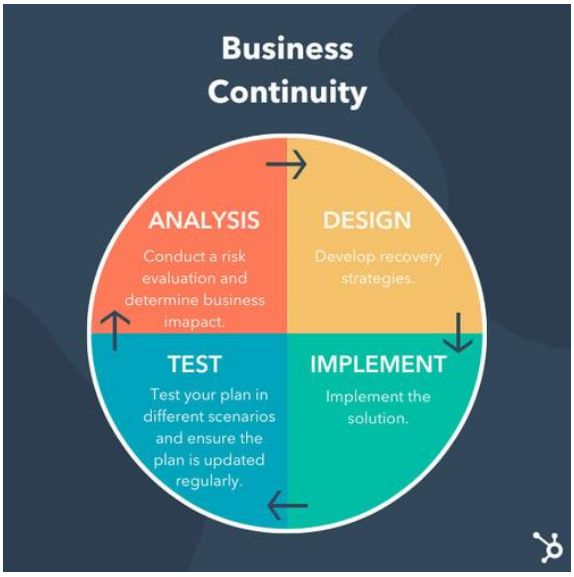
Systèmes de Management de la Continuité d'Activité

Meilleures pratiques et mise en œuvre de la norme ISO 22301

N° de la lecture individuelle :	5
Semestre	4
Étudiant	DAVID Guillaume, 803_1F
Sujet	Business Continuity Management



Support théorique

La recherche se base fondamentalement sur les documents présentés ci-dessous ainsi que de la recherche. Des apports, de l'aide à la construction des exemples, et des compréhensions ont également réalisés avec ChatGPT.

Support (livre)

Systèmes de Management de la Continuité d'Activité - Meilleures pratiques et mise en œuvre de la norme ISO 22301, 978-2-409-04271-3, 589 pages, décembre 2023

Table des matières

Introduction

Un peu d'histoire

La gestion de la continuité d'activité trouve ses racines dans des récits anciens tels que celui de l'arche de Noé, illustrant la préservation de la vie face à une menace imminente. Cependant, son importance et son évolution rapide sont manifestes à travers des événements plus récents tels que la pandémie de Covid-19 et les attentats du 11 septembre 2001. Étudier ces moments clés de l'histoire nous permet de mieux comprendre comment la résilience organisationnelle s'est adaptée aux défis contemporains, fournissant des perspectives précieuses pour l'avenir de la gestion de la continuité d'activité.

L'émergence du management trouve ses racines dans l'histoire, avec des figures telles que James McKinsey et Henri Ford contribuant à façonner les pratiques modernes, tandis que des penseurs comme Henri Fayol ont posé les bases de concepts clés comme le cycle PDCA. L'adoption du terme "management" par les Anglo-Saxons a été influencée par sa racine française, "mesnager", évoquant la gestion et le pilotage d'une organisation.

La catastrophe de Fukushima en mars 2011, déclenchée par un séisme suivi d'un tsunami dévastateur au Japon, a non seulement provoqué une crise nucléaire majeure mais a également eu des répercussions mondiales sur la continuité d'activité. Les chaînes d'approvisionnement internationales ont été gravement affectées, mettant en lumière leur vulnérabilité et l'importance de les inclure dans les plans de continuité. De plus, elle a souligné le besoin de considérer les scénarios de crise extrêmes et a mis en évidence l'importance cruciale de la communication transparente et efficace en temps de crise. En France, l'événement a conduit à une réévaluation de la résilience des sites nucléaires et au lancement de projets de renforcement des infrastructures pour faire face aux risques environnementaux.

La pandémie de Covid-19 de 2020 a entraîné des changements majeurs dans les plans de continuité d'activité (PCA) des entreprises à travers le monde. L'adoption massive du télétravail a exigé des ajustements technologiques et des politiques nouvelles pour assurer la sécurité des employés et maintenir les opérations. La crise a révélé les vulnérabilités des chaînes d'approvisionnement mondiales, incitant les entreprises à diversifier leurs fournisseurs et à renforcer leur résilience.

La crise entre la Russie et l'Ukraine en 2022 a révélé les risques géopolitiques majeurs pour les entreprises, malgré des années de préparation axées principalement sur la pandémie. Cette escalade du conflit a mis en évidence leur vulnérabilité face à des événements imprévus. Pour y faire face, des structures de gestion de crise plus solides et une disponibilité accrue d'informations fiables et en temps réel sont devenues essentielles. Les entreprises ont dû anticiper une volatilité géopolitique croissante et des pénuries de matières premières, telles que le pétrole et le gaz naturel, tout en gérant la fatigue liée aux crises et la montée en flèche des cyberattaques.

Les concepts de base

Les concepts de base en gestion de la continuité d'activité sont fondamentaux pour comprendre les principes qui sous-tendent cette pratique.

La norme ISO 22301 est devenue une référence en matière de continuité d'activité pour les organismes. Elle définit les exigences pour mettre en place un système de management visant à assurer la continuité des activités. Cette norme est internationale et ses principes sont adaptés nationalement.

Un organisme, tel qu'une entreprise ou une organisation, possède sa propre structure de gouvernance et ses objectifs spécifiques. Il peut être public, privé ou non gouvernemental, et opérer dans divers secteurs.

La continuité d'activité se définit comme la capacité d'un organisme à maintenir la délivrance de produits et services malgré une perturbation. Cette capacité est essentielle pour tous les types d'organismes et implique la gestion efficace des interruptions et des délais, tout en maintenant un niveau de capacité acceptable.

La gestion de la continuité d'activité permet à un organisme de poursuivre ses opérations sans interruption significative en cas de perturbation. Elle implique souvent une approche graduelle pour restaurer les activités à un niveau acceptable, évitant ainsi une chute drastique de la productivité.

La résilience organisationnelle, essentielle en gestion de la continuité d'activité, est définie comme la capacité d'assimilation et d'adaptation dans un environnement changeant. La norme ISO 22316 fournit des lignes directrices pour renforcer la résilience des organismes en abordant des concepts clés tels que la gestion des risques, la planification stratégique et la culture organisationnelle.

Les menaces, selon la norme ISO 22301, sont des événements, des conditions ou des situations potentiellement préjudiciables qui peuvent perturber ou causer des dommages à une organisation. Elles peuvent provenir de diverses sources telles que les catastrophes naturelles, les incidents technologiques, les problèmes de chaîne d'approvisionnement, les crises sanitaires, l'instabilité politique et sociale, les événements climatiques extrêmes et les risques opérationnels. L'identification et l'évaluation de ces menaces sont essentielles pour mettre en place des mesures appropriées de prévention, de préparation et de réponse dans le cadre de la gestion de la continuité d'activité.

Les plans de continuité d'activité (PCA) sont des documents essentiels pour guider les organisations dans la gestion des interruptions majeures. Voici un aperçu des différents types de plans qui composent généralement un PCA :

1. **Plan d'urgence**
   Axé sur les mesures immédiates à prendre en cas d'incident majeur pour assurer la sécurité des personnes, limiter les dommages matériels et communiquer efficacement avec les parties prenantes.

