Descriptif	DMIA
3	Critique	Grave	Tout événement susceptible de remettre en cause la survie d'un établissement ou d'un secteur métier indispensable au bon fonctionnement d'(CLIENT).	4h
2	Fort	Important	Tout événement susceptible de créer un handicap grave dans la marche d'un établissement ou d'un secteur métier d'(CLIENT). Sans toutefois mettre directement en cause sa survie (mais qui le pourrait à long terme ou suite à une répétition d'incident de ce type).	24h
1	Modéré	Significatif	Tout événement susceptible de diminuer durablement la performance d'un établissement ou d'un secteur métier d'(CLIENT).	72h
0	Faible	Limité	Evènement peu impactant au regard de l'entreprise.	1S (semaine)

L'analyse de risques

Les échelles de probabilité et d'impact

Définition des niveaux de probabilité

Ces définitions permettent de mieux interpréter les différents niveaux.

	Niveaux de probabilité	Description
3	Élevé	Il est très probable que cette cause se matérialise
2	Modéré	Il est probable que cette cause se matérialise
1	Faible	Il est peu probable que cette cause se matérialise

Définition des niveaux d'impact

Ces définitions permettent de mieux interpréter les différents niveaux

.	Niveaux d'impact	Description
3	Élevé	Conséquences directes et majeures sur l'intégrité physique des ressources humaines et matérielles, l'environnement ou la capacité à réaliser les activités (les activités sont inopérantes).
2	Modéré	Affecte l'intégrité physique des ressources humaines ou matérielles, ou encore l'environnement, mais les effets sont temporaires et réversibles. Conséquences directes sur le bon déroulement des activités. Les activités sont ralenties.
1	Faible	Affecte peu ou pas l'intégrité physique des ressources humaines et matérielles, l'environnement ou la capacité à réaliser les activités

L'analyse de risques

Les échelles de probabilité et d'impact

Description des niveaux de risque

Le niveau de risque résulte de la combinaison d'impact et de probabilité d'occurrence.

Impact	Probabilité d'occurrence		
	3 – Élevée	2 – Modérée	1 – Faible
3 – Élevé	9	6	3
2 – Modéré	6	4	2
1 – Faible	3	2	1

Le cadre de la gestion des risques : les grandes étapes

2. Identifier mes risques

Le cadre de la gestion des risques : les grandes étapes

3. Analyser mes risques

L'analyse de risques

L'intégration des risques dans le BIA

Scénario	Impacts	Probabilités/ Vraisemblance	RTO	RPO	Stratégie
xxx	Financier : perte CA, frais, mise en œuvre de solutions, assurance, pénalités, …	Faible	72h	24h	xxx
	Juridique : recours, pénalités, condamnation civile et pénale, interdiction d'exercer, …	Moyenne	24h	12h	
	Réputation : perte réputation, perte d'AO, déclassement commercial, baisse confiance des parties prenantes, …	Elevée	12h	4h	
	Opérationnel : perte de productivité, arrêt de service, défaut de pilotage, …	Très élevée	4h	1h	
	Relation client : perte de client, perte de confiance, effet domino, …				
	Actifs : perte immeuble, perte RH, perte de stocks, perte de matériel, …				

L'analyse de risques

Analyse de risques selon les impacts

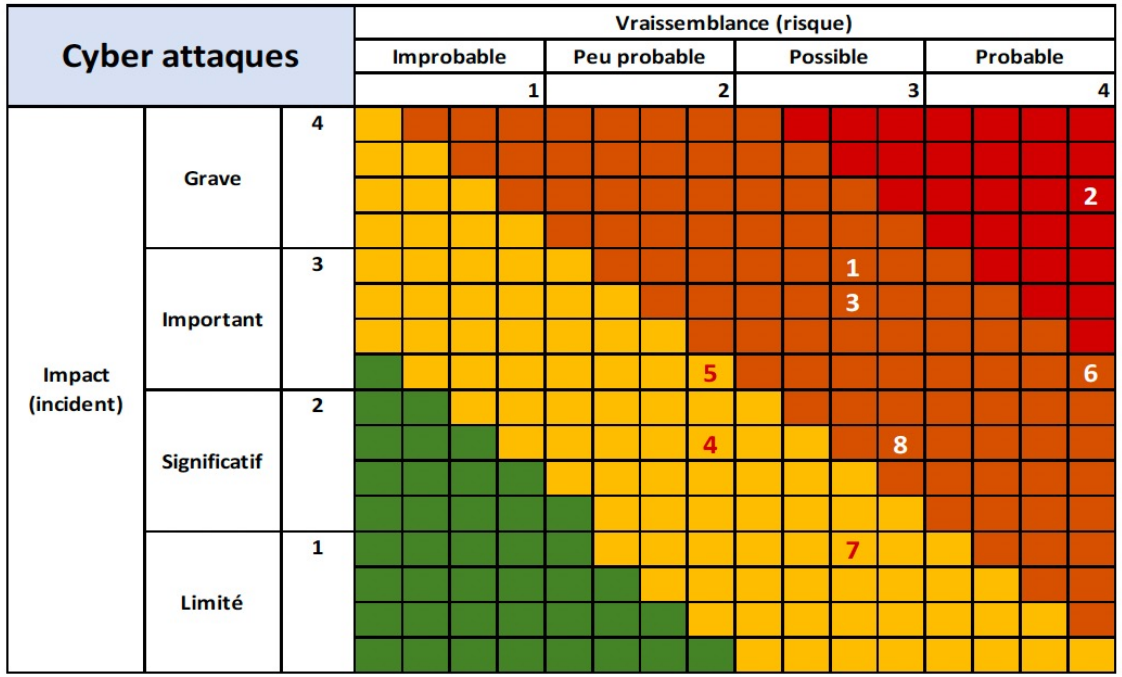
Nature de l'attaque	Or.	Risque Financier	Risque juridique	Risque d'image/de réputation	Risque opérationnel
Sabotage serveurs	I/E	• Majeur : perte de CA, paiement de pénalité	• Actions en justice clients, PS et usagers	• Majeur : perte de crédibilité sur le marché	• Suppression des services applicatifs • Suppression de logs
Vol de données	I/E	• En cas de publication : perte majeure de CA	• En cas de publication : fermeture de l'organisme	• En cas de publication : perte de crédibilité sur le marché	• Perte de données sensibles et personnelles
DDOS	E	• Vital : perte de CA, paiement de pénalités	• Limité à la responsabilité de l'organisme • Actions en justice clients, PS et usagers	• Si seuls attaqués : perte de crédibilité sur le marché • Si multi organismes : tout dépend de notre capacité à gérer la crise	• Saturation des accès réseaux via des support physiques (caméras, scans, …) • Plantage du service
Phishing-Spear	E	• S'il s'agit de l'identité d'un Dirigeant, possibilité de « rançonnage invisible »	• Mineur	• Mineur	• Usurpation d'identité
Modification volontaire du système d'authentification	I/E	• Majeur : détournement de fonds	• En cas de publication : actions en justice clients, PS et usagers	• En cas de publication : perte de crédibilité sur le marché	• Sabotage, récupération ou suppression de données • Plantage de services
Chiffrage des données et demande de rançon	E	• Majeur : détournement de fonds	• Mineur	• En cas de publication : perte de crédibilité sur le marché	• Obligation de lancer une action judiciaire • Si on refuse : sabotage, récupération ou suppression de données, plantage de services
Saturation serveur	I/E	• Majeur : détournement de fonds	• En cas de publication : actions en justice clients, PS et usagers	• En cas de publication : perte de crédibilité sur le marché	• Rediriger les requêtes vers un autre DNS local (chez les attaquants) • Blocage des postes des collaborateurs
Malware	E	• Mineur	• Mineur	• En cas de publication : perte de crédibilité sur le marché	• Non détection par les antivirus • Mettre à jour les antivirus

Le cadre de la gestion des risques : les grandes étapes

4. Prioriser mes risques

L'analyse des risques

Evaluation des risques



N°	Nature de l'attaque	V	I	VIT
1	Sabotage serveurs	2,67	3,00	8,00
2	Vol de données	4,00	3,33	13,33
3	DDOS	2,67	2,67	7,11
4	Phishing-Spear	2,00	1,75	3,50
5	Modification volontaire du système d'authentification	2,00	2,25	4,50
6	Chiffrage des données et demande de rançon	4,00	2,25	9,00
7	Saturation serveur	1,00	2,75	2,75
8	Malware	3,00	1,75	5,25

