E 26v19

Continuité d'activité

Objectif du module : Préparation à la mise en œuvre, la certification, le maintien et l'amélioration de votre système de management de la continuité d'activité (ISO 22301) pour pouvoir :

- assurer la protection de l'entreprise contre des crises majeures
- réduire la vraisemblance d'apparition d'évènements perturbateurs
- augmenter la confiance dans la résilience de l'entreprise

1 Continuité d'activité

1.1 Historique

Toute décision comporte un risque. Peter Barge

Le mot risque pourrait venir du mot latin resecum « ce qui coupe, écueil » d'où l'origine maritime « rocher escarpé » ou pourrait découler de l'italien ancien risicare, qui signifie "oser."

Les opportunités et les menaces sont les deux côtés de la même pièce appelée risque. Quand l'issue est favorable on parle d'opportunité, quand l'issue est défavorable on parle de menace.

Il y a environ 5200 ans dans la région de l'Euphrate, un groupe appelé Asipu était consultant en analyse du risque pour la prise de décisions risquées ou incertaines.

En Mésopotamie, il y a environ 3900 ans l'assurance a débuté comme l'une des plus anciennes stratégies de gestion du risque. La prime de risque pour les pertes de navires et de cargaison dans les contrats de base était formalisée dans le code d'Hamurabi.

Il a y plus de 2400 ans Périclès parle comment prendre des risques et les évaluer avant de réaliser une action. Son compatriote Socrate définit eikos (possible, probable) comme « vraisemblance à la vérité ».

Blaise Pascal et Pierre de Fermat ont jeté les bases de la théorie de la probabilité dans les années 1650 ce qui a ouvert la porte à l'évaluation quantitative du risque.

Pierre Simon de Laplace a développé en 1792 une analyse du risque avec ses calculs de la probabilité de décès avec et sans vaccination antivariolique.

La gestion du risque est relativement récente. Par exemple, l'accord de Bâle II sur les exigences de gestion du risque dans le secteur bancaire date de 2004. Quelques normes prescriptives (non certifiables) sur le risque sont apparues au début du XXI siècle.

Une difficulté dans la gestion du risque provient du fait que l'événement concerné (le dommage) se situe dans le futur. Il faut imaginer un événement qui n'aura peut-être jamais lieu.

Le risque zéro n'existe pas

La crise financière mondiale de 2008 a remis en question la contribution de la gestion du risque. Certains ont dit que les méthodes de gestion du risque n'ont pas réussi à éviter cette crise. Mais l'analyse révèle que cet échec est surtout dû :

- au manque d'une analyse équilibrée des bénéfices élevés et les risques encourus
- au mauvais jugement de l'improbabilité de certains événements (niveau du risque mal quantifié) basé sur des modèles financiers imprudents
- à la faible surveillance des paramètres clés
- à la compréhension divergente des différents acteurs sur le goût du risque et l'attitude face au risque
- à l'effondrement des marchés monétaires de gros non anticipé par les modèles de crédit utilisés par certaines banques

La gestion du risque a été considérée dans le passé par certains responsables comme quelque chose de superflu. Ces personnes pensaient que l'objectif principal était d'éviter le risque. Depuis beaucoup ont compris que le risque est inévitable et intrinsèque à toute activité mais doit être réduit à un niveau acceptable.

Le risque ne peut être éliminé

La gestion du risque est devenue une nécessité incontournable, même la norme ISO 9001 (systèmes de management de la qualité – exigences) depuis la version 2015 a inclus l'approche par les risques.

Le risque qui résulte de l'incertitude peut être géré. La capacité à identifier le risque, à l'analyser, à l'évaluer, puis à agir en conséquence est à la base de la gestion du risque.

Le management de la continuité d'activité est aussi relativement récent. Une des premières normes concernant le système de management de la continuité d'activité (SMCA) date de 2003 : BSI PAS 56, *Guide to Business Continuity Management* (Guide du management de la continuité d'activité), (cf. paragraphe 2.2).

La première édition de la norme ISO 22301 (« Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences ») date de 2012.

Depuis quelques décennies la majorité des entreprises a pris conscience que les coûts de la mise en place de la gestion de la continuité d'activité sont dérisoires comparés aux conséquences défavorables ou même aux assurances à contracter.

Quelques différences entre la gestion du risque et la gestion de la continuité d'activité sont montrées dans le tableau 1-1 :

Tableau 1-1. Différences

	Gestion du risque	**Gestion de la continuité d'activité**
Finalité	Réduction du risque	Survie (résilience) de l'entreprise
Activité	Incident du quotidien	Perturbation majeure
Domaine d'application	Un département	L'entreprise
Méthode	Analyse du risque	Analyse d'impact
Sujets concernés	La vraisemblance et impact	L'impact direct et dans le temps

Histoire vraie

Un incendie se déclenche dans un centre informatique. Les dommages sont énormes car le rétablissement de la situation sera réalisé après plus d'un mois.

Le centre avait signé un contrat de sauvegarde avec un prestataire externe.

Mais le contrat n'incluait pas de garantie contre un incendie et n'avait pas été testé correctement.

D'après une enquête d'Eagle Rock Alliance, 40 % des entreprises sondées estiment que 72 heures d'interruption de leur système informatique est un délai critique avant le risque de faillite.

L'objectif principal de la gestion de la continuité d'activité est d'assurer la survie de l'entreprise en toutes circonstances.

1.2 Mise en place

Se préparer au pire est une vision réaliste et pragmatique du monde

L'établissement et la mise en place du système de management de la continuité d'activité ISO 22301 sont montrés dans la figure 1-1.