2. **Plan de continuité d'activité (PCA)**
   Vise à maintenir les fonctions essentielles de l'organisation pendant une perturbation, en minimisant l'impact sur les opérations et en rétablissant les activités normales dans des délais acceptables.

3. **Plan de reprise après sinistre (PRAS)**
   Concerne la restauration des opérations normales après la résolution de l'incident perturbateur, en définissant les étapes pour récupérer les systèmes, les données et les processus critiques.

4. **Plan de gestion de crise**
   Fournit une structure et des procédures pour gérer efficacement une crise majeure, en définissant les rôles, les responsabilités, les protocoles de prise de décision et les actions à entreprendre pour atténuer les effets de la crise.

5. **Plan de communication de crise**
   Crucial pour assurer une communication claire et cohérente avec les parties prenantes internes et externes pendant une perturbation, en définissant les canaux de communication, les messages clés et les procédures de gestion des médias.

6. **Plan de sauvegarde des données**
   Essentiel pour assurer la protection et la disponibilité des informations critiques de l'organisation, en définissant les procédures de sauvegarde régulière des données, les mécanismes de récupération et les tests périodiques pour garantir l'intégrité des sauvegardes.

7. **Plan de gestion des ressources humaines**
   Aborde les aspects liés à la disponibilité du personnel clé et à la gestion des ressources humaines pendant une perturbation, en définissant les procédures de rappel du personnel, les politiques de travail à distance et les plans de relève pour les postes clés.

La structuration du PCA peut varier, mais il est essentiel de trouver un équilibre entre la complexité et la simplicité pour garantir son efficacité. La méthode de Resilient Shield offre un compromis approprié entre structure et simplicité, en proposant idéalement trois ou quatre types de plans associés à un ensemble de documents opérationnels.

Les exercices du plan de continuité d'activité (PCA) sont cruciaux pour valider et améliorer la préparation face aux crises. En simulant des scénarios réalistes, ces exercices permettent de tester les procédures établies, d'évaluer l'efficacité des équipements de secours et de former le personnel à réagir en cas d'urgence. Ils identifient également les lacunes du PCA et fournissent des opportunités d'amélioration continue. En résumé, les exercices du PCA sont essentiels pour maintenir la confiance de l'organisation dans sa capacité à faire face aux perturbations et à maintenir ses activités.

Normes, méthodologies et réglementations

Ouverture

Divers documents guident la conception des plans de continuité d’activité et de la résilience, révélant leur influence culturelle et géographique. Malgré la résistance de certaines méthodes, la normalisation vise à rationaliser cet éventail, tandis que la réglementation, notamment européenne, favorise une cohérence globale, comme illustré par le RGPD,

motivant une exploration à trois niveaux : mondial, européen, national, et incluant les contributions majeures des États-Unis dans ce domaine.

Les normes

Les normes ISO 22301 et ISO 22313

La norme ISO 22301 établit les exigences pour un système de management de la continuité d'activité (SMCA). Elle fournit un cadre complet et structuré pour aider les organisations à anticiper, prévenir, gérer et récupérer des incidents perturbateurs afin de maintenir la continuité de leurs activités vitales.

- Une meilleure préparation aux incidents et aux crises.
- Une réduction des perturbations et des temps d'arrêt.
- Une amélioration de la résilience organisationnelle.
- Une meilleure protection de la réputation et de la confiance des parties prenantes.
- Une amélioration de l'efficacité et de l'efficience des opérations.

Basée sur une approche de gestion de risques, cela signifie que les organisations doivent identifier et évaluer les risques susceptibles de perturber leurs activités. En comprenant les risques, les organisations ont la capacité de mettre en place des mesures préventives et des plans de continuité adaptés. Cette approche proactive permet de mieux anticiper les incidents et de réduire leur impact sur l'organisation.

La norme ISO 22301 définit les exigences relatives à la planification, à la mise en œuvre, au fonctionnement, à la surveillance et à l'amélioration continue du système. En adoptant cette norme, les organisations disposent d'un cadre solide pour gérer efficacement la continuité de leurs activités et s'assurer de faire face aux incidents majeurs.

Les normes sur la résilience ISO 22316 et ISO 22336

La norme ISO 22316 fournit des lignes directrices pour renforcer la résilience organisationnelle, en mettant l'accent sur une approche systématique et holistique. Elle couvre la compréhension du contexte, le leadership et l'engagement, l'évaluation de la résilience, la planification et la mise en œuvre, ainsi que la mesure et l'amélioration continue.

- Compréhension du contexte : évaluation de l'environnement interne et externe.
- Leadership et engagement : importance d'un leadership engagé et d'une culture favorable à la résilience.
- Évaluation de la résilience : identification des forces et faiblesses de l'organisation.
- Planification et mise en œuvre : élaboration de stratégies et définition d'objectifs.
- Mesure et amélioration continue : évaluation des performances et apprentissage organisationnel.

La norme ISO 22336, en cours de finalisation, offre des conseils sur le développement d'une capacité stratégique pour anticiper et répondre au changement. Elle aborde la compréhension de la résilience, l'identification des risques, l'élaboration et la mise en œuvre de stratégies, ainsi que le suivi et l'amélioration de la résilience.

La norme ISO 22316 se concentre sur le renforcement de la résilience organisationnelle face aux défis et changements imprévus, tandis que la norme ISO 22336 offre des conseils pour développer une capacité stratégique à anticiper et répondre au changement.

La norme ISO 27001

L'ISO 27001 est une norme internationale qui guide la création, la mise en œuvre et l'amélioration continue d'un système de management de la sécurité de l'information (SMSI). Ce système assure la confidentialité, l'intégrité et la disponibilité des informations, tout en gérant les risques de manière adéquate. Divisée en dix sections principales, elle couvre divers aspects tels que la planification, le leadership et l'amélioration. Complémentaire à l'ISO 22301 sur la continuité d'activité, l'ISO 27001 offre des synergies en matière de gestion des risques et de sécurité informatique, permettant une meilleure préparation face aux exigences de la continuité d'activité. En outre, leur structure commune facilite leur intégration et offre des possibilités d'optimisation, nécessitant cependant une étude de faisabilité pour confirmer leur applicabilité mutuelle.

Autres normes

En plus des normes ISO telles que l'ISO 27001 et l'ISO 22301, d'autres référentiels et standards sont disponibles, notamment :

- Autres normes ISO spécifiques à des domaines particuliers, comme l'ISO 9001 pour la qualité ou l'ISO 14001 pour l'environnement.
- Les directives du National Institute of Standards and Technology (NIST) aux États-Unis, telles que le Framework NIST pour l'amélioration de la cybersécurité des infrastructures critiques.
- Les normes et directives de l'Union européenne en matière de sécurité de l'information et de continuité des activités.
- Les lois nationales et réglementations propres à chaque pays en matière de sécurité de l'information et de continuité des activités.