Le cadre de la gestion des risques : les grandes étapes

5. Traiter mes risques

L'analyse de risques

Analyse d'un risque majeur

Sécurité des locaux informatiques (Etat des lieux)

Entité	Nature	Risque	Vrais.	Impact Brut	Impact Net	Risque brut	Rique net
Entité 1 - SI	Santé et sûreté	Intrusion physique	3	3	3	9	9
Entité 1 - SI	Santé et sûreté	Manque de moyens de sécurité	2	3	3	6	6

Solution	Coût
Sécuriser les locaux concernés (physique et numérique) : portes, cloisons, commandes électriques, caméras, détecteurs, badgeuse, …	Coût des audits et vérifications Coût de la mise en place des recommandations
Audit par les services généraux des salles informatiques (tests avec le siège) S'assurer de l'autonomie de l'onduleur (~15 min autonomie) Vérifier le système électrique pour toutes les salles informatique Evaluer la sécurité physique de l'intérieur des salles (armoires, serveurs, etc …)	

L'analyse de risques

Exemple

Conséquence	Cause	Risque			Mesures de contrôle et d'atténuation	Commentaires
		Impact	Probabilité	Niveau		
1 – Perte d'accès à l'emplacement / Perte de l'emplacement	• Incendie • Sinistre (dégât d'eau)	3	1	3	Il y a une procédure d'évacuation en place, mais elle n'a jamais été testée.	Étant donné que le bâtiment est neuf, il serait très surprenant qu'un incendie ravageur ou un bris de plomberie majeur survienne. Effectuer un exercice d'évacuation annuellement.
2 – Perte des systèmes informatiques et de communication (équipements, applications, téléphones)	• Incendie • Cyberattaque (virus, logiciels malveillants, sabotage)	3	2	6	Mettre en place ces mesures : • Relocaliser la salle des serveurs dans un local muni de mesures anti-feu. Faire effectuer périodiquement, par une firme externe, une maintenance de nos systèmes (antivirus…).	Se référer au document de conception pour les stratégies de continuité.
3 – Absentéisme anormal ou perte d'employés clés	• Démission Maladie	3	2	6	Aucune pour le moment	Éviter de dépendre d'un seul employé pour les compétences clés.
4 – Interruption des services d'un partenaire d'affaires clé (fournisseur ou sous-traitant)	• Faillite Problème de continuité chez le fournisseur	2	2	4	Aucune pour le moment	Se référer au document de conception pour les stratégies de continuité.
5 – Perte des ressources essentielles, d'équipements ou d'outils clés et des services	• Coupure d'électricité (tempête, incendie)	2	1	2	Aucune pour le moment	Se référer au document de conception pour les stratégies de continuité.

Priorisation des activités et reprise

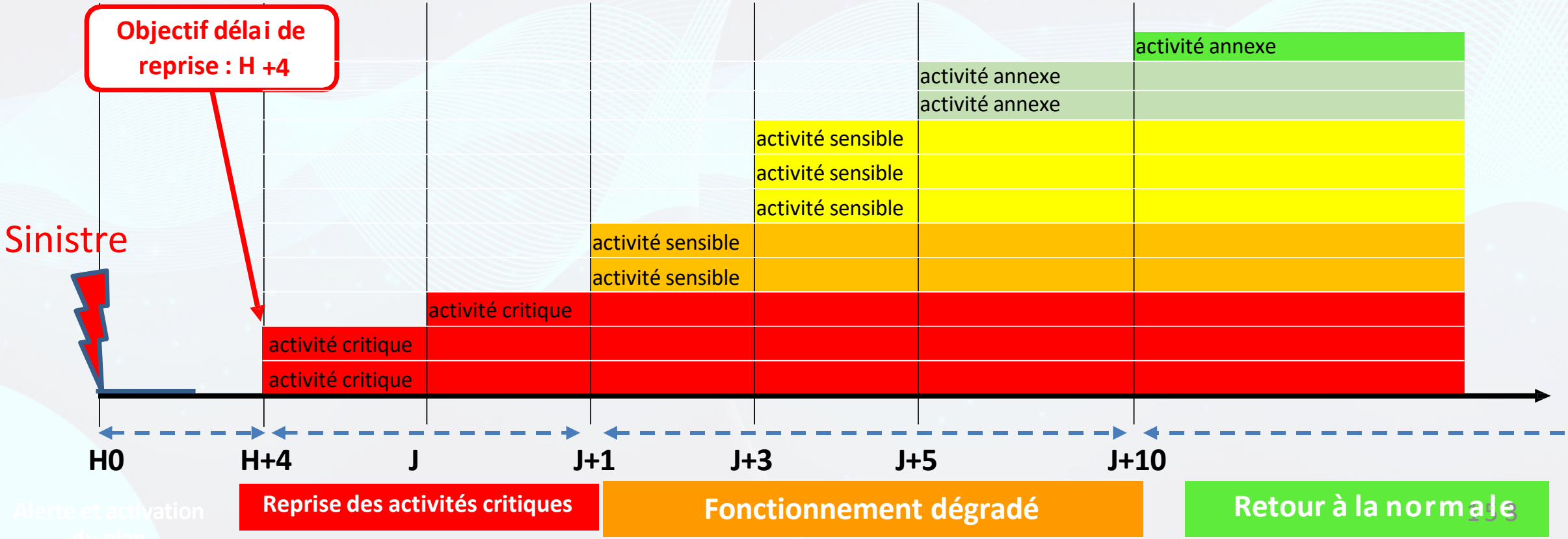
Priorisation des activités et reprise

Objectifs de reprise des métiers

		Objectifs de de reprise des métiers							
Métier	**Activité**	**Immédiat**	**24h**	**48h**	**56h**	**72h**	**5 jours**	**1 mois**	**3 mois**
gestion locative									
	Emettre les quittances			X					
	Virements des loyers aux propriétaires								
	Recouvrement des impayés								
Syndic									
	Planning des assemblées générales								
	tenir les assemblées générales								
	Contentieux								
Compta Fiuance									
	Compta générale								
	Compta ana								
	Fournisseurs								
RH									
	Paye								
	Recrutement / embauches								
	Relations sociales								
	Gestion du personnel : VM, congés, etc								