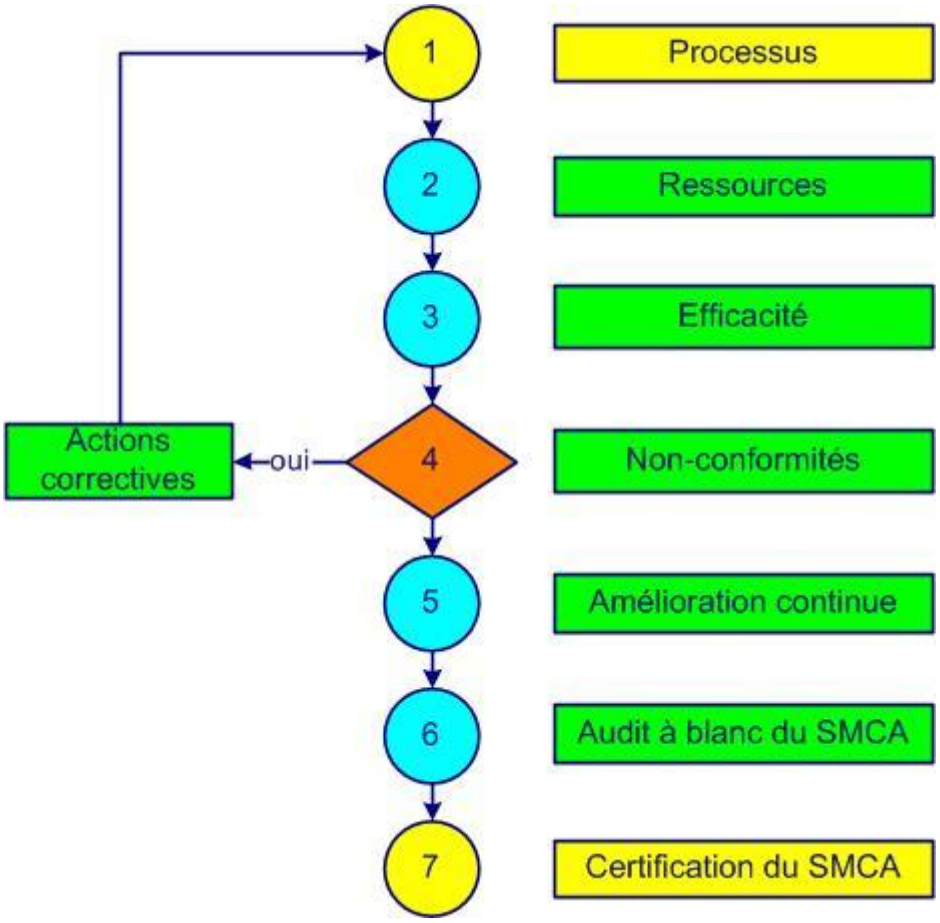


Figure 1-1. Mise en place d'un SMCA

L'**étape 1** consiste à expliquer l'importance d'avoir un SMCA, à identifier et définir les **processus**, les interactions, les pilotes, les responsabilités et les brouillons de certains documents. Avec la participation du maximum de personnes disponibles sont rédigés les premières versions des plans de continuité d'activité.

Dans l'**étape 2** sont fixées les **ressources** nécessaires pour atteindre la politique et les objectifs de continuité d'activité. Une planification des tâches, responsabilités et délais est établie. Une formation des auditeurs internes est prise en compte.

L'**étape 3** permet de définir et mettre en œuvre les méthodes permettant de mesurer l'**efficacité** et l'efficience de chaque processus et des plans de continuité d'activité. Des audits internes permettent d'évaluer le degré de la mise en place du SMCA.

Les **non-conformités** en tout genre sont répertoriées à l'**étape 4**. Une esquisse des différents écarts est établie. Des actions correctives sont mises en place et documentées.

Une première appréciation des outils et du domaine d'application du processus d'**amélioration continue** est faite à l'**étape 5**. Des risques sont déterminés, des actions sont planifiées et des opportunités d'amélioration sont trouvées. La communication en interne et en externe est établie et formalisée.

Pour effectuer l'**audit à blanc du SMCA** (**étape 6**) la documentation du SMCA est vérifiée et approuvée par les personnes appropriées. Une revue de direction permet d'évaluer le respect des exigences applicables. La politique et les objectifs de continuité d'activité sont finalisés. Un responsable du PCA d'une autre entreprise ou un consultant pourra fournir de précieuses remarques, suggestions et recommandations.

Quand le système est correctement mis en place et respecté, la **certification du SMCA** par un organisme externe devient une formalité (**étape 7**).

Un exemple de plan de projet de certification ISO 22301 comportant 26 étapes est présenté dans l'annexe 01.

Une méthode pertinente pour évaluer le niveau de performance de votre système de management de la continuité d'activité est la logique RADAR du modèle d'excellence de l'EFQM (European Foundation for Quality Management) avec ses 9 critères et sa note globale sur 1000 points.

Le cycle PDCA, ou cycle de Deming (figure 1-2) s'applique à la maîtrise de tout processus. Les cycles PDCA (de l'anglais Plan, Do, Check, Act ou Planifier, Dérouler, Comparer, Agir) sont une base universelle de l'amélioration continue.

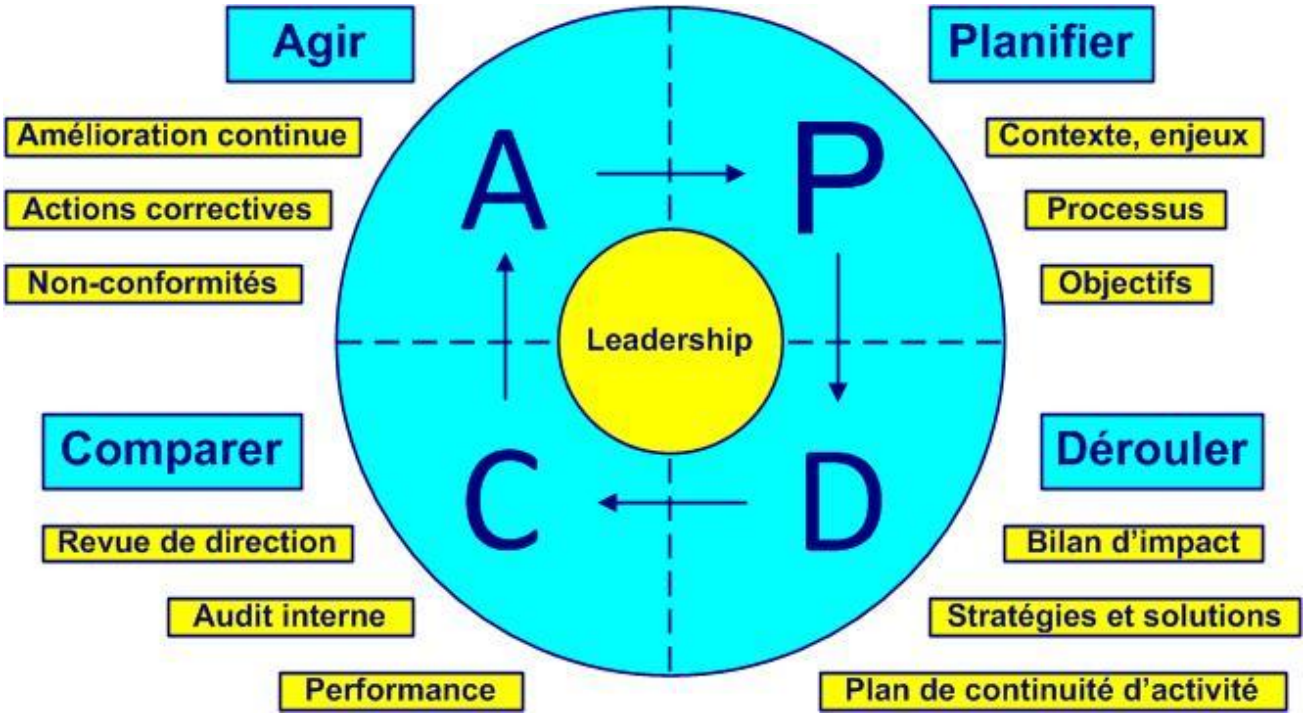


Figure 1-2. Le cycle de Deming

- Planifier, définir le contexte, les enjeux et les processus, faire preuve de leadership, établir la politique et les objectifs de continuité d'activité, traiter les risques (articles 4, 5, 6 et 7)

- Dérouler, faire preuve de leadership, analyser le bilan d'impact sur l'activité, apporter le support, établir les stratégies et les solutions, réaliser les plans de continuité d'activité et les tester (articles 5, 7 et 8)
- Comparer, faire preuve de leadership, évaluer, inspecter, conduire les audits et les revues de direction (articles 5 et 9)
- Agir, adapter, faire preuve de leadership, traiter les non-conformités, réagir avec des actions correctives et trouver de nouvelles améliorations (nouveau PDCA), (articles 5 et 10)

Pour approfondir ses connaissances sur le cycle de Deming et ses 14 points de la théorie du management vous pouvez consulter le livre « Hors de la crise » W. Edwards Deming, Economica, 2002 paru pour la première fois en 1982, cf. paragraphe 2.3.