Cet éventail de références offre aux organisations une variété d'options pour répondre à leurs besoins spécifiques en matière de sécurité et de résilience.

Les méthodologies

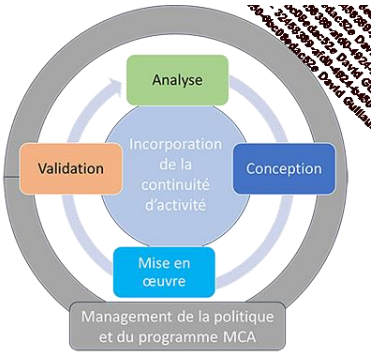
Chacune de ces méthodologies offre des approches complètes pour la gestion de la continuité d'activité, avec des éléments spécifiques qui peuvent être adaptés en fonction des besoins et des contextes organisationnels.

Méthodologie du DRII (Disaster Recovery Institute International) :

- Axée sur la continuité d'activité professionnelle.
- Approche globale couvrant la préparation, la réponse et la reprise après sinistre.
- Met l'accent sur un leadership engagé, une approche basée sur les risques, l'implication des parties prenantes, des processus documentés et des tests réguliers.
- Évaluation des risques, planification de la continuité d'activité, préparation et entraînement, réponse à l'incident, reprise après sinistre sont les étapes clés.
- Formation et certification internationale disponibles.

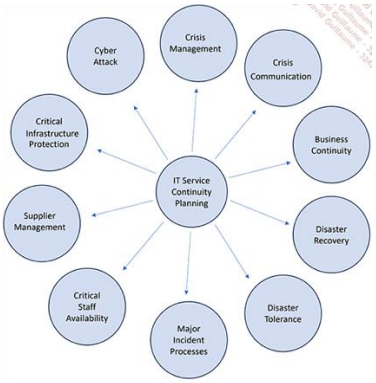
Méthodologie du BCI (Business Continuity Institute) :

- Met l'accent sur la préparation, la réponse et la reprise après sinistre.
- Évaluation approfondie des risques, planification détaillée, tests réguliers, formation des employés et certification professionnelle sont des éléments clés.
- Propose un système de certification professionnelle reconnu.
- Se distingue par une forte orientation régionale, avec une influence européenne marquée.
- Cycle comprenant six pratiques, dont deux de management et cinq techniques.



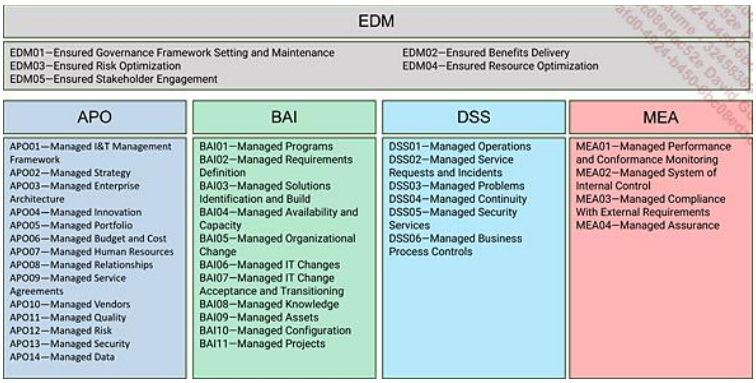
ITIL (Information Technology Infrastructure Library) et la gestion de la continuité d'activité :

- Intègre la gestion de la continuité d'activité pour assurer la résilience des services informatiques en cas d'incidents majeurs.
- Processus de gestion de la continuité des services (BCM) : analyse des besoins, évaluation des risques, développement de plans de continuité, tests et exercices réguliers, maintenance et amélioration continue.
- Couvre les aspects de gestion des services informatiques, y compris la continuité d'activité.
- Offre un cadre structuré pour la conception, la livraison et le soutien de services de qualité.



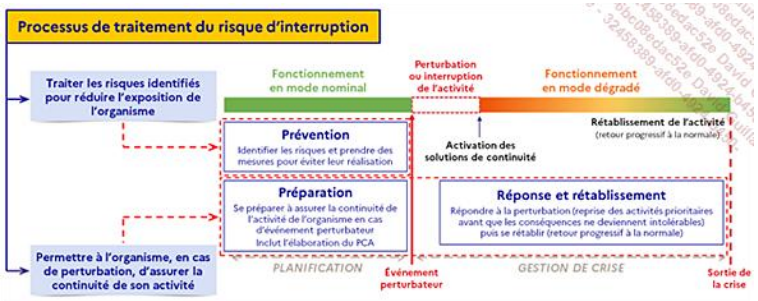
Gouvernance et continuité d'activité selon COBIT 2019

- COBIT est un cadre de référence pour la gouvernance et la gestion des systèmes d'information (SI), développé par l'ISACA.
- Il vise à aligner les SI sur les objectifs commerciaux, assurant ainsi une gouvernance efficace et une amélioration continue.
- COBIT 2019 définit cinq domaines : Évaluer, Diriger et Surveiller (EDM), Aligner, Planifier et Organiser (APO), Construire, Acquérir et Implémenter (BAI), Livrer, Servir et Supporter (DSS), et Surveiller, Évaluer et Analyser (MEA).
- Ces domaines couvrent un ensemble de processus visant à réduire les interruptions, améliorer la productivité et minimiser les coûts.



La méthode PCA du Secrétariat général de la défense et de la sécurité nationale (SGDSN)

- La méthode PCA du SGDSN a été récemment mise à jour en 2023 pour intégrer les concepts contemporains de résilience et de continuité des activités.
- Contrairement à la norme ISO 22301, cette méthode ne repose pas sur un système de management, mais offre une approche exhaustive de la conception des plans de continuité d'activité.
- Elle intègre la gestion de crise et couvre une variété de risques.
- En combinant cette méthode avec l'ISO 22301, les organisations peuvent bénéficier des avantages des deux approches pour une gestion efficace de la continuité des activités.



Les réglementations

Un écosystème réglementaire dense et varié encadre la continuité des activités, la résilience et la gestion des crises à travers différentes juridictions et secteurs d'activité. Des réglementations européennes, nationales et sectorielles telles que la directive européenne sur la résilience des infrastructures critiques, la loi française sur la sécurité civile, ou encore les normes internationales comme Solvabilité II dans le domaine de l'assurance, établissent des cadres essentiels pour promouvoir la stabilité, la sécurité et la préparation face aux défis et aux risques auxquels sont confrontées les entreprises et les institutions.

Ces réglementations offrent non seulement des directives, mais également des exigences et des normes à suivre, contribuant ainsi à renforcer la confiance des parties prenantes et à garantir la robustesse des organisations dans un monde en constante évolution.