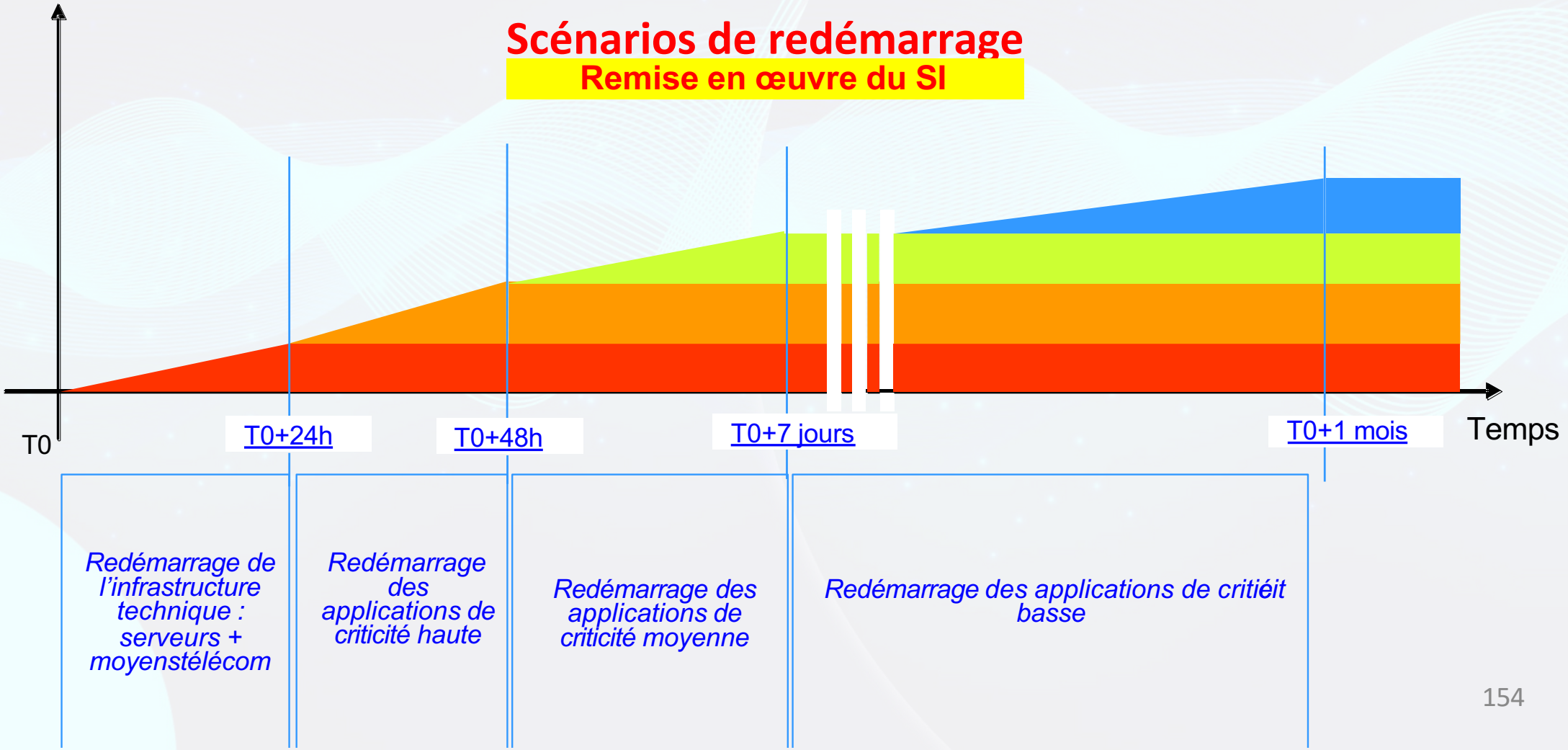
Priorisation des activités et reprise

La timeline de redémarrage des activités de l'organisation



Priorisation des activités et reprise

La timeline de redémarrage des activités de l'organisation



Priorisation des activités et reprise

Le choix des solutions de reprise

Identifier les moyens de reprise

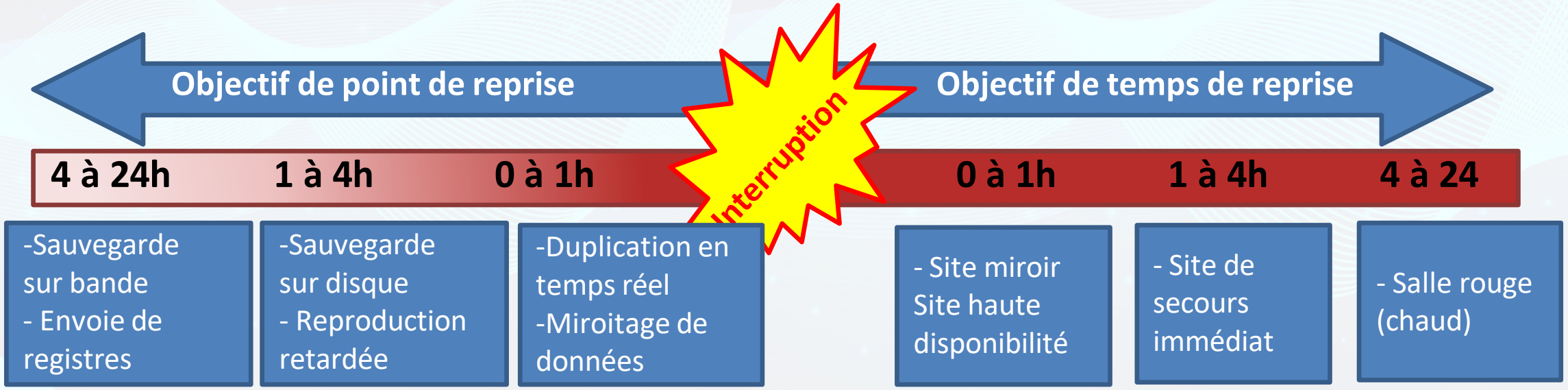
Consolider les solutions

Arbitrer et valider

Priorisation des activités et reprise

Le choix des solutions de reprise

Choisir les solutions => OPR et OTR influencent la stratégie



Quelles stratégie de protection des données ?

Quelle stratégie de reprise ?

Coût de la stratégie inversement proportionnel au temps

Secours utilisateurs

Secours utilisateurs

Principes généraux

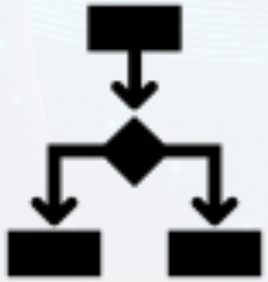
Plan de Secours Utilisateurs	Plan de Secours Informatique	Plan de Secours Logistique
Volet 1 - Infrastructure et locaux		
Volet 2 - Documentation et procédures		
Volet 3 - Organisationnel		
Livrables Plan de Reprise Utilisateurs Procédures de secours métiers	Livrables Plan de Reprise Informatique Procédures de secours informatique	Livrables Plan de Secours logistique

Secours utilisateurs

Définition

Le Plan de Secours Utilisateurs est un **dispositif nécessaire** à la **reprise d'activité en cas de sinistre affectant les locaux utilisateurs. Il est constitué de :**

Locaux de secours



Procédures et documentations

Organisation de crise

Secours utilisateurs

Les typologies de site de secours

Il existe plusieurs typologies de sites de secours

Salle blanche	Site chaud	Site froid	Site tiède
Salle machine protégée par des procédures d'accès et généralement secourue électriquement	Site où les systèmes informatiques sont à jour, interconnectés, paramétrés, alimentés à partir des données sauvegardées et prêt à fonctionner	Site de secours qui peut avoir une autre utilisation en temps normal	Site intermédiaire avec des machines installées avec les données sur bande mais non importées dans les systèmes de données.

- Systèmes distribués sur plusieurs sites
- Site de secours mobile

Le déploiement d'une solution de secours utilisateurs

Mise en place de la solution

Organisation du plateau de repli

- Définition d'un plan de salle (zoning)

Configuration des PdT

- Masterisation des postes lourds
- Utilisation de postes virtualisés

Gestion de la téléphonie

- Bascule des appels vers le site de repli

Connexions réseaux

- Vérification de la bande passante
- Vérification des configurations de filtrage
- Table de routage
- Utilisation de scripts systèmes

Logistique du site de secours

- Gestion du courrier
- Hébergement
- Moyens d'accès
- Stationnement

Secours utilisateurs

La construction d'un plan de reprise utilisateurs

Plan de reprise utilisateurs

Introduction	Rappel des objectifs du PCA
	Scénarios de sinistres envisagés
	Descriptif rapide de la solution de secours
Reprise globale des métiers	Ouverture du site de secours
	Préparation du site pour l'accueil des utilisateurs
	Montée en charge des activités
	Répartition des utilisateurs
	Actions prioritaires
	Moyens à disposition sur le site
Informations pratiques	Localisation, itinéraire et modalités d'accès
	Contacts et assistance sur le site
	Restauration et hébergement

Secours utilisateurs

Les procédures de secours métiers

Procédures de secours métiers

- Rappel des principales étapes du PCA
- Premières actions à mener en cas d'activation
- Nombre de personnes et positions prévu
- Liste des personnes mobilisées pour la reprise et coordonnées de contact
- Moyens à disposition sur le site de secours
- Liste des applications métiers demandées sur le site de secours
- Rappel de la stratégie de continuité d'activité du métier
- Premières actions de reprise métier identifiées
- Annuaire des contacts métiers
- Coordonnées du support et assistance

Attention au respect de la confidentialité des personnes à mobiliser en cas de sinistre

Secours informatique

Secours informatique

Principe

Plan de Secours Utilisateurs	Plan de Secours Informatique	Plan de Secours Logistique
	Volet 1 - Infrastructure et locaux	
	Volet 2 - Documentation et procédures	
	Volet 3 - Organisationnel	
Livrables	**Livrables**	**Livrables**
Plan de Reprise Utilisateurs	Plan de Reprise Informatique	Plan de Secours logistique
Procédures de secours métiers	Procédures de secours informatique	