1.3 Bénéfices

Préparer la guerre en temps de paix

Souvent la décision de mettre en place un SMCA et des PCA est prise après avoir subi une crise ou une situation très proche d'une catastrophe financière.

Des incidents, des accidents, des crises, des sinistres et des catastrophes n'arrivent pas qu'aux autres !

Chaque perturbation est spécifique et cause des dommages souvent inattendus et différents. Une préparation à ces événements d'origine naturelle (séisme, inondation, incendie) ou d'origine humaine (terrorisme, cyber attaque, perte de personnel qualifié) ne peut que nous être bénéfique.

Une réponse à une perturbation partielle ou totale, potentielle ou réelle, consiste à avoir un plan de continuité d'activité et une équipe de crise désignée. Alors vous pourrez diminuer certains risques, atténuer les impacts et reprendre les activités prioritaires pendant et après une perturbation.

Bénéfices attendus de la gestion de la continuité d'activité :

- prévenir les situations de crise
- renforcer sa résilience en évaluant et réduisant les conséquences d'une crise
- maintenir les activités vitales de l'entreprise pendant une perturbation
- mettre en place les outils et équipements de protection civile
- sensibiliser et former le personnel sur le comportement à adopter en cas de crise
- protéger le patrimoine de l'entreprise
- réduire les coûts d'assurance (renégociation du contrat)
- protéger et améliorer la réputation de l'entreprise
- renforcer la confiance des parties prenantes
- consolider l'avantage concurrentiel
- répondre aux exigences légales et réglementaires
- anticiper les incidents perturbateurs et réduire le risque de sinistre
- disposer de processus efficaces pour garantir la continuité d'activité
- établir une base fiable pour la prise de décisions en temps de crise
- analyser et comprendre les principales menaces et domaines de vulnérabilité
- augmenter la vraisemblance d'atteindre les objectifs
- accroître les opportunités à saisir
- diminuer les pertes

Histoire vraie

Amazon, l'un des leaders mondiaux du commerce électronique, a mis en place l'ISO 22301 pour améliorer la confiance des clients dans la capacité de l'entreprise à maintenir ses services en cas d'incident majeur.

La certification ISO 22301 a permis à Amazon de démontrer son engagement envers la continuité de ses services et de rassurer ses clients.

Amazon a enregistré une augmentation de la confiance des clients, démontrant l'importance de la continuité d'activité pour les clients du e-commerce.

Qui s'excuse s'accuse

Excuses courantes pour expliquer un échec :

- c'était de la responsabilité de la direction
- ce n'était pas une exigence explicite dans le contrat
- comment avoir un plan efficace face à tellement de problèmes potentiels
- donnez-moi assez de temps et tout sera réglé
- en cas de situation d'urgence grave, l'implication sera tout autre
- il n'y avait pas assez de temps
- il n'y avait pas de personnel disponible
- il y a des choses plus importantes à faire
- j'étais sûr que nous pourrions faire face
- je ne me suis pas rendu compte que c'était si grave
- je ne pensais pas que c'est un processus clé
- je ne pensais pas que cela arriverait
- l'assurance devait prendre cette situation en charge
- le contrat était déjà signé
- vous ne pouvez pas planifier l'imprévu

Une liste de succès et d'échecs de la continuité d'activité se trouve dans l'annexe 02.

2 Définitions, normes et livres

2.1 Définitions

Le début de la sagesse est la définition des termes. Socrate

Un risque peut avoir des impacts négatifs (on parle de menaces) ou bien des impacts positifs (on parle d'opportunités).

Saisir une opportunité c'est prendre des risques, mais ne pas saisir une opportunité peut nous exposer à des risques.

Les définitions du mot **risque** sont multiples. Quelques exemples :

- combinaison de la probabilité d'occurrence d'un dommage et de sa gravité. ISO 51 (1999)
- combinaison de la probabilité d'un évènement et de ses conséquences. ISO Guide 73 (2002)
- combinaison de la probabilité de la manifestation d'un événement dangereux et de la gravité de la lésion ou de l'atteinte à la santé causée à des personnes par cet événement. ILO-OSH (2001)
- danger éventuel plus ou moins prévisible. Le Petit Robert
- description d'un événement spécifique qui peut se produire ou non, ainsi que ses causes et ses conséquences. IRM (2013)
- effet de l'incertitude sur l'atteinte des objectifs. ISO Guide 73 (2009)
- effet de l'incertitude sur les objectifs. ISO 22301 (2019)
- effet de l'incertitude. ISO 45001 (2018)
- effet négatif de l'incertitude. Christopher Paris
- espérance mathématique d'une fonction de probabilité d'événements. Daniel Bernoulli
- événement dont l'arrivé aléatoire, est susceptible de causer un dommage aux personnes ou aux biens ou aux deux à la fois. Serge Braudo
- événement éventuel incertain dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer un dommage. Larousse
- incertitude des résultats, qu'il s'agisse d'une opportunité positive ou d'une menace négative. OGC - UK (2005)
- l'impact futur d'un danger non maîtrisé. Sean Chamberlin
- la mesure du danger. Georges-Yves Kervern
- la possibilité que quelque chose se passe qui aura un impact sur les objectifs. AS 4360 (2004)
- la vraisemblance que quelque chose se passe. IFRIMA (1994)
- l'ampleur de la perte potentielle. Evan Picoult
- le risque devrait être proportionnel à la probabilité d'occurrence ainsi qu'à l'étendue de dommage. Blaise Pascal
- probabilité et ampleur d'une perte, d'un désastre ou d'un autre événement indésirable. Douglas Hubbard

Notre préférence :

Risque : *vraisemblance d'apparition d'une menace ou d'une opportunité*

Identifier le danger c'est se demander qu'est-ce qui pourrait mal se passer

Souvent le risque est assimilé à un danger et utilisé couramment à la place de menace.

L'incertitude et la probabilité sont des notions subjectives avec des quantités fictives.

La probabilité peut être considérée comme mesure de l'incertitude. Si la probabilité peut être mesurée elle est donc reliée à quelque chose qui s'est passé. La vraisemblance est plus générale comme notion car elle peut inclure un effet qui ne s'est jamais passé.