Bonnes pratiques

Pour naviguer efficacement à travers les obligations réglementaires et établir une gestion solide de la continuité d'activité, deux questions clés se posent :

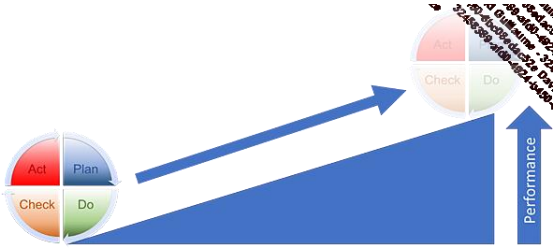
1. Quelles sont les obligations réglementaires auxquelles nous devons répondre en fonction de la nature de nos activités et de la localisation de notre organisme ?
2. Compte tenu de ces obligations et de notre culture d'entreprise, quel référentiel méthodologique est le plus approprié ?

Système Management de la Continuité des Activités (SMCA)

Analyse de risques

Un système de management, tel que défini par l'ISO, est l'ensemble des processus par lesquels une organisation gère ses activités pour atteindre ses objectifs. Analogiquement comparable au système immunitaire, il protège contre les risques et améliore les performances. Ses éléments, tels que des employés formés, des politiques claires et un processus d'amélioration continue, agissent ensemble comme des cellules immunitaires combattant les menaces. Tout comme l'immunité, un système de management efficace s'adapte en permanence à un environnement changeant, soulignant ainsi son importance cruciale pour la survie et la réussite organisationnelle.

La route de Deming



La roue de Deming, également connue sous le nom de cycle PDCA (Plan-Do-Check-Act), représente une caractéristique essentielle du système de management. Ce cycle consiste en quatre phases successives où chaque tour de roue vise à améliorer la performance globale. Planifier les actions, les mettre en œuvre, les contrôler et ajuster en conséquence sont les étapes clés de ce processus. L'objectif est d'assurer que chaque action programmée contribue positivement et mesurablement à l'amélioration continue de l'organisation. Cette approche dynamique nécessite une remise en question constante pour se rapprocher des objectifs et renforcer les capacités de l'organisme à remplir sa mission.

Phase	Explications
Planifier (*Plan*)	Établir une politique, des objectifs, des cibles, des contrôles, des processus et des procédures de continuité des activités pertinents pour améliorer la continuité des activités en vue de fournir des résultats conformes aux politiques et objectifs généraux de l'organisation.
Développer (*Do*)	Mettre en œuvre et faire fonctionner la politique, les contrôles, les processus et les procédures de continuité des activités.
Contrôler (*Check*)	Surveiller et passer en revue les performances par rapport à la politique et aux objectifs de continuité des activités. Communiquer les résultats à la direction pour examen. Déterminer et autoriser les actions de correction et d'amélioration.
Ajuster (*Act*)	Maintenir et améliorer le SMCA en prenant des mesures correctives sur la base des résultats de la revue de direction et en réévaluant la portée du SMCA, la politique et les objectifs de continuité des activités.

La mise en œuvre des quatre phases du cycle PDCA engendre un cercle vertueux d'amélioration du système de management. Ce processus prend son envol lors de la phase "Contrôler", où les dysfonctionnements et les opportunités d'amélioration sont repérés, fournissant ainsi une base de connaissances pour la maintenance évolutive. Il est crucial de reconnaître que le système de management est une entité complexe qui agit sur l'organisation, ses composantes étant constituées de personnes avec des responsabilités bien définies. Sa programmation n'est pas basée sur des circuits, mais sur des procédures.

Le système de management appliqué à la continuité d'activité

La norme ISO 22301 applique le concept de système de management à la continuité d'activité, similaire au système de management de la sécurité de l'information (SMSI) décrit dans l'ISO 27001. Elle définit le système de management de la continuité d'activité (SMCA) comme un système destiné à assurer la continuité des opérations. Cette norme précise que le SMCA comprend la structure de l'organisme, les politiques, les activités de planification, les responsabilités, les procédures, les processus et les ressources. La lecture de l'ISO 22301 offre les explications nécessaires pour créer le SMCA, incluant des documents descriptifs, des plans, des procédures, des checklists, des présentations, et des politiques. Elle recommande également des pratiques qui, bien que non impératives, sont bénéfiques pour renforcer le

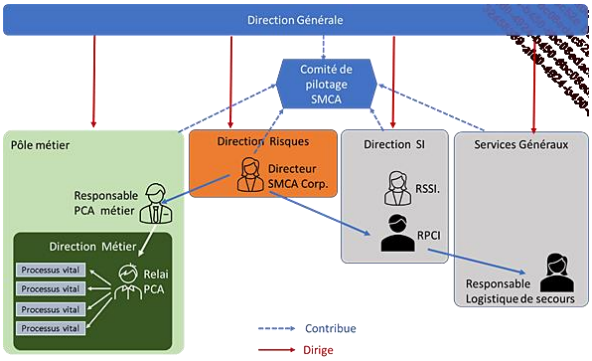
SMCA. Investir dans ces pratiques peut ultimement justifier l'efficacité et la performance du système de gestion de la continuité d'activité.

La politique de continuité d'activité

La politique de continuité d'activité, élément crucial d'un système de management, représente les intentions et orientations officielles de l'organisme en matière de continuité d'activité. Sa rédaction est guidée par la norme ISO 22301, mais dans la pratique, elle nécessite une collaboration étroite avec la direction pour être approuvée. La rédaction du premier brouillon est relativement simple, mais les itérations subséquentes impliquant la direction peuvent être plus laborieuses. Il est courant d'envisager plusieurs réunions avec la direction pour parvenir à un consensus sur le contenu de la politique. En plus des besoins et des désirs de la direction, la politique doit également être en accord avec les impératifs externes tels que la réglementation, la législation et la stratégie commerciale de l'entreprise. Pour garantir cette conformité, des ateliers de travail, utilisant des techniques de résolution de problèmes comme le brainstorming, peuvent être organisés pour impliquer efficacement la direction dans le processus de rédaction.

Leadership

Le leadership dans la continuité d'activité est formalisé dans la politique de continuité d'activité, où l'engagement de la direction est crucial pour le succès du projet, comme le confirme la norme ISO 22301. La désignation d'un responsable du SMCA est une responsabilité initiale de la direction, bien que souvent l'initiative de mettre en place un SMCA soit prise par celui qui dirigera le projet. Après avoir obtenu le feu vert de la direction, celle-ci doit continuer à contribuer activement tout au long du cycle du SMCA et lors de dates clés. Une organisation de pilotage et de gestion est nécessaire pour assurer la gestion à long terme du SMCA, comprenant un comité de pilotage de la continuité d'activité, présidé par le sponsor du SMCA, un responsable du SMCA, des équipes pour l'évolution du dispositif et des personnes chargées du contrôle de la performance du système.



Comment concevoir un SMCA ?

La démarche de conception du SMCA, similaire au reengineering de l'organisme, vise à transformer celui-ci pour répondre à des scénarios de crise. La première étape consiste à formuler la vision de la continuité d'activité, en comprenant la situation actuelle et la position future souhaitée. Des stratégies d'implémentation doivent être pensées pour générer des bénéfices à court, moyen et long terme. Le brainstorming est recommandé pour formuler cette vision, et un tableau de bord est conseillé pour mesurer les progrès. Les stratégies d'implémentation nécessitent des actions concrètes sur différents axes, comme l'axe humain, l'organisation et les processus.

