Chapitre 3
Introduction aux systèmes de management

1. Introduction

Les entreprises performantes savent que pour atteindre leurs objectifs, elles doivent s'appuyer sur une organisation cohérente, des règles de fonctionnement claires, des responsabilités bien définies, et surtout une démarche d'amélioration continue. C'est là qu'intervient une notion centrale : le système de management. Mais alors, qu'est-ce que cela représente concrètement ? Et comment les systèmes de management fonctionnent ?

Si vous souhaitez en savoir plus, vous êtes au bon endroit.

2. Définition du système de management

Un système de management est un ensemble d'éléments interdépendants au sein d'une organisation qui interagissent pour établir des politiques, des objectifs et des processus afin d'atteindre ces objectifs de manière cohérente et durable. Il fournit un cadre structuré pour la planification, la mise en œuvre, le contrôle, l'évaluation et l'amélioration continue des activités d'une organisation dans un domaine spécifique.

Son objectif fondamental est de garantir que l'organisation fonctionne de manière cohérente, efficace et efficiente.

Cette logique de management structuré s'applique à de nombreuses thématiques auxquelles les organisations sont confrontées dans leur quotidien. C'est ainsi qu'ont émergé, sous l'impulsion de l'Organisation internationale de normalisation, plusieurs référentiels internationaux couvrant chacun un domaine spécifique : la qualité avec l'ISO 9001, l'environnement avec l'ISO 14001, la santé et la sécurité au travail avec l'ISO 45001, la continuité d'activité avec l'ISO 22301, et la sécurité de l'information avec l'ISO/IEC 27001.

Ces référentiels partagent tous une même architecture, une même philosophie et un même moteur : le cycle PDCA (planifier, déployer, contrôler, améliorer) qui garantit à l'organisation une démarche d'amélioration continue, rigoureuse et mesurable.

3. Principes fondamentaux du management

3.1 L'engagement de la direction générale

Mettre en place un système de management quel que soit le domaine concerné (qualité, sécurité de l'information, environnement ou santé, etc.) repose sur des principes fondamentaux que tout professionnel se doit d'adopter s'il souhaite garantir la réussite et la pérennité de sa démarche.

Le tout premier de ces principes est celui de l'engagement de la direction générale. En effet, il constitue le socle du système de management. C'est à la direction qu'il revient de donner du sens, de fixer les ambitions et de porter la vision. Elle est responsable de créer un alignement stratégique entre les objectifs du système et ceux de l'organisation dans son ensemble. Dans le cas d'un système de management de la sécurité de l'information (SMSI), cela signifie que la sécurité ne doit pas être traitée comme une simple question technique, mais comme un levier de confiance et de compétitivité. La direction doit afficher clairement sa volonté de protéger les actifs informationnels, de maîtriser les risques, de se conformer aux exigences légales et contractuelles, et d'instaurer une culture de sécurité à tous les niveaux de l'entreprise.

© Editions ENI - All rights reserved

Cet engagement s'exprime de différentes manières à savoir :

– la validation d'une politique claire et cohérente ;
– la définition d'objectifs mesurables ;
– la nomination de responsables compétents ;
– la mise à disposition des ressources humaines et financières ;
– la communication active sur l'importance de la sécurité de l'information à toutes les parties intéressées ;
– la réalisation de visites ;
– la présence de la sécurité de l'information comme point des réunions de direction ;
– la valorisation de l'engagement du personnel en matière de sécurité, au travers de promotions, de primes, de reconnaissance des bonnes pratiques ou d'autres gratifications ;
– le suivi des indicateurs clés de performance de sécurité.

Cette approche est loin d'être exhaustive, il convient aux dirigeants de traduire leur engagement par des actes répétés, visibles, structurants, qui montrent à l'ensemble des collaborateurs que la sécurité de l'information est un choix stratégique assumé par la plus haute autorité de l'organisation.

3.2 La mobilisation du personnel

Il convient pour la direction de faire en sorte que chaque employé comprenne pleinement les objectifs du système de management de la sécurité de l'information, perçoive clairement en quoi ceux-ci sont liés à ses missions quotidiennes, et se sente véritablement investi dans la réussite collective de l'organisation. Qu'il s'agisse d'un assistant administratif, d'un développeur, ou d'un agent de sécurité, chacun détient une part de responsabilité et contribue, par ses décisions et ses gestes, soit à renforcer la protection du patrimoine informationnel de l'entreprise, soit, à l'inverse, à exposer ce dernier à des vulnérabilités.

Cette culture peut être développée en réalisant les actions non exhaustives suivantes :

– des sessions de formation et de sensibilisation, adaptées aux profils et aux métiers ;
– des campagnes de phishing ;
– des stress test ;
– des communications via l'envoi de courriels, d'alertes, de newsletters internes ou de rappels contextuels.