Secours informatique

Définitions

Le Plan de Secours Informatique est un **dispositif nécessaire** à la **reprise du système d'information en cas de sinistre.** Il est constitué de :

Secours informatique

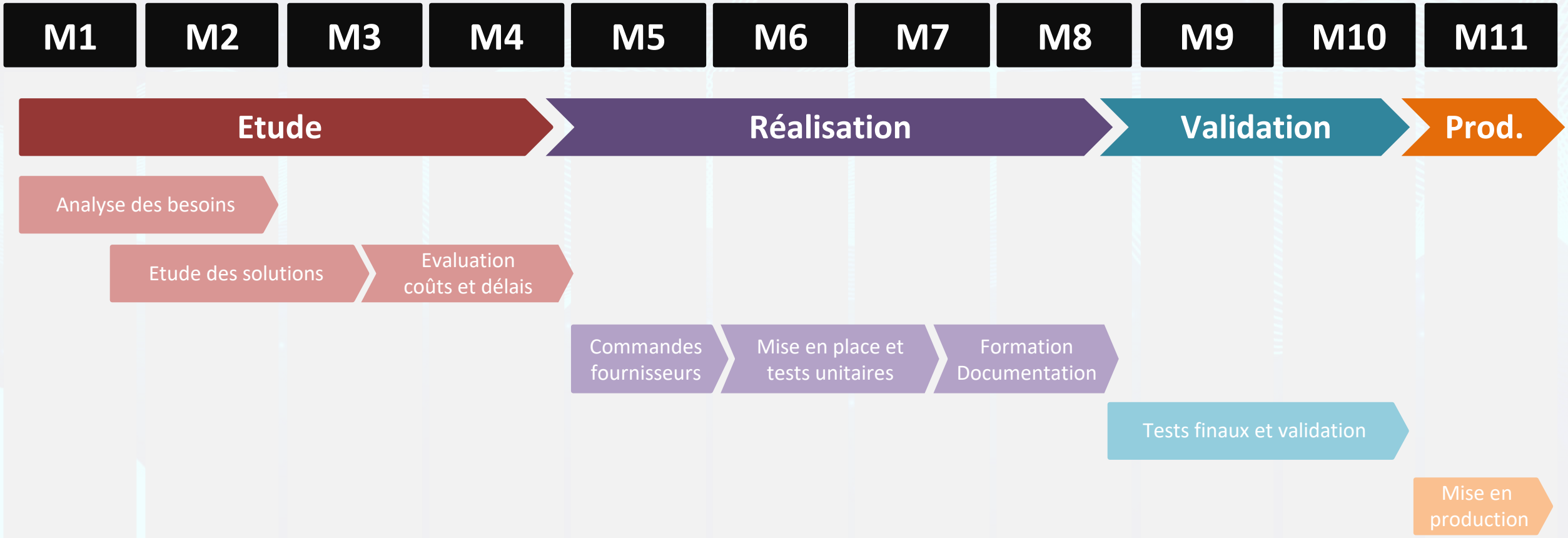
Procédures de secours

Documentation technique

Organisation de crise

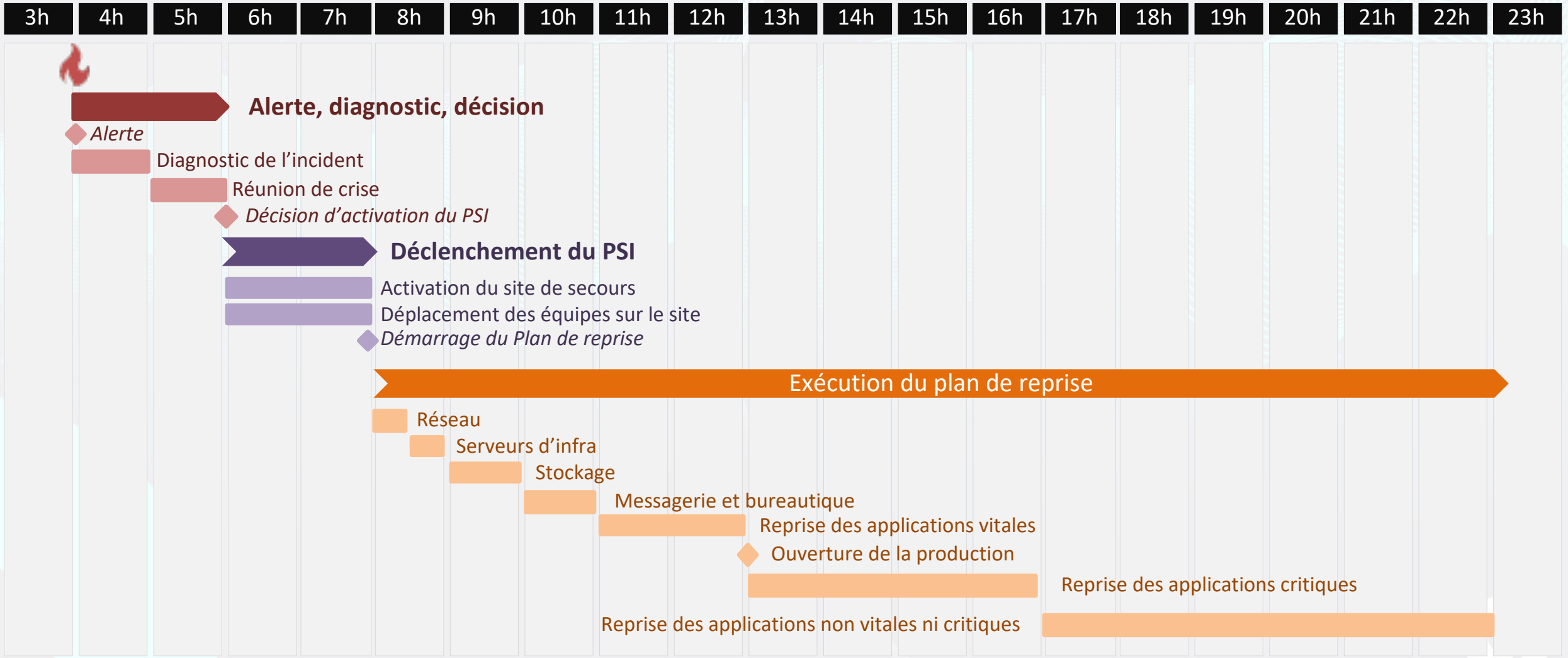
Secours informatique

Planning de mise en œuvre d'un plan de secours informatique



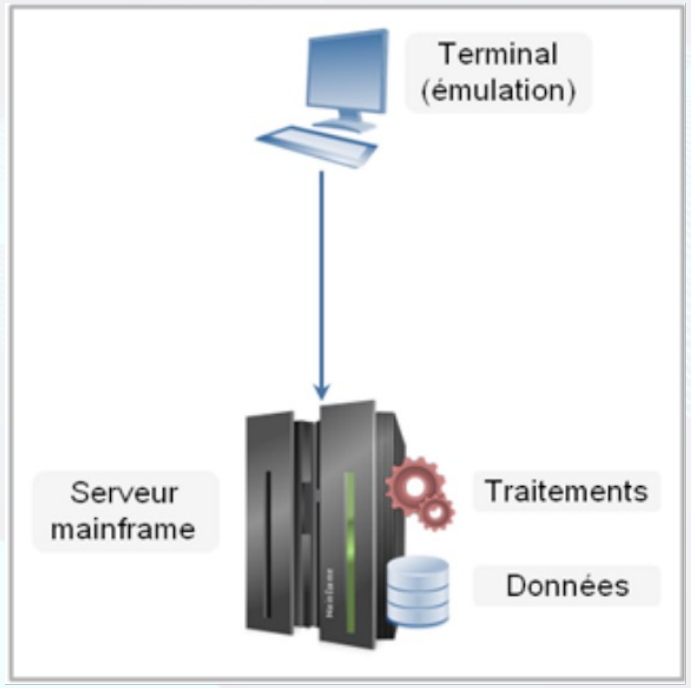
Secours informatique

Déclenchement d'un plan de secours informatique

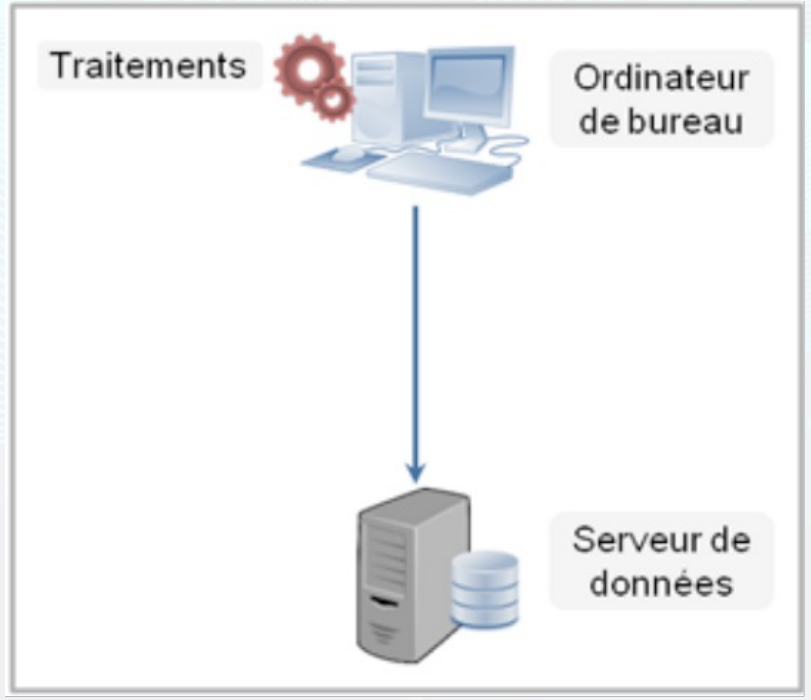


Secours informatique

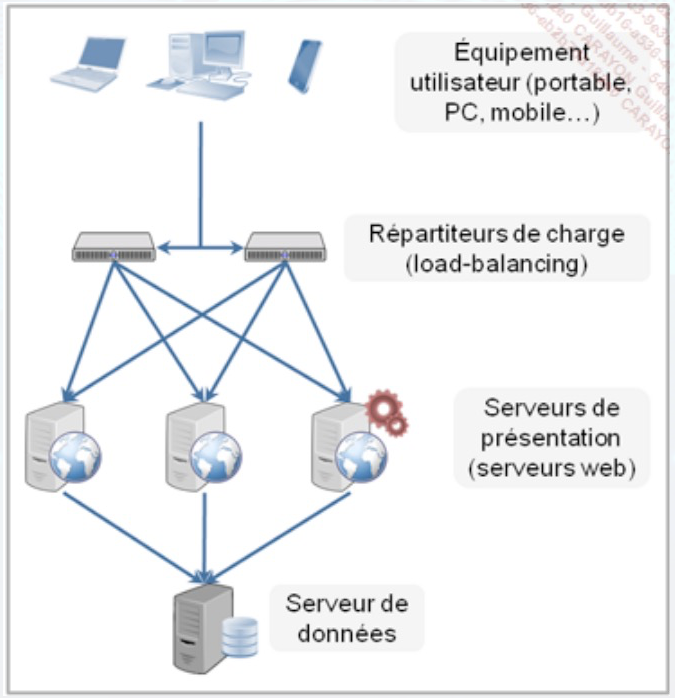
Panorama des solutions techniques



Mainframe



Client-serveur



N-tiers

Secours informatique

Panorama des solutions techniques

- Le secours à froid sur sauvegarde
- La réplication de données
- Le fonctionnement en cluster
- La virtualisation de serveur
- Le cloud

Secours logistique

Secours logistique

Principes

Plan de Secours Utilisateurs	Plan de Secours Informatique	Plan de Secours Logistique
Volet 1 - Infrastructure et locaux		
Volet 2 - Documentation et procédures		
Volet 3 - Organisationnel		
Livrables	**Livrables**	**Livrables**
Plan de Reprise Utilisateurs<	Plan de Reprise Informatique	Plan de Secours logistique
Procédures de secours métiers	Procédures de secours informatique	

Secours logistique

Définition

Mise en œuvre des moyens logistiques et matériels nécessaires en cas d'activation du PCA

Immobilier

Réacheminement du courrier

Déménagement et transport d'équipements

Gestion des fournisseurs spécialisés