Quelques définitions et abréviations :

Activité : *ensemble de tâches pour obtenir un livrable*
AMDEC : *Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité. En anglais FMEA ou FMECA. Démarche de prévention des risques techniques*
Analyse du risque : *activité de l'appréciation du risque pour comprendre la nature d'un risque et déterminer son impact*
Appréciation du risque : *processus d'identification, d'analyse et d'évaluation du risque*
Benchmarking : *technique d'analyse comparative par rapport à un ou plusieurs concurrents*
Bilan d'impact sur l'activité (BIA) : *analyse de l'impact d'une perturbation sur l'entreprise*
Brainstorming : *voir remue-méninges*
Continuité d'activité : *capacité d'une entreprise à poursuivre la livraison de produits et la fourniture de services durant et après une perturbation*
Contrôle : *voir inspection*
Critères du risque : *indices pour évaluer l'importance du risque*
Danger : *situation pouvant conduire à un incident*
Détrompeur : *simple équipement pour éviter les erreurs et ne pas permettre de produire des non-conformités, appelé aussi Poka-yoké ou dispositif anti-erreurs*
DMTP : *durée maximale tolérable de perturbation*
Estimation du risque : *activités pour affecter des valeurs à la vraisemblance et à l'impact du risque*
Évaluation du risque : *activités de l'appréciation du risque pour déterminer si le risque est acceptable*
Exigence : *besoin ou attente implicite ou explicite*
Facteur du risque (péril, danger) : *élément susceptible de causer un risque*
FMEA : *Failure Mode and Effects Analysis. Voir AMDEC*
Gaspillage : *tout ce qui ajoute des coûts mais pas de valeur*
Gestion de la continuité d'activité : *méthode visant à assurer qu'en cas de crise les fonctions critiques restent opérationnelles ou le redeviennent le plus vite possible (voir aussi résilience)*
Gestion du risque : *activités pour restreindre la possibilité que quelque chose se passe mal*
Gravité du risque : *mesure de l'impact du risque*
Identification du risque : *activité de l'appréciation du risque pour trouver et décrire les risques*
Impact : *conséquence d'un événement affectant les objectifs*
Incertitude : *existence de plus d'une possibilité*
Inspection *: actions de mesures, d'essais et d'examens d'un produit, service, processus ou matériel pour déterminer le respect des exigences*

Kaizen : *du japonais kai - changement, zen - mieux. Amélioration continue pas à pas pour créer plus de valeur et moins de gaspillages. Démarche fondée sur le bon sens et sur la motivation du personnel*

Menace : *événement incertain pouvant avoir un impact négatif sur les objectifs*

Mesure du risque : *ensemble de possibilités avec des probabilités et des pertes quantifiées*

Niveau du risque : *criticité du risque en fonction de l'impact et de la vraisemblance*

Non-qualité : *écart entre la qualité attendue et la qualité perçue*

Opportunité *: événement incertain pouvant avoir un impact favorable*

PCA *: plan de continuité d'activité*

Perturbation : *incident qui entraîne un dérèglement de la livraison de produits et la fourniture de services*

Pilote du risque : *personne ayant la responsabilité et l'autorité de gérer le risque*

Plan de gestion du risque : *mesures planifiées afin de traiter le risque*

Poka-yoké : *du japonais Poka - erreur involontaire, Yoké - éviter. Voir Détrompeur*

Prévention du risque : *activités de réduction de la vraisemblance d'apparition du risque*

Protection du risque : *activités de réduction des impacts du risque*

Registre des risques : *dossier contenant les informations relatives aux risques identifiés*

Remue-méninges : *approche d'équipe pour développer des idées et trouver des solutions. En anglais "Brainstorming"*

Résilience : *capacité à résoudre une crise et à continuer de fonctionner comme avant*

Responsabilité : *capacité à prendre une décision tout seul*

Responsable du PCA : *leader du voyage vers la résilience*

Sécurité : *absence de risque inacceptable*

Seuil du risque : *limite d'acceptation (au-dessous) ou de non tolérance (au-dessus)*

Stratégie : *démarche globale pour atteindre des objectifs*

Surveillance : *ensemble d'actions planifiées pour garantir l'efficacité des mesures de maîtrise*

SWOT : *de l'anglais Strengths, Weaknesses, Opportunities, Threats ou forces, faiblesses, opportunités, menaces. Outil pour structurer une analyse des risques*

Système de gestion du risque (SGR) : *ensemble de processus permettant d'atteindre les objectifs risque*

Système de management (SM) : *ensemble de processus permettant d'atteindre les objectifs*

Système de management de la continuité d'activité (SMCA) : *ensemble de processus permettant d'atteindre les objectifs de continuité d'activité*

Système : *ensemble de processus interactifs*

Traitement du risque : *activités de modification du risque*

Vraisemblance : *possibilité que quelque chose arrive*

Dans la terminologie des systèmes de management ne pas confondre :

- accident et incident
  - l'accident est un événement imprévu grave
  - l'incident est un événement qui peut entraîner un accident
- anomalie, défaillance, défaut, dysfonctionnement, non-conformité et rebut
  - l'anomalie est une déviation par rapport à ce qui est attendu
  - la défaillance est la non satisfaction d'une fonction

    - le défaut est la non satisfaction d'une exigence liée à une utilisation (prévue)
    - le dysfonctionnement est un fonctionnement dégradé qui peut entraîner une défaillance
    - la non-conformité est la non satisfaction d'une exigence spécifiée (en production)
    - le rebut est un produit non conforme qui sera détruit
- audit, inspection, audité et auditeur
    - l'audit est le processus d'obtention des preuves d'audit
    - l'inspection est la vérification de conformité d'un processus ou d'un produit
    - l'audité est celui qui est audité
    - l'auditeur est celui qui réalise l'audit
- cause et symptôme
    - la cause est la circonstance entraînant une défaillance
    - le symptôme est le caractère lié à un état
- cartographie et organigramme
    - la cartographie est la présentation graphique des processus et leurs interactions dans une entreprise
    - l'organigramme est la présentation graphique des départements et leurs liens dans une entreprise
- client, prestataire externe et sous-traitant
    - le client reçoit un produit
    - le prestataire externe procure un produit
    - le sous-traitant procure un service ou un produit sur lequel est réalisé un travail spécifique
- danger, problème et risque
    - le danger c'est l'état, la situation, la source qui peut aboutir à un accident
    - le problème c'est l'écart entre la situation réelle et la situation souhaitée
    - le risque est la mesure, la conséquence d'un danger et c'est toujours un problème potentiel
- efficacité et efficience
    - l'efficacité est le niveau d'obtention des résultats escomptés
    - l'efficience est le rapport entre les résultats obtenus et les ressources utilisées
- exactitude et précision
    - l'exactitude est une mesure avec une faible erreur systématique
    - la précision est une mesure avec une faible erreur aléatoire
- informer et communiquer
    - informer c'est porter une information à la connaissance de quelqu'un
    - communiquer c'est transmettre un message, écouter la réaction et dialoguer
- gestion du risque et de crise
    - la gestion du risque c'est comme faire de la prévention des incendies
    - la gestion de crise c'est comme éteindre le feu
- maîtriser et optimiser
    - la maîtrise est le respect des objectifs
    - l'optimisation est la recherche des meilleurs résultats possibles
- objectif et indicateur
    - l'objectif est un engagement recherché
    - l'indicateur est l'information de la différence entre le résultat obtenu et l'objectif fixé
- processus, procédure, produit, procédé, activité et tâche
    - le processus est la façon de satisfaire le client en utilisant le personnel pour atteindre les objectifs
    - la procédure est la description de la façon dont on devrait se conformer aux règles