3.3 L'approche par processus

Un processus se définit comme un ensemble d'activités corrélées qui transforment des éléments entrants en éléments sortants en produisant une valeur ajoutée. Cette transformation s'appuie sur des ressources humaines, techniques, etc. En effet, il permet d'avoir une vision globale et transversale de l'entreprise, d'optimiser les flux de travail et de mieux maîtriser les interactions entre les différentes activités. Plutôt que de considérer les activités de l'entreprise comme des tâches isolées ou des fonctions indépendantes, cette approche invite à penser et organiser l'entreprise comme un ensemble cohérent de processus interconnectés, chacun contribuant à la création de valeur et à l'atteinte des objectifs fixés.

Ces processus, bien qu'adaptés à chaque contexte spécifique, peuvent être regroupés en trois grandes catégories.

– Les processus de management : un processus de management est un ensemble structuré, coordonné et piloté d'activités décisionnelles visant à orienter, encadrer et contrôler l'organisation afin d'assurer l'atteinte durable de ses objectifs stratégiques. Il constitue le mécanisme de gouvernance par lequel la direction définit les orientations, alloue les ressources, fixe les priorités, évalue les performances et déclenche les actions correctives nécessaires.

© Editions ENI - All rights reserved

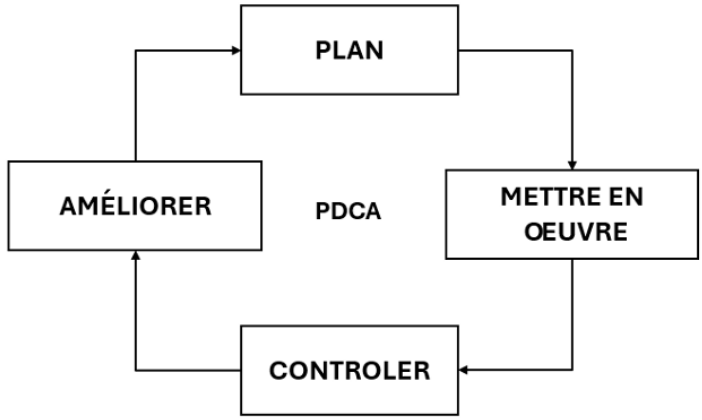
– Les processus opérationnels : aussi appelés processus métier ou processus de réalisation. Ils représentent l'ensemble des actions directement liées à la production et à la mise à disposition de produits ou services répondant aux attentes des clients et parties prenantes. Ce sont ces processus que le client perçoit et évalue directement. Leur performance détermine la qualité des produits et services fournis, et conditionne la satisfaction et la fidélité des parties prenantes. Dans une entreprise bancaire, les processus opérationnels couvrent l'ouverture et la gestion des comptes clients, l'octroi de crédits, le traitement des virements et des transactions, etc.
– Les processus support : les processus support sont les activités qui fournissent les ressources, les outils et les conditions nécessaires au bon fonctionnement des processus opérationnels et de management. Ils n'interviennent pas directement dans la production de produits ou services, mais leur contribution est indispensable à la performance globale de l'organisation. Ces processus ne sont pas directement visibles par le client, mais leurs carences dégradent inévitablement la qualité de l'offre. Une organisation dont les fonctions support sont vulnérables voit l'ensemble de son activité fragilisé à terme. Cela concerne aussi bien les ressources humaines que la comptabilité, la maintenance des équipements ou les systèmes d'information.

3.4 L'amélioration continue

L'amélioration continue est un processus permanent par lequel une organisation cherche à optimiser ses performances, ses pratiques et ses résultats de façon progressive et structurée. Elle se matérialise à travers le cycle PDCA dont chaque phase s'enchaîne naturellement à la suivante.

– Planifier (*Plan*) consiste à définir les objectifs à atteindre, à analyser la situation existante et à déterminer les actions à mettre en place pour combler les écarts identifiés.
– Déployer (*Do*) consiste à exécuter les actions planifiées en mobilisant les ressources humaines, techniques et organisationnelles nécessaires à leur réalisation.

– Contrôler (*Check*) consiste à mesurer les résultats obtenus, à les comparer aux objectifs fixés et à identifier les écarts et les points d'amélioration.
– Améliorer (*Act*) consiste à traiter les écarts constatés, à capitaliser sur les succès et à intégrer les enseignements tirés pour enrichir le cycle suivant.



Cycle PDCA

Remarque

Ce cycle ne s'arrête jamais. Chaque itération produit un niveau de maturité supérieur au précédent, permettant à l'organisation de progresser de façon continue.

© Editions ENI - All rights reserved

4. Les systèmes de management existants

Il existe aujourd'hui une grande diversité de systèmes de management, chacun conçu pour répondre à des enjeux spécifiques.