Plan de secours logistique

Etude des solutions logistiques et des Moyens Généraux

Gestion de l'immobilier :

- Recherche et qualification des locaux existants en interne.
- Étude des offres de fournisseurs spécialisés pour un repli externe.
- Identification de la place disponible et des locaux vacants utilisables dans une stratégie de relocalisation des utilisateurs en cas de sinistre.
- Évaluation de la charge de travail et des coûts de la préparation éventuelle des locaux utilisateurs en mobilier et câblage.

Etude des solutions logistiques et des Moyens Généraux

Logistique PCA :

- Etude des besoins liés au PCA
- Besoins logistiques en cas d'activation du secours
- Gestion des stocks de matériel éventuels
- Préparation de la distribution du matériel en cas d'activation

Etude des solutions logistiques et des Moyens Généraux

Gestion du courrier

Gestion des fournisseurs Moyens Généraux

Tests du PCA/PRA

Objectifs généraux

Le test du PCA est la vitrine du PCA

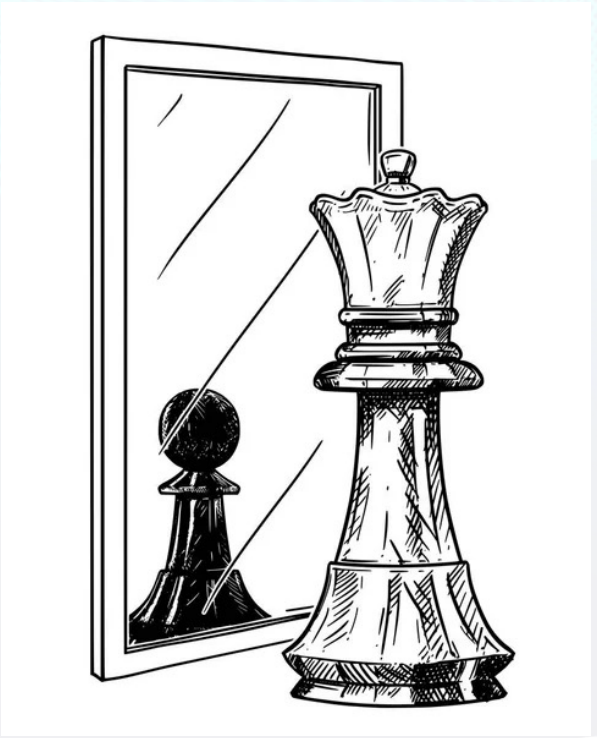
Démontrer le fonctionnement du PCA (homologation)

Vérifier le fonctionnement du PCA de manière régulière

Identifier les problèmes et réaliser les actions correctives

Participer à la formation des utilisateurs au PCA

Se conformer aux exigences d'autorités de tutelle (ex : AMF)



Tests du PCA/PRA

Que tester et quand ?

Il est impératif de tester tous les composants du PCA

- Secours utilisateur
- Secours informatique
- Secours logistique
- Organisation de crise

Au moins deux fois par an chaque composant du PCA (si possible de manière combiné)

Tests du PCA/PRA

Que tester ?