    - le produit est le résultat d'un processus
    - le procédé est la façon d'exécuter une activité
    - l'activité est un ensemble de tâches
    - la tâche est une suite de simples opérations
- prévention et protection, cf. figure 2-1
    - la prévention ce sont les moyens permettant de diminuer la vraisemblance et la fréquence d'apparition d'un risque (vérifier la pression des pneus)
    - la protection ce sont les moyens permettant de limiter l'impact d'un risque (attacher sa ceinture de sécurité)
- probabilité, incertitude et vraisemblance
    - la probabilité exprime l'analyse quantitative de l'incertitude
    - l'incertitude c'est l'imprécision de prévoir
    - la vraisemblance exprime l'analyse qualitative de l'incertitude
- suivi et revue
    - le suivi est la vérification d'atteinte de résultats d'une action
    - la revue est l'analyse de l'efficacité à atteindre des objectifs

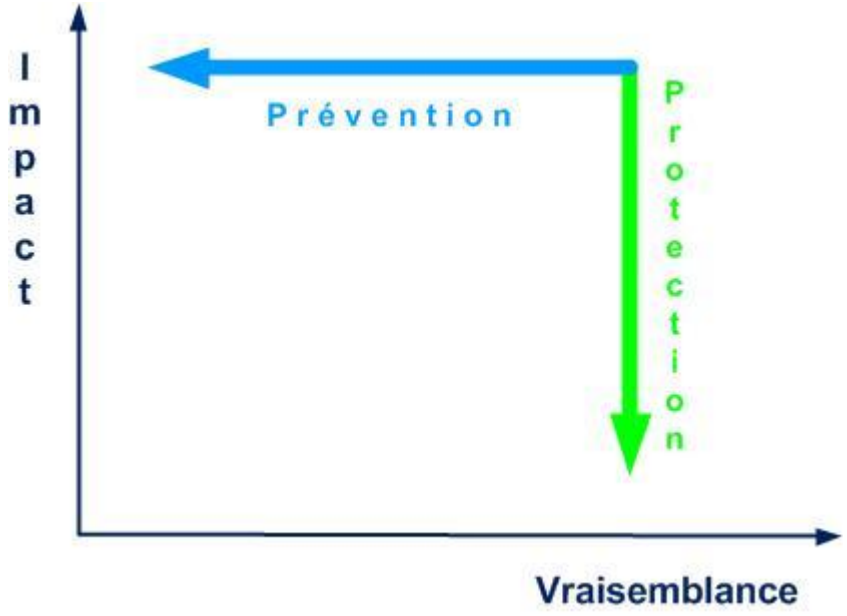


Figure 2-1. La prévention et la protection

Remarque 1 : entre gestion du risque et management du risque notre préférence est pour gestion du risque

Remarque 2 : entre apparition et occurrence notre préférence est pour apparition

Remarque 3 : entre pilote du risque et propriétaire du risque notre préférence est pour pilote du risque

Remarque 4 : entre vraisemblance (likelihood) et probabilité (probability) notre préférence est pour vraisemblance (d'apparition)

Remarque 5 : entre domaine d'application et périmètre d'application (en anglais scope) notre préférence est pour domaine d'application

Remarque 6 : entre surveillance (en anglais monitoring) et suivi notre préférence est pour surveillance

Remarque 7 : entre processus et procédé notre préférence est pour processus (en anglais « process »).

Remarque 8 : le mot anglais « organization » est traduit par organisme dans certaines normes (ISO 9001, ISO 22301) et par organisation dans d'autres normes (ISO 2600, EFQM) et institutions (ISO, ONU, OTAN). Pour éviter la confusion avec organisme de certification et organisation notre préférence est pour le terme entreprise

Remarque 9 : le mot anglais « control » a plusieurs sens. Il peut être traduit par maîtrise, autorité, commande, gestion, contrôle, surveillance, inspection. Pour éviter des malentendus notre préférence est pour maîtrise et inspection au détriment de contrôle.

Remarque 10 : chaque fois que vous utiliserez l'expression « opportunité d'amélioration » à la place de non-conformité, dysfonctionnement ou défaillance vous gagnerez un peu plus la confiance de votre interlocuteur (client externe ou interne).

Remarque 11 : l'important est de définir et d'utiliser un langage commun et sans équivoque.

Pour d'autres définitions, commentaires, explications et interprétations que vous ne trouvez pas dans ce module et l'annexe 06 vous pouvez consulter : 

- Electropedia de l'IEC
- Plateforme de consultation en ligne (OBP) de l'ISO

Les icônes utilisées dans ce module :

-  explication, exemple, détail, règle
-  processus
-  procédure (documentée)
-  enregistrement
-  blague
-  jeu
-  écart à éviter

2.2 Normes

Il ne peut y avoir d'améliorations là où il n'existe pas de normes. Masaaki Imai

Normes et référentiels liés aux risques et la continuité d'activité (par ordre chronologique) :

- AS 4360 (1995), *Risk management* (Gestion du risque)
- ANAO Better Practice Guide (2000), *Business Continuity Management—Keeping the wheels in motion* (Guide de meilleures pratiques, Gestion de la continuité d'activité : garder les roues en mouvement)
- BSI PAS 56 (2003), *Guide to Business Continuity Management* (Guide du management de la continuité d'activité)
- HB 221 (2004), *Business Continuity Management* (Gestion de la continuité d'activité)

- NFPA 1600 (2004), *Standard on Disaster/Emergency Management and Business Continuity Programs* (Norme sur les programmes de gestion des catastrophes/urgences et de continuité des activités)
- BS 25999-1 (2006), *Business Continuity Management – Part 1: Code of Practice* (Gestion de la continuité d'activité, Partie 1, code de pratique)
- FD X50-252 (2006), Management du risque - Lignes directrices pour l'estimation des risques
- BS 25999 – 2 (2007), *Business continuity management – Specification* (Gestion de la continuité d'activité, Partie 2, Spécification)
- ISO/PAS 22399 (2007), Sécurité Sociétale – Lignes directrices pour être préparé à un incident et gestion de continuité opérationnelle
- SI 24001 (2007) *Organizational resilience management system (ORMS) – Requirements and guidance for use* (Système de gestion de la résilience organisationnelle (SGRO) – Exigences et conseils d'utilisation)
- ISO Guide 73 (2009), Management du risque - Vocabulaire
- ANSI/ASIS SPC1 (2009), *Organisational Resilience : Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use* (Résilience organisationnelle : systèmes de gestion de la sécurité, de la préparation et de la continuité – Exigences avec conseils d'utilisation)
- SS 540 (2008), Singapore Standard for Business Continuity Management (BCM) (Norme de Singapour pour la gestion de la continuité d'activité)
- ANSI/ASIS/BSI BCM.01 (2010), *Business Continuity Management Systems : Requirements with Guidance for Use* (Systèmes de gestion de la continuité d'activité : exigences et conseils d'utilisation)
- BP Z74-700 (2011), Référentiel de bonnes pratiques, Plan de Continuité d'Activité (PCA)
- ISO/IEC 27031 (2011), Technologies de l'information - Techniques de sécurité - Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité
- ISO 22398 (2013), *Societal security, Guidelines for exercises* (Sécurité sociétale, Lignes directrices pour exercice)
- FD X50-259 (2014), Management du risque - Plan de continuité d'activité (PCA) - Démarche de mise en place et de maintien
- BS 11200 (2014), *Crisis management - Guidance and good practice* (Gestion des crises - Guide et bonnes pratiques)
- FD X50-259 (2014), Fascicule de documentation - Management du risque - Plan de continuité d'activité (PCA) - Démarche de mise en place et de maintien
- BS 65000 (2014), *Guidance on organizational resilience* (Guide sur la résilience organisationnelle)
- ISO 22316 (2017), *Security and resilience - Organizational resilience - Principles and attributes* (Sécurité et résilience - Résilience organisationnelle - Principes et attributs)
- ISO 31000 (2018), Management du risque – Lignes directrices
- ISO 19011 (2018), Lignes directrices pour l'audit des systèmes de management
- ISO/TS 22330 (2018), Sécurité et résilience - Systèmes de gestion de la poursuite des activités - Lignes directrices concernant les aspects humains de la poursuite des activités
- ISO/TS 22331 (2018), Sécurité et résilience - Systèmes de management de la continuité des activités - Lignes directrices relatives à la stratégie de continuité d'activité

