Chapitre 3
Le SMCA

1. Le système de management : définition et principes

"Un système de management est l'ensemble des processus par lesquels un organisme gère les éléments corrélés ou en interaction de ses activités afin d'atteindre ses objectifs".

Nous trouvons cette définition sur le site de l'ISO. Elle est donc exacte. Cependant, la nature profonde de ce qu'est réellement un système de management nous échappe encore à ce stade.

Le système de management est comme le système immunitaire d'une organisation. Il est responsable de la protection de l'organisation contre les risques et de l'amélioration de ses performances dans un environnement changeant. Tout comme le système immunitaire, le système de management est composé de nombreux éléments qui travaillent ensemble pour identifier et combattre les menaces.

Certains des éléments du système de management sont les suivants :

– Des employés formés et motivés.
– Des politiques et des procédures claires et concises.
– Un système de surveillance et de suivi efficace.
– Un processus d'amélioration continue.

En poursuivant l'analogie que nous avons proposée : les employés combattent les menaces de l'organisation comme les lymphocytes éliminent les germes de la maladie. Les procédures sont le code génétique qui reprogramme la résilience des cellules. La direction de l'entreprise est comme le cerveau, elle ne traite pas directement les conséquences de l'infection mais elle influence son évolution en facilitant le travail du système immunitaire.

Immunité

Un système de management efficace permet à une organisation de se protéger contre les risques et de réussir dans un environnement complexe et en constante évolution. Tout comme le système immunitaire, le système de management est un système dynamique qui s'adapte en permanence aux nouvelles menaces. Il est donc essentiel pour les organisations d'investir dans un système de management solide et efficace.

Les systèmes organisés que nous avons créés sont, en quelque sorte, à notre image. Les entreprises doivent s'adapter en permanence au marché dans lequel elles évoluent. Les produits qu'elles vendent et les processus qui les animent doivent répondre à la demande et évoluer de la même manière que les êtres vivants : naître, grandir et s'adapter ou mourir.

Le premier système de management certifiable est né en 1987 et concerne la qualité. Il formalise ce qui était auparavant transmis de génération en génération dans les entreprises qui se maintiennent en tête du peloton : les principes et les procédures de bonne gouvernance.

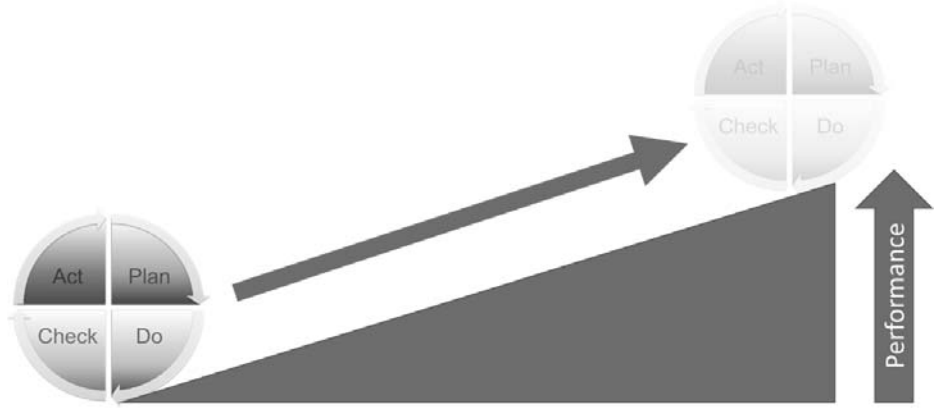
Nous devons développer la définition du système de management pour en comprendre la composition. Les éléments clés sont des processus, donc nous devons concrètement rédiger des procédures de fonctionnement, des documents descriptifs et des politiques (autrement dit, les intentions de l'organisme et ses objectifs tels qu'ils sont formulés par la direction).

La norme ISO 22301 apporte les précisions nécessaires à notre compréhension. Elle indique ainsi les composantes clés du système :

– Les rôles et les responsabilités.
– La structure du système.
– La planification, c'est-à-dire la "partie du management consacrée à définir les objectifs de continuité et à spécifier les processus opérationnels nécessaires et les ressources associées afin de remplir les objectifs de continuité d'activité (source ISO 22300).
– Le fonctionnement de l'organisme.

2. La roue de Deming

La plupart des systèmes de management comportent un principe d'amélioration continue. Il est illustré par la roue de Deming, appelée également "cycle PDCA".



Principe d'amélioration continue

En fait, la roue de Deming est une représentation symbolique d'une caractéristique majeure du système de management. Ce système est construit sur un cycle où quatre phases se succèdent : *Plan, Do, Check et Act*. Comme le montre l'image, la rotation de la roue permet d'atteindre un niveau supérieur de performance. À chaque tour, le système revient à la première phase et le cycle se reproduit.

Ce système mnémotechnique est souvent traduit en français par "Planifier - Développer - Contrôler - Ajuster". Bien évidemment, cette roue n'a aucune existence physique et vous n'êtes pas supposé la fabriquer. Il faut retenir de ce concept que toutes les actions qui sont programmées dans le système doivent apporter un progrès par rapport à la situation antérieure. Ce progrès doit être mesurable de manière objective. À l'inverse, certaines décisions peuvent éventuellement faire régresser le système et doivent être neutralisées rapidement. Nous sommes dans une approche dynamique qui doit être remise en cause à chaque instant afin de se rapprocher des objectifs et d'augmenter les capacités de l'organisme à accomplir sa mission.