Les étapes suivantes doivent être méthodologiquement réalisées et étudiées :

- La politique de gestion de la continuité d'activité.
- L'identification des risques et des menaces.
- L'analyse d'impact sur les activités de l'entreprise.
- La définition des stratégies de continuité.
- La mise en place et la gestion des plans de continuité d'activité.
- La formation et la sensibilisation des employés à la continuité d'activité.
- La gestion des incidents et des crises.
- La gestion des fournisseurs et des partenaires.
- La gestion des communications.
- La gestion de la reprise d'activité après une interruption.
- La réalisation d'exercices et de tests réguliers.
- La surveillance et la révision régulières du SMCA pour garantir son efficacité et son adaptation aux changements.

Ces actions doivent être mesurables à l'aide d'indicateurs. Le SMCA se formalise progressivement et inclut divers éléments tels que la politique de gestion de la continuité d'activité, l'identification des risques, la gestion des fournisseurs, etc. Des réunions et des ateliers de travail sont nécessaires pour recueillir les informations et formuler les lignes directrices du SMCA, le nombre dépendant de la complexité de l'organisme et de l'ambition du projet.

Exemple :

Entreprise : [Nom de l'entreprise]
Auteur : S.Hesschentier
Version : 1.0 du 12/12/2023
Gestion documentaire et diffusion : xxxxxxx

1. Introduction

Le système de management de la continuité d'activité (SMCA) de [Nom de l'entreprise] est conçu pour garantir la résilience de nos activités et la continuité de nos services face aux incidents perturbateurs. Ce document définit les politiques, les procédures et les responsabilités associées à notre SMCA, en alignement avec les normes fictives de continuité d'activité (ex. norme NCA 2023).

2. Objectifs

Les objectifs de notre SMCA sont les suivants :

a) Identifier les risques et les menaces susceptibles d'affecter la continuité de nos activités.
b) Développer des plans de continuité d'activité pour assurer la reprise rapide et efficace de nos services.
c) Mettre en place un système de surveillance et de gestion des incidents pour minimiser les interruptions d'activité.
d) Former et sensibiliser nos employés à la continuité d'activité et aux procédures d'urgence.
e) Réaliser des exercices et des tests réguliers pour évaluer et améliorer notre résilience opérationnelle.

3. Responsabilités

3.1 Direction
La direction de [Nom de l'entreprise fictive] est responsable des actions suivantes :
Établir la politique de continuité d'activité et fournir les ressources nécessaires pour sa mise en œuvre.
Nommer un responsable de la continuité d'activité (RCA) chargé de superviser le SMCA et d'assurer sa conformité aux exigences.
Examiner régulièrement les résultats des évaluations de risques et des tests, et prendre des mesures correctives et préventives.
3.2 Responsable de la continuité d'activité (RPCA)
Le RPCA est responsable des actions suivantes :
Élaborer et mettre en œuvre le SMCA en conformité avec la politique de continuité d'activité de l'entreprise.
Superviser les activités de continuité d'activité et coordonner les différentes parties prenantes internes et externes.
Mettre à jour et maintenir les plans de continuité d'activité, les procédures d'urgence et les mesures de sauvegarde et de reprise.
Assurer la formation des employés et la sensibilisation à la continuité d'activité.
Coordonner les exercices de simulation et les tests réguliers pour évaluer l'efficacité du SMCA.
3.3 Responsables de la gestion des risques
Les responsables de la gestion des risques sont chargés des actions suivantes :
Identifier et évaluer les risques et les menaces pouvant affecter la continuité des activités.
Mettre en place des mesures de prévention, de mitigation et de réponse aux risques identifiés.
Surveiller les tendances et les évolutions des risques, et proposer des ajustements au SMCA en conséquence.
3.4 Responsables des services opérationnels
Les responsables des services opérationnels sont responsables des actions suivantes :
Contribuer à l'identification des activités critiques et à l'évaluation de leur impact sur la continuité d'activité.
Coopérer avec le RCA pour élaborer et maintenir les plans de continuité d'activité spécifiques à leurs services.
Assurer la mise en œuvre des procédures d'urgence et des mesures de sauvegarde pour assurer la reprise rapide des opérations.
3.5 Composition et responsabilités du comité de pilotage :
Directeur général : directeur du comité
RPCA : animateur
RSSI : expert et rédacteur du rapport
Participants : [Insérer les noms et fonctions des participants]

4. Procédures clés

4.1 Analyse d'impact sur les activités (BIA)

La procédure BIA est utilisée pour identifier les activités critiques, évaluer leur impact sur la continuité d'activité et déterminer les objectifs de temps de reprise (RTO) et les objectifs de point de récupération (RPO) associés. Les étapes de la procédure BIA comprennent les éléments suivants :

Identification des activités critiques et des dépendances.

Évaluation de l'impact des interruptions d'activité sur les opérations, les clients, les partenaires et les parties prenantes.

Détermination des RTO et des RPO en fonction des objectifs de continuité d'activité de l'entreprise.

4.2 Plan de continuité d'activité (PCA)

Le plan de continuité d'activité est élaboré en fonction des résultats de la procédure BIA et fournit les directives et les procédures détaillées pour assurer la reprise des activités essentielles. Les éléments clés du PCA incluent ceci :

Les responsabilités et les rôles des équipes de gestion de crise et des membres clés du personnel.

Les procédures d'activation du plan de continuité d'activité en cas d'incident.

Les plans de communication pour informer les parties prenantes internes et externes des actions en cours.

4.3 Gestion des incidents

La procédure de gestion des incidents vise à détecter, à évaluer et à gérer les incidents pouvant affecter la continuité d'activité. Les étapes de la gestion des incidents comprennent les éléments suivants :

La détection précoce des incidents grâce à une surveillance continue et à des mécanismes d'alerte.

L'évaluation rapide de l'impact et de la gravité de l'incident.

La mise en place de mesures de réponse appropriées pour minimiser les perturbations et restaurer les opérations normales.

5. Formation et sensibilisation

[Nom de l'entreprise] s'engage à fournir une formation et une sensibilisation régulières à tous les employés pour garantir une compréhension claire de leurs rôles et responsabilités en matière de continuité d'activité. Les activités de formation peuvent inclure les éléments suivants :

Des sessions de sensibilisation sur la continuité d'activité et les procédures d'urgence.

Des exercices de simulation et des tests réguliers pour évaluer les compétences et les connaissances des employés.

6. Exercices et tests

Des exercices et des tests réguliers sont réalisés pour évaluer l'efficacité du SMCA et pour identifier les opportunités d'amélioration. Ces activités peuvent inclure les éléments suivants :

Les exercices de simulation de crise pour évaluer les plans de continuité d'activité et les procédures d'urgence.

Les tests de reprise des systèmes informatiques critiques.