Bien qu'ils partagent une architecture commune, leurs champs d'application, leurs objectifs et leurs exigences diffèrent sensiblement.

– Le système de management de la qualité (SMQ), encadré par la norme ISO 9001, garantit la conformité des produits et services aux exigences des clients. Il instaure une culture de la qualité à tous les niveaux de l'organisation, réduit les défauts, optimise les processus internes et renforce la satisfaction comme la fidélisation des clients. L'ISO 9001 s'applique à toute organisation, quels que soient sa taille, son secteur d'activité ou son statut juridique.
– Le système de management de la continuité d'activité (SMCA), encadré par la norme ISO 22301, permet d'assurer la résilience face aux crises majeures. Il repose sur l'analyse d'impact sur l'activité, l'élaboration de plans de continuité et de reprise, ainsi que la réalisation de tests réguliers. Le SMCA garantit le maintien des activités critiques en cas d'incident grave.
– Le système de management environnemental (SME ISO - 14001) constitue un cadre structuré permettant à une organisation d'identifier, de maîtriser et de suivre les impacts environnementaux liés à ses activités, à ses produits et à ses services.

  Par ailleurs, il vise à améliorer de façon mesurable et durable la performance environnementale de l'organisation, à prévenir la pollution sous toutes ses formes, à optimiser l'utilisation des ressources naturelles et énergétiques, à garantir la conformité permanente aux exigences légales applicables, et à renforcer la crédibilité de l'organisation auprès de l'ensemble de ses parties prenantes.

– Le système de management de la protection de la vie privée (*Privacy Information Management System*), dont la norme de référence internationale est l'ISO 27701 est un cadre structuré qui vient étendre et compléter le système de management de la sécurité de l'information (SMSI - ISO 27001) en y intégrant des exigences spécifiques relatives à la protection des données à caractère personnel et à la gestion de la vie privée. Il constitue une réponse normative aux enjeux croissants de confidentialité des données dans un contexte de transformation numérique accélérée et de renforcement des législations sur la protection de la vie privée à l'échelle mondiale. Il permet à l'organisation de gérer de manière systématique, traçable et proactive les informations personnelles qu'elle traite, collecte, stocke ou transfère en établissant des règles claires de gouvernance des données personnelles, en définissant les rôles et responsabilités des acteurs impliqués dans leur traitement, en identifiant et en traitant les risques d'atteinte à la vie privée des personnes concernées, et en garantissant le respect des droits fondamentaux des individus.

– Le système de management anticorruption a pour norme de référence internationale l'ISO 37001. Cette norme spécifie les exigences et fournit des conseils pour l'établissement, la mise en œuvre, le maintien et l'amélioration continue d'un dispositif anticorruption au sein de l'organisation. Il vise à aider les organisations à prévenir, détecter et répondre aux actes de corruption, tout en leur permettant de se conformer aux législations anticorruption en vigueur. Les organisations qui souhaitent attester formellement de la solidité et de la crédibilité de leur dispositif ont par ailleurs la possibilité d'obtenir la certification contre cette norme auprès d'un organisme certificateur accrédité et indépendant.

Remarque

Il convient de souligner que la liste des systèmes de management présentés ne prétend pas à l'exhaustivité.

© Editions ENI - All rights reserved

5. Structure de haut niveau des normes ISO

La structure de haut niveau, désignée en anglais par l'expression *High Level Structure* et communément abrégée en HLS, est un cadre architectural commun imposé par l'Organisation internationale de normalisation à l'ensemble de ses normes de systèmes de management.

La structure de haut niveau poursuit plusieurs objectifs :

– assurer une cohérence entre les normes de management ;
– simplifier l'intégration de plusieurs systèmes au sein d'une même organisation ;
– réduire les redondances documentaires ;
– harmoniser les concepts et définitions clés.

Dans son essence, la structure de haut niveau impose à toutes les normes ISO de systèmes de management une architecture identique, articulée autour de dix chapitres fondamentaux dont l'ordre, l'intitulé et le contenu de base sont strictement identiques d'une norme à l'autre. Ces dix chapitres se présentent comme suit.

– Chapitre 1 : Domaine d'application

  Ce premier chapitre définit l'objet de la norme, son périmètre d'application et les types d'organisations auxquelles elle est destinée. Il précise également les résultats attendus du système de management concerné et fixe les limites dans lesquelles les exigences de la norme s'appliquent.

– Chapitre 2 : Références normatives

  Ce chapitre recense les documents de référence indispensables à l'application de la norme, c'est-à-dire les autres normes ou textes normatifs dont le contenu est incorporé, en tout ou partie, dans les exigences de la norme considérée. Pour certaines normes de systèmes de management, ce chapitre est souvent déclaré sans objet, en l'absence de références normatives externes obligatoires.