Scénario de sinistre	Plan de secours testé
Site inaccessible	• Plan de secours utilisateurs
Site détruit	• Plan de secours utilisateurs • Plan de secours informatique*
Crise sanitaire	• Plan de secours utilisateurs
Salle informatique détruite ou sinistrée	• Plan de secours informatique

Tests du PCA/PRA

Types de tests

Évaluation sur papier

- Réalisé par les acteurs clés qui survolent le plan sur papier
- On essaie d'identifier ce qui pourrait survenir dans des cas particuliers
- Plan étudié en partie ou entièrement. Précède habituellement le test de préparation

Test de préparation

- Version localisée du test complet au cours duquel les ressources actuelles simulent une panne système
- Permet de tester différents aspects du plan et de l'améliorer étape par étape
- Permet d'obtenir progressivement les preuves de l'efficacité du plan

Test opérationnel complet

- Avant ce test on s'assure d'avoir correctement testé le plan sur papier et dans sa version localisée
- Interruption complet des opérations et test en grandeur nature

Tests du PCA/PRA

Préparation des tests

Bien rédiger les plans de tests

Mobiliser un nombre significatif de personnes

Tests du PCA/PRA

Communication

Annoncer le lancement du test

Diffuser les comptes-rendus d'avancement régulier

Réaliser un post-mortem

Tests du PCA/PRA

Démarche de test

La démarche de réalisation d'un test PCA

Planification → Préparation → Exécution → Post-mortem

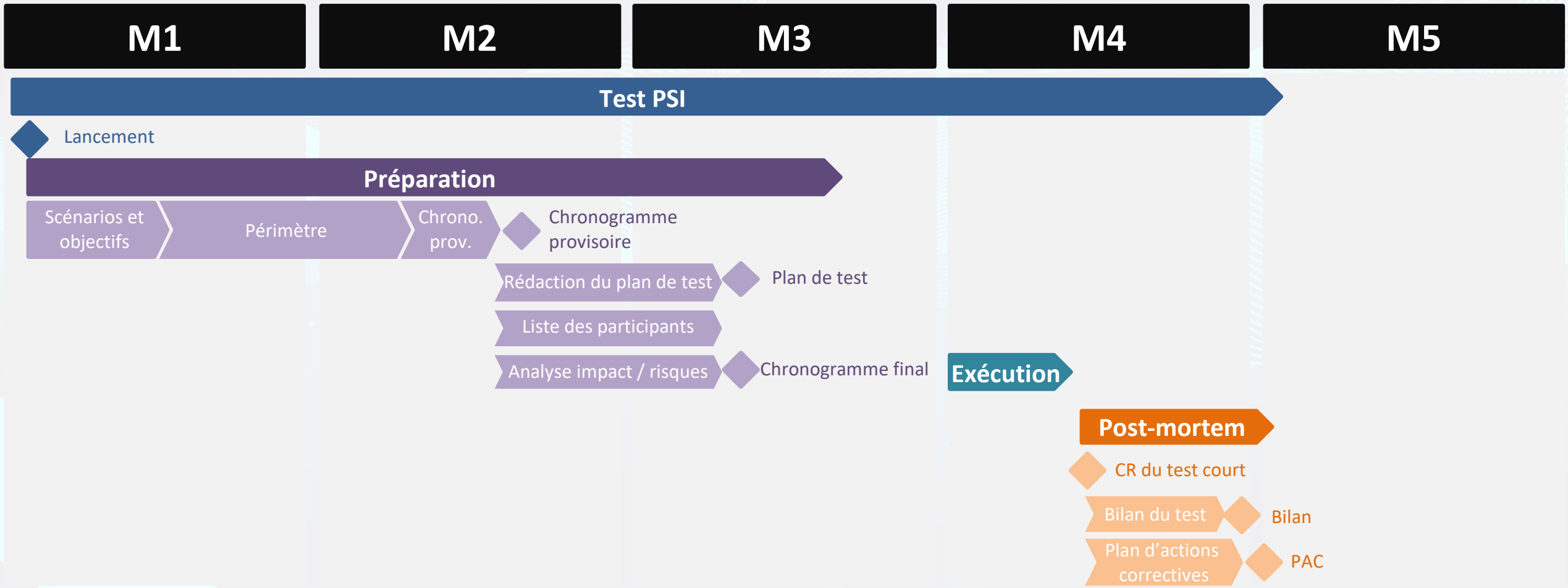
Les principaux livrables

- Cahier des charges de test
- Chronogramme du test
- Plans de test
- Bilan de test
- Plan d'actions correctives