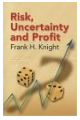
- ISO 22320 (2018), *Security and resilience, Emergency management, Guidelines for incident management* (Sécurité et résilience, Gestion des urgences, Lignes directrices pour la gestion des incidents)
- ISO 22301 (2019), Sécurité et résilience - Systèmes de management de la continuité d'activité - Exigences
- IEC 31010 (2019), Management du risque - Techniques d'appréciation du risque
- ISO 22313 (2020), Sécurité et résilience - Systèmes de management de la continuité d'activité - Lignes directrices sur l'utilisation de l'ISO 22301
- AS/NZS 5050(Int) (2020), *Managing disruption-related risk* (Gérer les risques liés aux perturbations)
- BS 31100 (2021), *Risk management. Code of practice* (Gestion du risque. Code de pratique)
- ISO 22300 (2021), Sécurité et résilience, Vocabulaire
- ISO/TS 22317 (2021), Sécurité et résilience - Systèmes de management de la continuité d'activité - Lignes directrices pour le bilan d'impact sur l'activité
- ISO/TS 22318 (2021), Sécurité et résilience - Systèmes de management de la continuité d'activité - Lignes directrices pour le management de la continuité de la chaîne d'approvisionnement
- CSA Z1600:F17 (2022), Programme de gestion des urgences et de la continuité
- ISO 22322 (2022) *Security and resilience, Emergency management, Guidelines for public warning* (Sécurité et résilience, Gestion des situations d'urgence, Lignes directrices relatives aux mises en garde de la population)
- 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

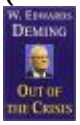
Aucune de ces normes n'est obligatoire mais comme disait Deming :

Il n'est pas nécessaire de changer. La survie n'est pas obligatoire

2.3 Livres

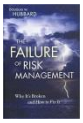
Pour aller plus loin quelques livres, classés par ordre chronologique :

- 

Frank Knight, *Risk, Uncertainty And Profit*, University of Chicago Press, 1921 (Le risque, incertitude et profit)
- 

Edwards Deming, *Out of the crisis*, MIT Press, 1982 (

Hors de la crise, Economica, 1991)
- 
Clusif, Comment gérer les risques dans l'entreprise, Dunod, 1993
- 
Daniel Guinier, Catastrophe et management, plans d'urgence et continuité des systèmes d'information, 1995

-  Peter Bernstein, *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons, New York, 1998 (Contre les Dieux : L'histoire remarquable du risque)
-  Michael Gallagher, *Business Continuity Management - How to Protect Your Company from Danger*, Prentice Hall, 2002 (Gestion de la continuité d'activité – Comment protéger votre entreprise des dangers)
-  Nancy Tague, *The Quality Toolbox*, ASQC Quality Press, 2005 (La boîte à outils qualité)
-  Emmanuel Besluau, Management de la continuité d'activité, Eyroles, 2008
-  Douglas Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*, Wiley, 2009 (L'échec de la gestion du risque: pourquoi c'est cassé et comment le réparer)
-  Jean-Claude Serre, Managers, osez le management par les risques: Pour réussir en période de crise !, AFNOR, 2009
-  Pascal Kerebel, Management des risques, Eyrolles, 2009
-  Matthieu Bennasar, Plan de continuité d'activité et système d'information - Vers l'entreprise résiliente, DUNOD, 2010
-  Jean-Luc Wybo, Maîtrise des risques et prévention des crises : anticipation, construction de sens, vigilance, gestion des urgences et apprentissage, Lavoisier, 2012
-  Bernard Carrez, Antonio Pessoa, Alexandre Planche, Plan de Continuité d'Activité - Concepts et démarche pour passer du besoin à la mise en œuvre du PCA, ENI, 2013
-  Jean-Paul Louisot, Risk Management et stratégie selon la norme ISO 31000 - Les bénéfices de l'intégration de l'ERM dans les processus stratégiques, AFNOR, 2016

-  Jean-David Darsa, La gestion des risques en entreprise: Identifier, comprendre, maîtriser, Gereso, 2016
-  Laurent Combalbert, Le management des situations de crise : anticiper les risques et gérer les crises, ESF, 2018
-  Cécile Weber, Plan de continuité des activités et gestion de crise, AFNOR, 2020
-  FAP, PCA par ci, PCA pas là ! - Regards croisés sur le plan de continuité d'activité, Les Éditions du NET, 2020
-  collectif, *ISO 22301 A Complete Guide - 2021 Edition*, The Art of Service, 2020 (ISO 22301 – Un guide complet, edition 2021)
-  James Crask, *Business Continuity Management: A Practical Guide to Organizational Resilience and ISO 22301*, Kogan Page, 2021 (Gestion de la continuité d'activité: Un guide pratique de résilience d'entreprise et ISO 22301)
-  Jean-Pierre Galland, La gestion des risques - Origines, succès et limites du risk management, L'Harmattan, 2022
-  Stéphane Hesschentier, Systèmes de Management de la Continuité d'Activité - Meilleures pratiques et mise en œuvre de la norme ISO 22301, ENI, 2023

Quand je pense à tous les livres qu'il me reste encore à lire, j'ai la certitude d'être encore heureux. Jules Renard

3 Approche processus

3.1 Types de processus

Si vous ne pouvez pas décrire ce que vous faites en tant que processus, vous ne savez pas ce que vous faites. Edwards Deming

Le mot processus vient de la racine latine procedere = marche, développement, progrès (Pro = en avant, cedere = aller). Chaque processus transforme les éléments d'entrée en éléments de sortie en créant de la valeur ajoutée et des nuisances potentielles.

Un processus a trois éléments de base : entrées, activités, sorties. 

Un processus peut être très complexe (lancer une fusée) ou relativement simple (auditer un produit).

Un processus est :

- répétable
- prévisible
- mesurable
- définissable
- dépendant de son contexte
- responsable de ses fournisseurs

Un processus est défini, entre autres, par :

- son intitulé et son type
- sa finalité (pourquoi ?)
- son bénéficiaire (pour qui ?)
- son objet et ses activités
- ses déclencheurs
- ses enregistrements
- ses éléments d'entrée
- ses éléments de sortie (intentionnels et non intentionnels)
- ses contraintes
- son personnel
- ses ressources matérielles
- ses objectifs et indicateurs
- son responsable (pilote) et ses acteurs (intervenants)
- ses moyens d'inspection (surveillance, mesure)
- sa cartographie
- son interaction avec les autres processus
- ses risques et écarts potentiels
- ses opportunités d'amélioration continue

Une Revue de processus est faite périodiquement par le pilote du processus (cf. annexe 03). 