La première version de la norme ISO 22301 comportait des explications sur les phases *Plan, Do, Check* et *Act* qui ne sont plus présentées dans la version actuelle. Voici les informations manquantes :

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.

Phase	Explications
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.

Dynamique d'amélioration

La mise en œuvre de ces quatre phases génère un cercle vertueux d'amélioration des composantes du système de management. Cette dynamique est déclenchée au niveau de la troisième phase, c'est-à-dire "Contrôler". Les dysfonctionnements et les opportunités d'amélioration sont identifiés au cours de cette période. Ils constituent la base de connaissance sur le système qui alimente le processus de maintenance évolutive mis en œuvre dans la phase suivante.

Nous devons prendre conscience que le système de management est une machine d'une nature particulière. Elle agit sur l'organisation. Dans ses entrailles, il n'y a pas de circuits ou des rouages mais des personnes avec des responsabilités et des rôles bien identifiés. La programmation du système n'est pas logicielle mais procédurale.

3. Les différents systèmes de management

L'ISO a développé plusieurs systèmes de management depuis celui de la qualité. À l'heure actuelle, ils concernent des domaines extrêmement variés. Seule une partie de ces documents présente un intérêt direct ou connexe au domaine de la continuité d'activité.

Les normes suivantes sont signalées "HS", pour *Harmonized Structure*, et disposent d'un corpus commun de termes et de définitions, et nous intéressent dans le cadre de la continuité d'activité :

Référence	Titre
ISO 22301:2019	Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences
ISO 22313:2020	Sécurité et résilience - Systèmes de management de la continuité d'activité - Lignes directrices sur l'utilisation de l'ISO 22301
ISO/IEC 27001:2022	Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences
ISO/IEC 27003:2017	Technologies de l'information -Techniques de sécurité -Systèmes de management de la sécurité de l'information - Lignes directrices
ISO 9001-2015	Systèmes de management de la qualité - Exigences
ISO/TS/ 9002:2016	Systèmes de management de la qualité - Lignes directrices pour l'application de l'ISO 9001

Cette convergence conceptuelle est intéressante pour les organismes qui souhaitent répondre à plusieurs systèmes de management. Ils peuvent alors mettre en place un système de management intégré qui répond à toutes les exigences sans apporter de coûteuses redondances entre les systèmes.

ISO

Un système de management intégré est une excellente idée vers laquelle tous les organismes ayant entrepris cette démarche doivent tendre. Une des difficultés importantes qui s'opposent à l'achèvement de ce système intégré réside dans la diversité des entités concernées. La qualité, la gestion des risques, la sécurité ou la continuité d'activité sont souvent confiées à des directions spécifiques qui n'ont pas de relations directes et hiérarchiques entre elles. La création d'un système de management unifié soulève donc des questions organisationnelles sérieuses, en particulier celle-ci : "Qui prend la direction du système ?". Le système de management intégré est donc le fruit d'un projet de reengineering à part entière qui demande la collaboration de compétences spécifiques : celle des systèmes de management eux-mêmes et des connaissances liées à la gestion du changement, la résolution de problèmes et l'organisation des ateliers de travail basés sur des techniques de brainstorming.

4. Le système de management appliqué à la continuité d'activité

La norme ISO 22301 a appliqué le concept de système de management à la continuité d'activité. Le système de management de la continuité d'activité (SMCA) comporte de nombreuses similitudes avec le dispositif décrit dans la norme ISO 27001 et appelé système de management de la sécurité de l'information, ou SMSI.

La définition apportée par la norme ISO 22301 au SMCA est évidente et simple : c'est un "système de management destiné à la continuité d'activité".

Elle précise également le contenu du SMCA : "la structure de l'organisme, les politiques, les activités de planification, les responsabilités, les procédures, les processus et les ressources". Cette définition synthétique ne donne pas une idée concrète de l'ampleur de la tâche.

La lecture de la norme ISO 22301 fournit toutes les explications dont vous avez besoin pour créer le SMCA. La récolte des informations nécessaires à la continuité d'activité et les fruits de votre réflexion sur les stratégies à mettre en œuvre génèrent le SMCA. Il comporte donc des documents descriptifs, des plans, des procédures, des checklists, des présentations pour réunions, des politiques, etc.

Le SMCA comporte non seulement la description de tous les processus nécessaires à la continuité d'activité mais également les enregistrements créés par l'exécution de ces processus. Par exemple, vous devez intégrer dans la base documentaire du SMCA la méthode d'analyse des risques, les questionnaires et checklist associées ainsi que les rapports créés à chaque application du processus d'analyse des risques.

Il est assez facile d'établir la liste des documents indispensables pour le SMCA. En général, ils sont formellement cités ou décrits dans la norme ISO 22301.

La norme comporte également des recommandations qui n'ont pas forcément un caractère impératif. Les documents associés sont donc plus souhaitables que nécessaires. Nous vous recommandons de ne pas faire d'économies inappropriées et de les prendre sérieusement en considération. Tôt ou tard, leur contribution à la performance du SMCA apporte la justification de l'investissement consenti.