Il faut s'appuyer sur la documentation existante

Tests du PCA/PRA

Macro-planning d'un test d'un plan de secours informatique



Tests du PCA/PRA

Cahier des charges d'un test de plan de secours informatique

Scénario

Spécificités du test

Objectifs et facteurs clés de succès

Périmètre technique et fonctionnel

Acteurs

Support interne et externe

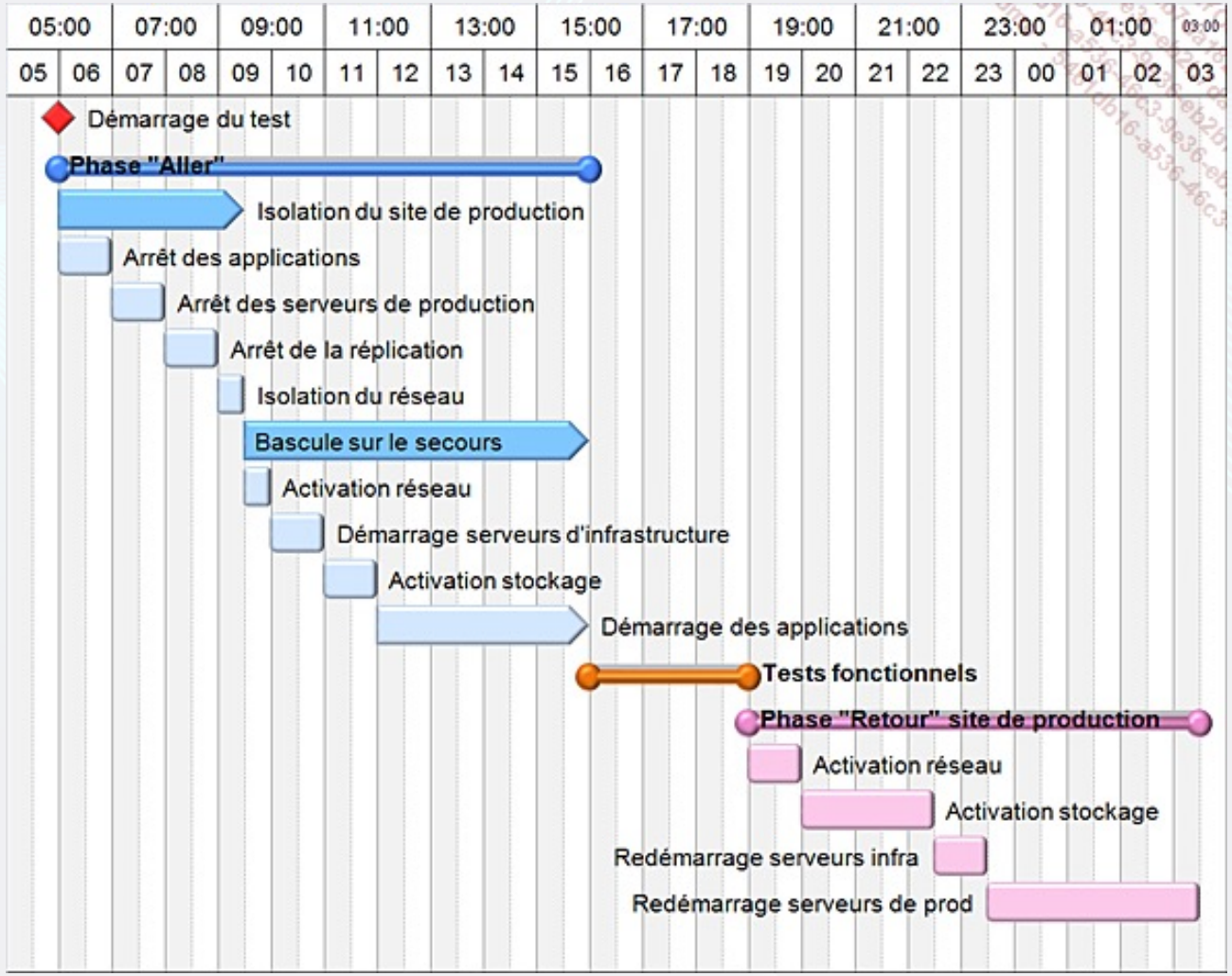
Logistique et informations pratiques

Chronogramme provisoire

Reporting et communication

Tests du PCA/PRA

Proposition de chronogramme d'un test de plan de secours informatique



Tests du PCA/PRA

Analyse d'impact d'un test de plan de secours informatique

Identification des impacts sur le système d'information


Systèmes et applications


Batchs


Services


Utilisateurs


Communication auprès du comité chargé d'accorder l'exécution du test


Identifier et proposer les mesures permettant d'atténuer les impacts

Tests du PCA/PRA

Analyse de risques d'un test de plan de secours informatique

Identifier les risques d'incidents qui peuvent survenir lors d'un test

Problèmes techniques de redémarrage du SI

Panne de matériel

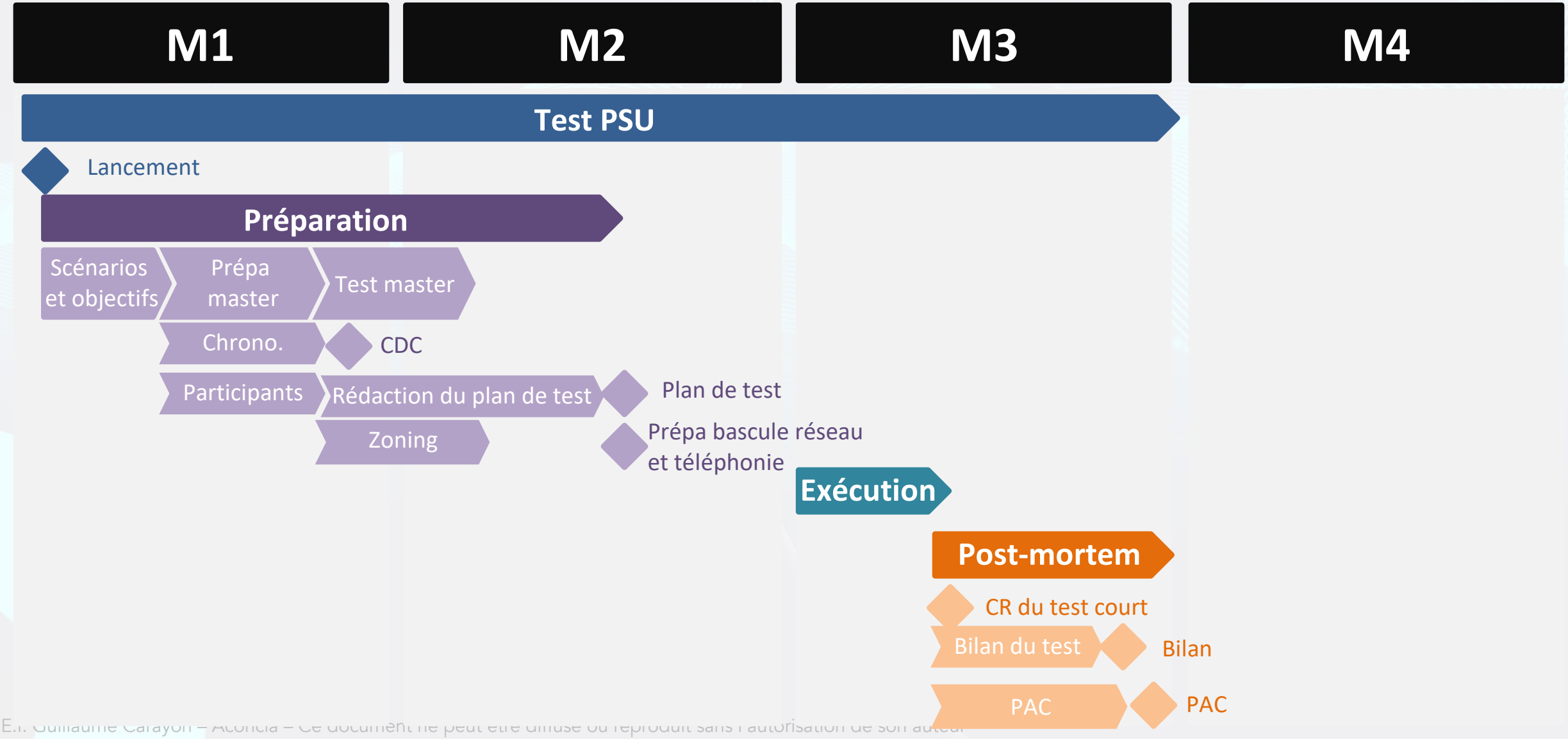
Erreur humaine

Risques opérationnels

Prévoir un plan de réduction du risque

Tests du PCA/PRA

Macro-planning d'un test d'un plan de secours utilisateurs



Tests du PCA/PRA

Cahier des charges d'un test d'un plan de secours utilisateurs

Scénario

Objectifs et facteurs clés de succès

Spécificités du test

Liste des participants

Zoning

Liste des applications et masters

Renvoi des flux réseau et de la téléphonie

Support interne et externe

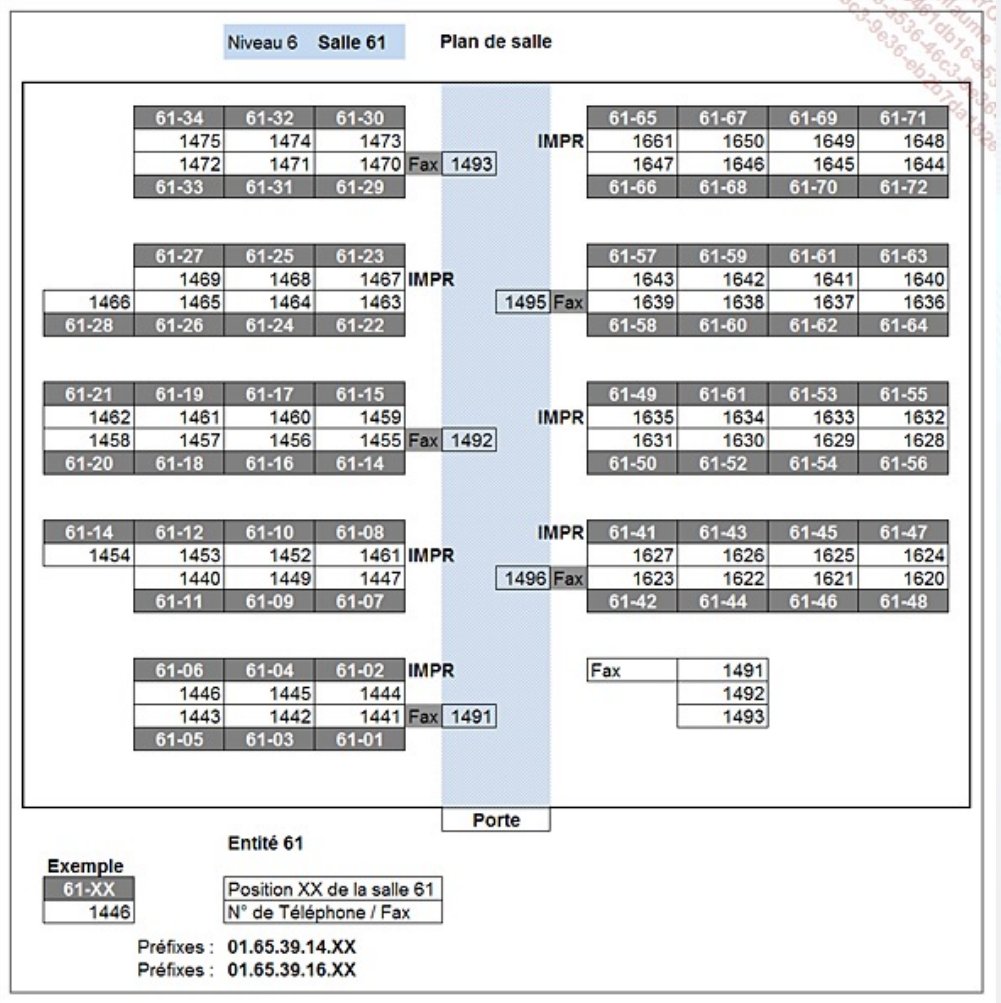
Logistique et informations pratiques

Chronogramme provisoire du test

Reporting et communication

Tests du PCA/PRA

Cahier des charges d'un test d'un plan de secours utilisateurs – zoning



Tests du PCA/PRA

Plan de tests

Description des opérations fonctionnelles testées sur les applications après la bascule du secours (appelés aussi scénarios de test ou protocoles de tests)