Les audits et les revues régulières pour évaluer la conformité aux politiques et aux procédures du SMCA.

7. Revue du SMCA et amélioration continue

Le SMCA de [Nom de l'entreprise fictive] est régulièrement revu pour s'assurer de sa pertinence et de son efficacité. Des revues internes et des évaluations externes sont réalisées pour

identifier les opportunités d'amélioration. Les résultats de ces revues alimentent les actions correctives et préventives visant à renforcer la résilience de l'entreprise.

8. Stockage du SMCA

Le SMCA est stocké sur le serveur de fichiers X2Y3Z dans le répertoire Risk sous forme de l'arborescence suivante :

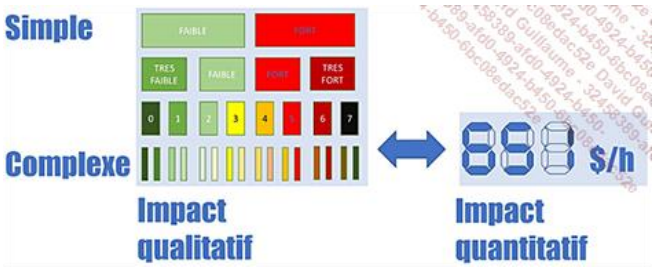
Décrire le répertoire SMCA

Bilan d'impact sur les activités (BIA)

Le BIA, ou Bilan d'Impact sur l'Activité, est essentiellement une évaluation approfondie des répercussions qu'une perturbation peut avoir sur les opérations d'une organisation. C'est comme une analyse approfondie des "et si" pour les affaires. Voici une structure ludique pour comprendre le BIA :

1. **Activités de l'organisation**
   Imaginez que l'organisation est un jeu avec plusieurs niveaux. Chaque niveau représente une activité essentielle, comme la comptabilité, le service client, la fabrication, la logistique, etc. Chaque niveau a ses propres règles et objectifs pour avancer dans le jeu.

2. **Impact**
   Si une perturbation survient, cela équivaut à l'apparition d'un obstacle dans le jeu. Cet obstacle peut être financier, de réputation, environnemental, etc. Plus l'obstacle est important, plus il est difficile pour les joueurs (c'est-à-dire l'organisation) de progresser.



3. **Maximum Acceptable Outage (MAO)**
   C'est comme un compte à rebours dans le jeu. Si le joueur n'arrive pas à surmonter l'obstacle dans un laps de temps défini, le jeu est terminé. Par exemple, si un site de commerce en ligne est hors service pendant trop longtemps, les clients vont aller jouer ailleurs.

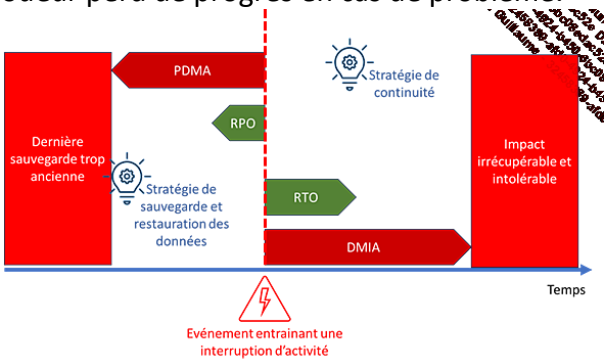
4. **Maximum Tolerable Period of Disruption (MTPD)**
   C'est comme la longueur maximale d'une panne qui ne met pas fin au jeu, mais qui le rend vraiment difficile à gagner. Par exemple, une banque peut tolérer une panne informatique d'une journée, mais si cela dure plus longtemps, ça devient vraiment difficile pour elle de continuer à jouer.

5. **Minimum Business Continuity Objectives (MBCO)**

Ce sont comme les "power-ups" ou les aides spéciales que les joueurs peuvent obtenir pour surmonter les obstacles. Ces aides sont essentielles pour que le joueur puisse continuer à jouer même lorsque les choses deviennent difficiles.

6. **Recovery Time Objective (RTO)**
   C'est le temps qu'il faut au joueur pour rétablir la situation après avoir rencontré un obstacle. Plus le RTO est court, plus vite le joueur peut revenir dans le jeu et continuer à avancer.

7. **Recovery Point Objective (RPO)**
   C'est comme la dernière sauvegarde que le joueur a faite dans le jeu. Si le joueur perd ses progrès après cette sauvegarde, il doit recommencer depuis ce point-là. Plus le RPO est court, moins le joueur perd de progrès en cas de problème.



Le BIA est comme une carte au trésor dans le jeu des affaires. Il aide les organisations à identifier les obstacles, à trouver les meilleures stratégies pour les surmonter et à garder le jeu en cours, peu importe ce qui se passe.

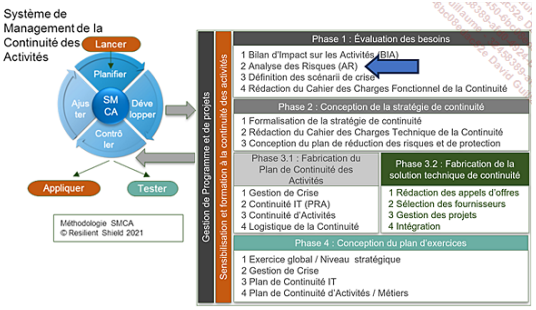
L'analyse des risques

L'analyse des risques dans le contexte de la continuité

L'analyse des risques est une étape cruciale dans l'évaluation des besoins, intervenant après le bilan d'impact sur l'activité. Cette approche permet de focaliser l'attention sur les processus vitaux, évitant ainsi la dispersion des ressources sur l'ensemble de l'organisme.

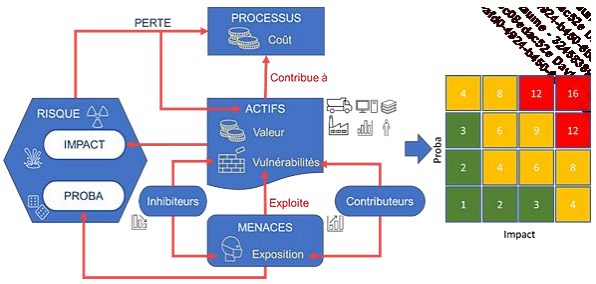
Sa complexité peut varier selon la taille de l'organisation, mais les principes sous-jacents restent simples et logiques. Elle est généralement partagée entre différents dispositifs de management tels que la gestion des risques, la sécurité du système d'information ou encore la continuité d'activité, chacun ayant des objectifs spécifiques à atteindre.

Deux grandes catégories d'analyse des risques sont couramment utilisées : **quantitative** et **qualitative**. La première repose sur des données chiffrées et nécessite une compréhension solide des mathématiques, tandis que la seconde se base sur l'expérience et des données non chiffrées pour classer les menaces et obtenir une vision globale pour des décisions éclairées. Pour des raisons pratiques, les systèmes de gestion de la continuité d'activité intègrent souvent une analyse qualitative des risques, mieux adaptée à leurs besoins spécifiques.