Les composantes d'un processus sont montrées dans la figure 3-1 : 

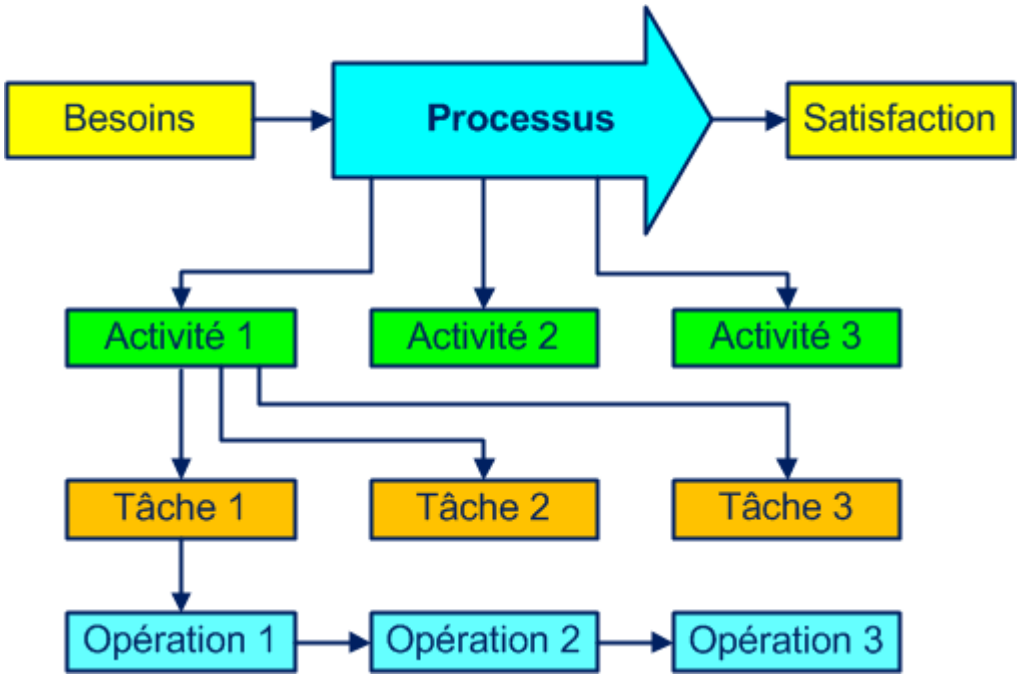


Figure 3-1. Les composantes d'un processus

La figure 3-2 montre un exemple qui aide à répondre aux questions :

- quelles matières, quels documents, quels outils ? (entrées)
- quel intitulé, quelles activités, exigences, contraintes ? (processus)
- quels produits, quels documents ? (sorties)
- comment, quelles inspections ? (méthodes)
- quel est le niveau de la performance ? (indicateurs)
- qui, avec quelles compétences ? (personnel)
- avec quoi, quelles machines, quels équipements ? (ressources matérielles)

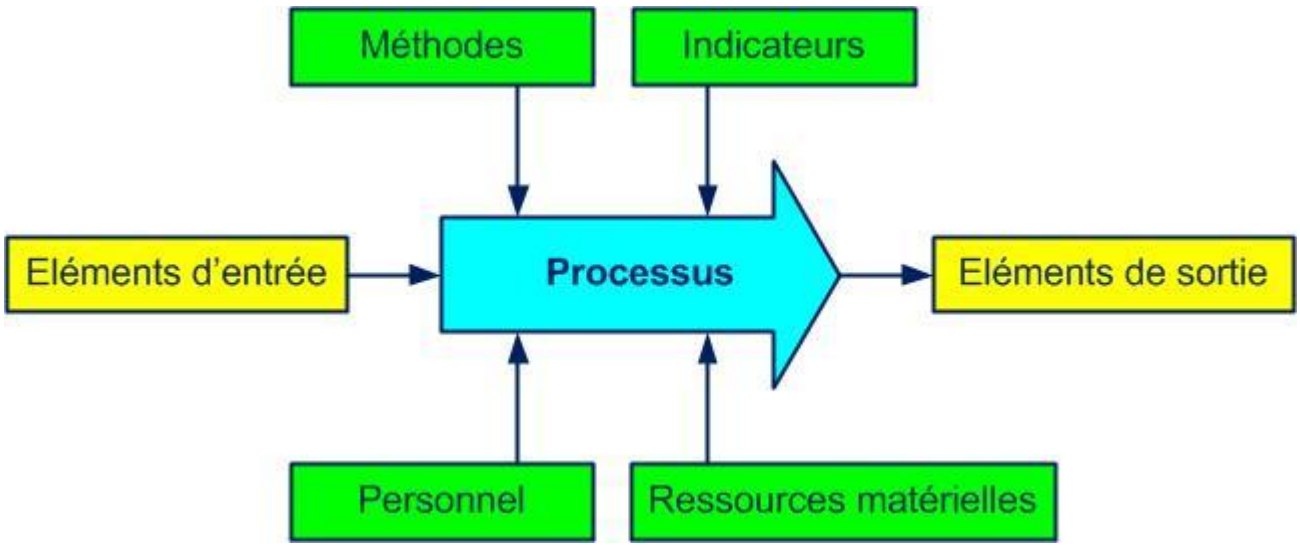


Figure 3-2. Certains éléments d'un processus

Souvent l'élément de sortie d'un processus est l'élément d'entrée du processus suivant.

Vous pouvez trouver quelques dizaines d'exemples de fiches processus dans l'ensemble de documents E 02.

Toute entreprise peut être considérée comme un macro processus, avec sa finalité, ses éléments d'entrée (besoins et attentes clients) et ses éléments de sortie (produits/services pour satisfaire les exigences des clients).

Notre préférence pour identifier un processus est l'utilisation d'un verbe (acheter, produire, vendre) à la place d'un nom (achats, production, vente) pour différencier le processus du département de l'entreprise ou de la procédure et rappeler la finalité du processus.

Les processus sont (comme nous allons voir dans les paragraphes suivants) de type management, réalisation et support. Ne pas attacher trop d'importance au classement des processus (parfois c'est très relatif) mais bien vérifier que toutes les activités de l'entreprise entrent dans un des processus.

3.1.1 Les processus de management

Aussi appelés de direction, de pilotage, de décision, clés, majeurs. Ils participent à l'organisation globale, à l'élaboration de la politique, au déploiement des objectifs et à toutes les vérifications indispensables. Ils sont les fils conducteurs de tous les processus de réalisation et de support.