Tests techniques	Tests fonctionnels
Figurent dans la procédure technique de reprise de chaque application	Opérations réelles ou fictives qui seront réalisées sur les applications basculées

- **Réalisé pour chaque application et couvrir des opérations métiers usuels**
- **Décrit les opérations à réaliser, leurs données en entrée, le cas échéant et les résultats attendus**

Tests du PCA/PRA

Déroulement d'un test

LANCEMENT

- Mise à disposition de kit de test
- Check-list de vérification de la position de travail
- Vérification des prérequis de l'exécution du test

DEROULEMENT

- Suivi des plans définis
- Mise à disposition d'une équipe de coordination

FIN

- Remise d'un questionnaire de satisfaction
- Collecte des feedbacks

Tests du PCA/PRA

Déroulement d'un test - questionnaire

Le questionnaire peut intégrer les rubriques suivantes

- Locaux
- Logistique
- Communication
- Support
- Outils
- Résultat global du test
- Remarques et suggestions

Tests du PCA/PRA

L'après test

Flash report

- Tendance générale du déroulement du test
- Principaux jalons chronologiques du test
- Liste des opérations réalisées et leur statut provisoire

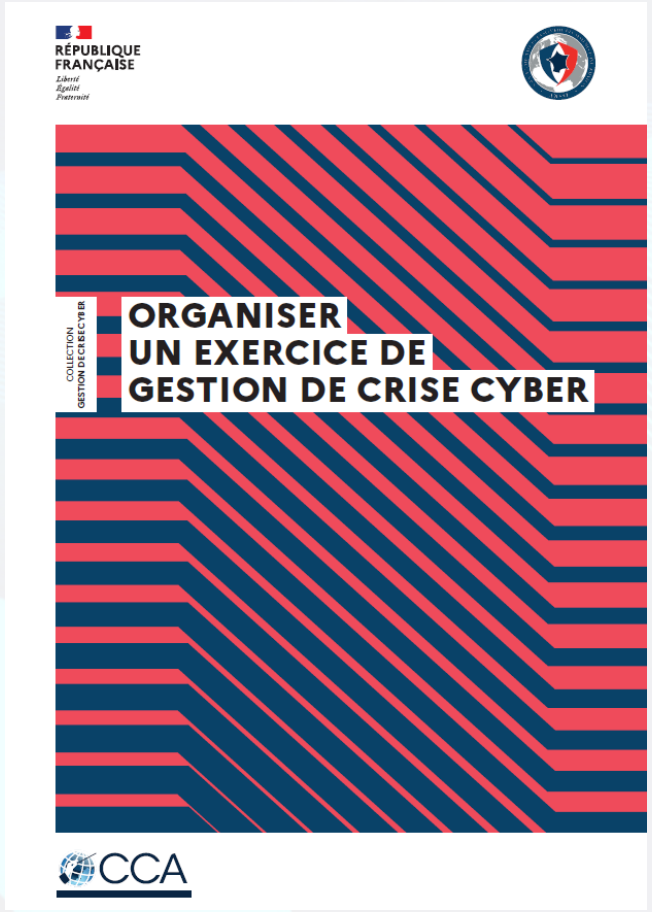
Bilan de test

- Executive summary
- Atteinte des objectifs
- Synthèse de la satisfaction globale des intervenants
- Leçons retenues
- Détail des résultats
- Description et statut des problèmes rencontrés

Formalisation des plans d'actions correctives

Tests du PCA/PRA

L'exercice de gestion de crise cyber

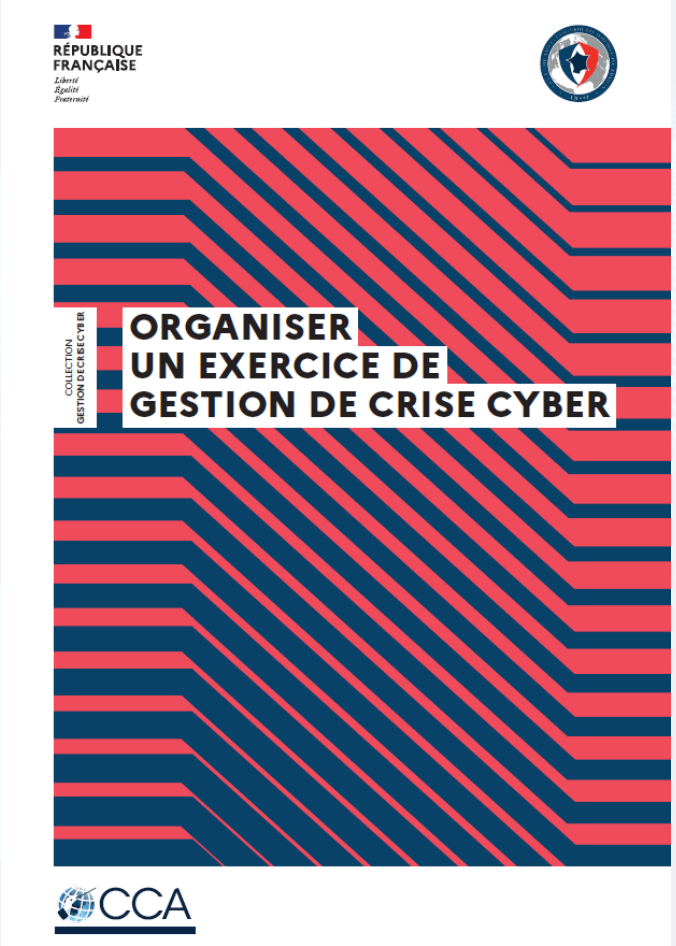


Focus sur le guide de l'ANSSI

« Organiser un exercice de gestion de crise cyber »

Tests du PCA/PRA

L'exercice de gestion de crise cyber



Sur la base de l'exemple RANSOM20 proposé dans le guide, réalisez deux exemples de tableau de bord :

1) Un tableau de bord permettant de suivre la gestion de la crise elle-même (périmètre touché, niveau de remédiation…)
2) Un tableau de bord permettant de mesurer le succès ou non d'un exercice de crise cyber (compréhension des procédures, temps de prise de décision…)

Vous transmettrez ces deux tableaux de bord au format le plus approprié à guillaume.carayon@ynov.com

Maintien en condition opérationnel

Objectifs

Maintien en Condition Opérationnel

=

Pérenniser l'investissement du PCA

Rôles et responsabilités clés

Le responsable PCA : Référent et animateur du PCA

- Assurer la gouvernance PCA
- Identifie les évolutions de l'organisation
- Identifie les évolutions des moyens
- Organise les tests
- Tient à jour la documentation
- Sensibilise et forme les utilisateurs
- Assures la relation avec les partenaires
- Anime le réseau de correspondants

Rôles et responsabilités clés

Le responsable PCA idéal

- Positionné dans la Direction transverse rattaché au Directeur adjoint ou VP de cette Direction transverse
- Plus de savoir-être et de savoir-faire que d'expertise technique
- Sens politique développé
- Compréhension du métier

Rôles et responsabilités clés

Les correspondants PCA : Relais du RPCA, proche des métiers

- Identifient les évolutions de l'organisation, des outils, des équipes, des processus…
- Remonte les informations au fil de l'eau
- Suit le référentiel des utilisateurs prévus en repli
- Rédige les tests avec les utilisateurs ou les responsables métiers
- Relais du RPCA dans l'organisation des tests

Maintien en condition opérationnel (MCO)

Maintenabilité

Hébergement

- Locaux informatiques dédiés
- Cloud

Architecture

- Urbanisation du SI

Réseau

Poste de travail

Téléphonie

Maintenabilité

Système de Gestion Electronique des Documents :

- Facilité de mise à jour
- Gestion des versions
- Portabilité et disponibilité sur différentes plateformes
- Organisation formalisée de suivi et de mise à jour

Maintenabilité

Secours croisé

- Peu coûteux à mettre en place
- Maintenance plus coûteuse
- Double évolution

Secours dédié

- Investissement important
- Mise à jour à prendre en compte
- Facilité de réalisation des tests

Maintien en condition opérationnel (MCO)

Maintenabilité

- Indicateurs
- Revues et compte-rendus
- Retours
- Rapports d’audits internes