Une définition du risque

La norme ISO 13335, bien qu'obsolète, a fourni un modèle de risque influent, tandis que la définition du risque selon l'ISO GUIDE 73:2009 comprend des précisions telles que l'effet pouvant être positif ou négatif et les objectifs pouvant être de nature diverse, ce qui influence la manière dont les risques sont qualifiés et gérés.

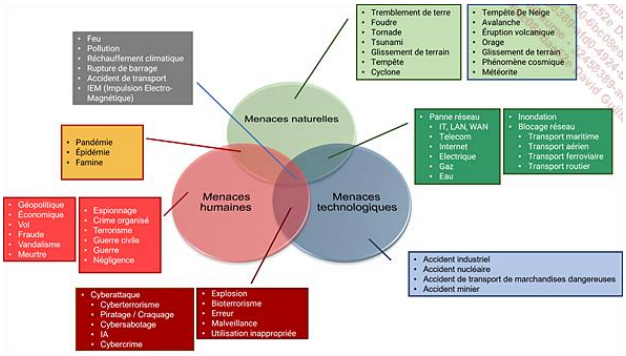


Les actifs

Les actifs d'une entreprise comprennent ses biens et ressources utilisés pour générer de la valeur ajoutée, regroupés en catégories telles que les infrastructures, les équipements, les produits et les ressources humaines, chacun étant exposé à des menaces et présentant des vulnérabilités, nécessitant parfois une évaluation simplifiée mais significative dans le cadre de la gestion de la continuité d'activité.

Les menaces

Le système de management de la continuité d'activité vise à identifier les menaces pouvant impacter l'organisme, qui peuvent être classées en catégories telles que les menaces **technologiques**, **humaines** et **naturelles**, chacune ayant des origines spécifiques et des caractéristiques propres en termes de probabilité et d'impact, nécessitant une analyse et une gestion adaptées pour prévenir les dommages potentiels aux actifs de l'entreprise.



Objectifs et exigences de l'analyse de risques

Les objectifs et exigences de l'analyse des risques dans le cadre du système de management de la continuité d'activité sont les suivants :

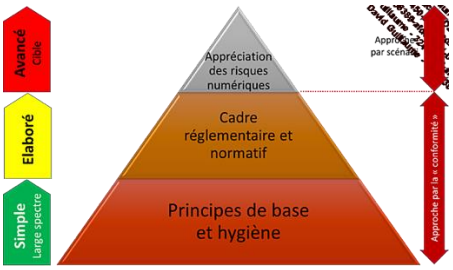
- Justification de la décision de mettre en place un système de management de la continuité d'activité en identifiant au moins un scénario plausible d'interruption des activités vitales de l'organisme, avec une menace associée.
- Établissement de priorités dans le traitement des scénarios d'interruption en tenant compte des contraintes budgétaires et de la pertinence des menaces.
- Adoption d'une approche proactive et réactive en combinant des mesures pour réduire l'impact ou la probabilité des menaces, en plus des mesures réactives pour assurer la continuité des activités.
- Définition de stratégies de traitement des scénarios de catastrophe en fonction de leur faisabilité, simplicité et coût, avec une évaluation des risques réels pour l'organisation.
- Contribution à la conception d'exercices réalistes en concevant des scénarios basés sur des risques envisageables et en tenant compte des limites du plan de continuité d'activité.
- Utilisation de toute méthode d'analyse des risques sérieuse répondant à ces objectifs, compatible avec les besoins de l'organisme et basée sur des résultats suffisamment récents pour être représentatifs.

Choisir sa méthode d'analyse des risques

Les méthodes d'analyse des risques mentionnées dans le texte sont les suivantes :

1. **Méhari**
   Méthode développée par le Club de la sécurité informatique français (Clusif), disponible en deux versions (Mehari classique et Mehari Manager BC). Utilise une base de connaissances sous forme de formulaires Excel pour guider l'analyse des risques.

2. **EBIOS**
   Méthode développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), structurée en sept étapes, axée sur une approche pluridisciplinaire et la prise en compte des besoins de sécurité des systèmes d'information.



3. **OCTAVE**
   Cadre de gestion des risques informatiques divisé en trois phases (évaluation organisationnelle, évaluation de l'infrastructure, élaboration d'une stratégie et de plans de sécurité), flexible et adaptable aux besoins spécifiques de chaque organisation.

4. **Arbres de défaillance, arbres d'événements et papillon**
   Méthodes d'analyse des risques qui permettent d'identifier les défaillances potentielles d'un système ou d'un processus, d'évaluer leurs conséquences et de hiérarchiser les risques en fonction de leur importance.

5. **Réseaux de Bayes**
   Méthode d'analyse probabiliste permettant de modéliser les relations de cause à effet entre les différentes variables d'un système, utilisée pour évaluer les probabilités des événements et des conséquences dans les arbres de défaillance.

6. **AMDEC**
   Méthode d'analyse de fiabilité largement utilisée dans divers domaines industriels, permettant d'identifier les modes de défaillance potentiels d'un système, d'évaluer leurs effets et de déterminer leur criticité.

7. **...**

Ces méthodes varient en termes d'approche, de complexité et d'applicabilité, et chacune peut être adaptée en fonction des besoins spécifiques de l'organisation ou du système à analyser.

Stratégie de continuité d'activité

Qu'est-ce qu'une stratégie ?

La stratégie est une approche globale et à long terme qui consiste à combiner diverses actions pour atteindre un objectif spécifique. À l'origine un concept militaire, la stratégie a évolué pour s'appliquer à divers domaines, y compris les affaires, la gestion de projet et la vie personnelle.

En comparaison, la tactique se concentre sur des actions à court terme et dans un contexte spécifique, tandis que la stratégie prend en compte une vision plus large et à long terme.
Dans le contexte de la continuité d'activité, la stratégie joue un rôle crucial dans la planification et la préparation aux crises et aux situations d'urgence. Les objectifs de la stratégie de continuité peuvent être de niveau stratégique, tactique ou opérationnel, en fonction de leur portée et de leur impact sur l'organisation.

Il est important de reconnaître que tous les niveaux d'action dans la gestion de la continuité d'activité sont importants, et qu'ils se complètent mutuellement pour assurer la résilience de l'organisation face aux perturbations.

Principes des stratégies de continuité d'activité

Les stratégies de continuité d'activité sont élaborées pour garantir la reprise des activités essentielles face à divers scénarios de crise, en tenant compte de trois niveaux de perturbation potentielle : stratégique, tactique et opérationnel.

- **Niveau Stratégique**: Les crises peuvent impacter les produits et services, nécessitant une planification stratégique de la continuité.
- **Niveau Tactique**: Les infrastructures peuvent être affectées, exigeant une approche tactique dans la planification.
- **Niveau Opérationnel**: Les processus de production peuvent être perturbés, nécessitant une planification opérationnelle.
-

La construction des stratégies de continuité repose sur des bases établies lors de l'identification et de l'analyse des impacts (BIA), prenant en compte les délais maximums d'indisponibilité admissible (DMIA) et les objectifs de temps de réponse (OTR). Ces stratégies doivent atteindre un OTR cible tout en respectant un budget défini.

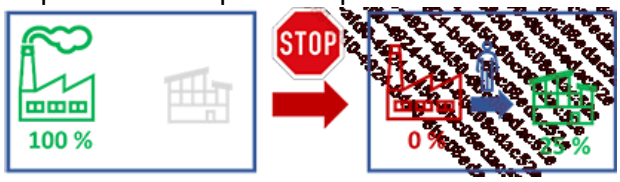
Les 7 stratégies de continuité d'activité sont :

1. **Ne rien faire**
   Cette stratégie reconnaît que toutes les activités ne nécessitent pas une réponse immédiate en cas de crise. Certains processus peuvent rester en "stand-by" jusqu'au retour à la normale.

2. **Diversification**
   La diversification implique la répartition des ressources et des activités sur différents sites géographiques pour faire face aux interruptions en transférant les activités vers d'autres sites fonctionnels.

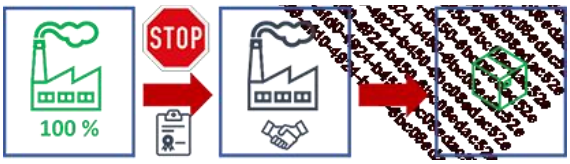
3. **Réplication**
   Cette stratégie consiste à établir un site de remplacement contenant toutes les ressources nécessaires, inactif jusqu'à ce qu'une interruption survienne sur le site principal.

4. **Site de repli ou site de secours**
   C'est une version allégée de la réplication, permettant d'accueillir une partie du personnel vital et des processus les plus critiques.



5. **Acquisition post-incident**
   Implique l'acquisition rapide ou la reconstruction des actifs critiques après un incident majeur pour rétablir les opérations et minimiser les perturbations.

6. **Sous-traitance**
   Délégation de certaines fonctions clés à des tiers pour assurer la continuité des opérations en cas d'interruption, offrant flexibilité, expertise spécialisée, et gestion des risques.



7. **Assurance**
   Transfert d'une partie des risques et des coûts associés à une interruption des opérations à un assureur, atténuant ainsi les conséquences financières d'un incident

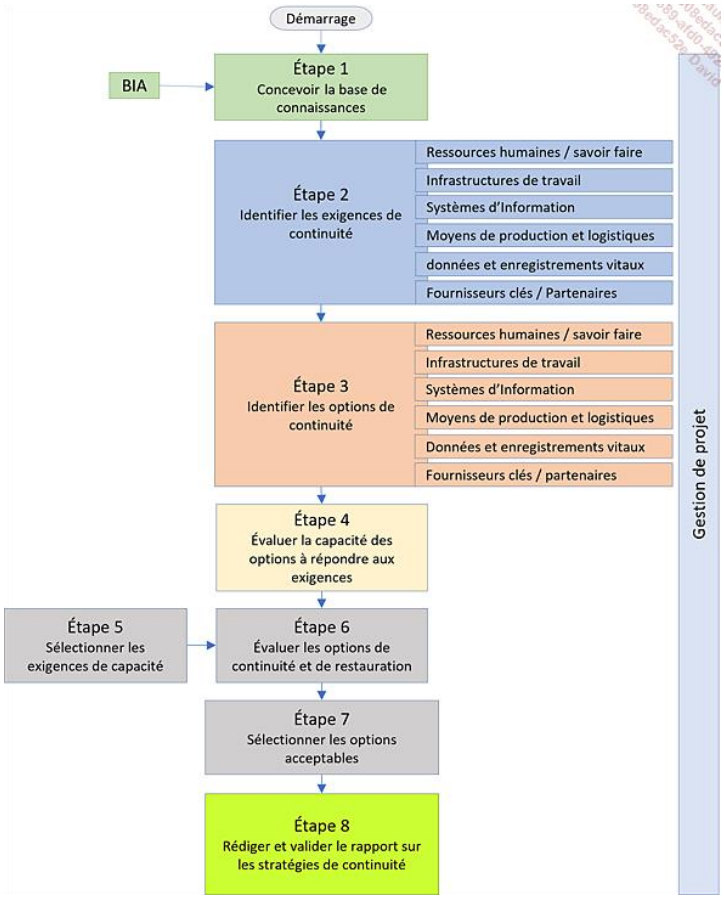
majeur. Cela comprend l'assurance de biens, de responsabilité civile et de perte d'exploitation.

Chaque stratégie présente ses avantages et ses inconvénients, et leur sélection dépend des besoins spécifiques et des ressources disponibles de l'organisation.

Méthode de conception des stratégies de continuité d'activité

Ce processus repose sur l'implication d'un groupe d'experts chargés de développer des stratégies pertinentes pour garantir la continuité des activités. Ces experts doivent se baser sur une base de connaissances regroupant toutes les informations et les besoins exprimés lors des activités précédentes. Les résultats de l'analyse d'impact sur les activités (BIA) et de l'analyse des risques constituent les principaux éléments de cette base d'informations. Ainsi, pour bien démarrer, il est essentiel de connaître ce qui a déjà été acquis et d'identifier les domaines nécessitant encore des éclaircissements.

Le processus de conception des stratégies de continuité d'activité comprend huit étapes :



Les erreurs à éviter

Voici une liste des erreurs à éviter dans la gestion de la continuité d'activité :

1. **Tout miser sur le télétravail**
   Le télétravail peut être efficace dans certaines situations, mais il présente des limites et des risques, notamment en cas de dépendance excessive aux infrastructures technologiques, de vulnérabilités en matière de sécurité, et de besoins d'une présence physique sur site pour certaines activités.

2. **Copier les tactiques des autres**
   Chaque organisation est unique, donc adopter les stratégies d'autres entreprises sans tenir compte des besoins spécifiques, des risques et des ressources peut conduire à des erreurs. Il est essentiel de personnaliser les stratégies en fonction du contexte et des priorités de chaque organisation.

3. **Écarter les scénarios peu probables**
   Négliger les stratégies pour des scénarios peu probables peut être une erreur, car même s'ils ont une faible probabilité, ils peuvent avoir un impact significatif et leur occurrence n'est pas impossible. Ignorer ces scénarios peut rendre une organisation vulnérable à des risques non anticipés et compromettre sa résilience.

Bibliographie

https://blog.hubspot.com/hs-fs/hubfs/Google%20Drive%20Integration/What%20Is%20A%20Business%20Continuity%20Plan%3F%20%5B+%20Template%20%26%20Examples%5D-Dec-21-2022-06-08-04-3501-PM.jpeg?width=500&height=500&name=What%20Is%20A%20Business%20Continuity%20Plan%3F%20%5B+%20Template%20%26%20Examples%5D-Dec-21-2022-06-08-04-3501-PM.jpeg

**Les images non référencées dans la bibliographie proviennent du livre ou document étudié.*