Les processus suivants peuvent intégrer cette famille (* obligatoire, cf. annexe 04) : 

- élaborer la stratégie
- faire face aux risques
- apprécier les risques * (paragraphe 8.2.3)
- gérer les risques opérationnels
- élaborer des plans d'urgence
- enquêter sur un incident
- satisfaire aux exigences
- définir la politique
- piloter les processus
- améliorer
- auditer en interne * (paragraphe 9.2.2)
- communiquer
- planifier le SM
- acquérir les ressources
- évaluer la performance
- réaliser la revue de direction
- négocier le contrat
- analyser les données

3.1.2 Les processus de réalisation

Les processus de réalisation (opérationnels) sont liés au produit, augmentent la valeur ajoutée et contribuent directement à la satisfaction du client.

Ils sont principalement (* obligatoire) :

- concevoir et développer les nouveaux produits
- acheter les composants
- vendre les produits
- produire les produits

- inspecter la production
- anticiper les situations d'urgence
- maintenir les équipements
- respecter les exigences légales et réglementaires * (paragraphe 4.2.2)
- analyser le bilan d'impact * (paragraphe 8.2.1)
- restaurer les activités * (paragraphe 8.4.5)
- appliquer la traçabilité (identifier et garder l'historique)
- réceptionner, stocker et expédier
- maîtriser les non-conformités (NC)
- réaliser les actions correctives

3.1.3 Les processus de support

Les processus de support (soutien) fournissent les ressources nécessaires au bon fonctionnement de tous les autres processus. Ils ne sont pas liés directement à une contribution de la valeur ajoutée du produit mais sont toujours indispensables.

Les processus support sont souvent :

- gérer la documentation
- fournir l'information
- acquérir et maintenir les infrastructures
- dispenser la formation
- gérer les moyens d'inspection
- tenir la comptabilité
- administrer le personnel

3.2 Cartographie

La cartographie des processus est par excellence un travail pluridisciplinaire. Ce n'est pas une recommandation formelle de la norme ISO 22301 mais la cartographie est toujours bienvenue.

Les 3 types de processus et quelques interactions sont montrés dans la figure 3-3.

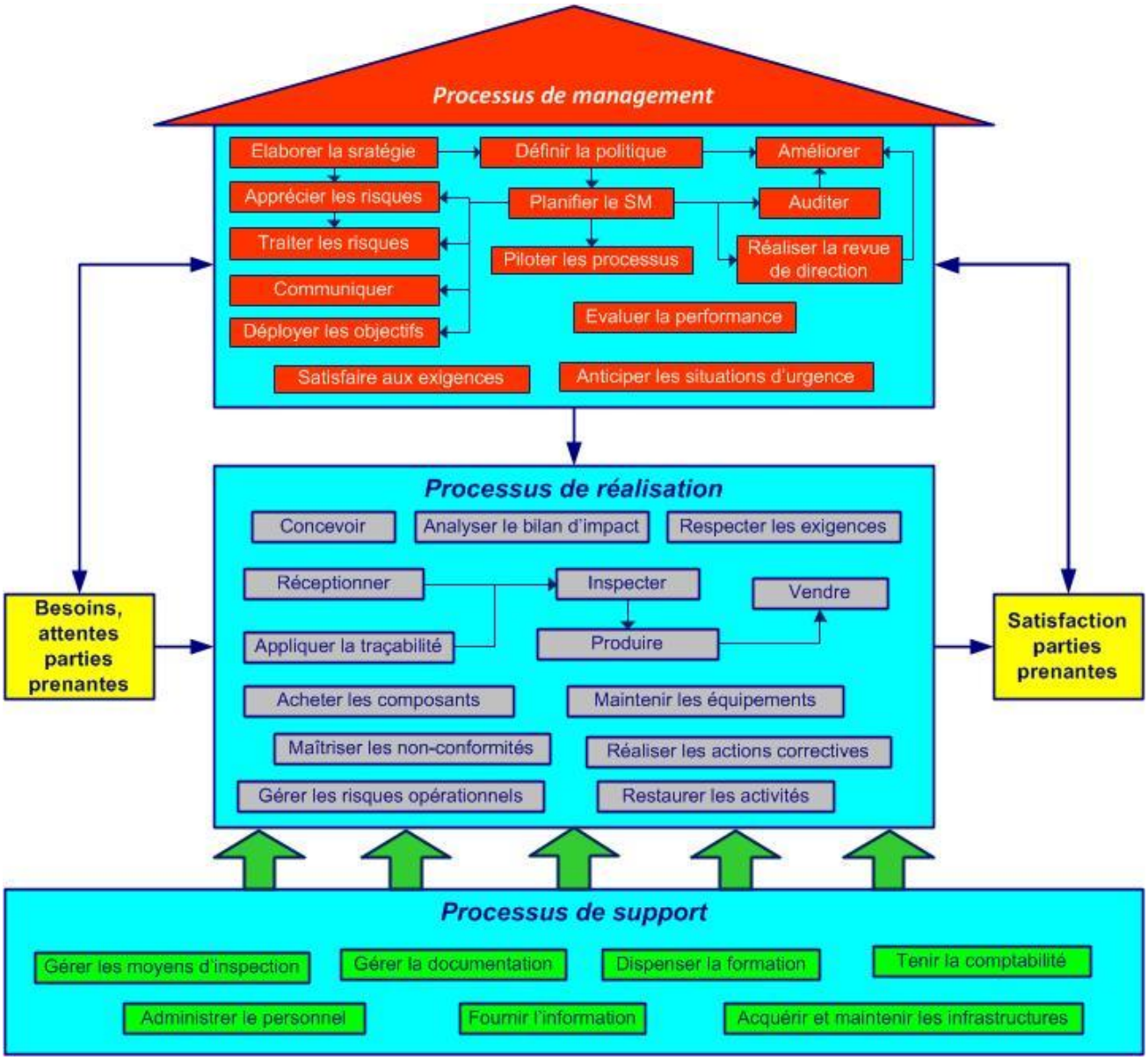


Figure 3-3. La maison des processus

La cartographie permet, entre autres :

- d'obtenir une vision globale de l'entreprise
- d'identifier les bénéficiaires (clients), les flux et les interactions
- de définir les règles (simples) de communication entre les processus

Pour obtenir une image plus claire on peut simplifier en utilisant au total une quinzaine de processus essentiels. Un processus essentiel peut contenir quelques sous-processus, par exemple dans un processus « Développer le SM » peuvent entrer les processus : 

- élaborer la stratégie
- gérer le risque
- satisfaire aux exigences
- définir la politique
- planifier le SM
- déployer les objectifs
- acquérir les ressources

- piloter les processus
- améliorer

Une liste de processus souvent utilisés est montrée dans l'annexe 04.

3.3 Approche processus

Les solutions simples pour maintenant, la perfection pour plus tard

Le quatrième principe de management de la qualité est « Approche processus », cf. ISO 9000, 2.3.4. Certains bénéfices :

- obtenir une vision globale de l'entreprise grâce à la cartographie
- identifier et gérer les responsabilités et ressources
- atteindre une gestion efficace de l'entreprise en s'appuyant sur les indicateurs des processus
- gérer les risques pouvant influe sur les objectifs

Approche processus : *management par les processus pour mieux satisfaire les clients, améliorer l'efficacité de tous les processus et augmenter l'efficience globale*

L'approche processus intégrée au cours du développement, la mise en œuvre et l'amélioration continue d'un système de management permet d'atteindre les objectifs liés à la protection de l'entreprise contre les crises, comme le montre la figure 3-4.

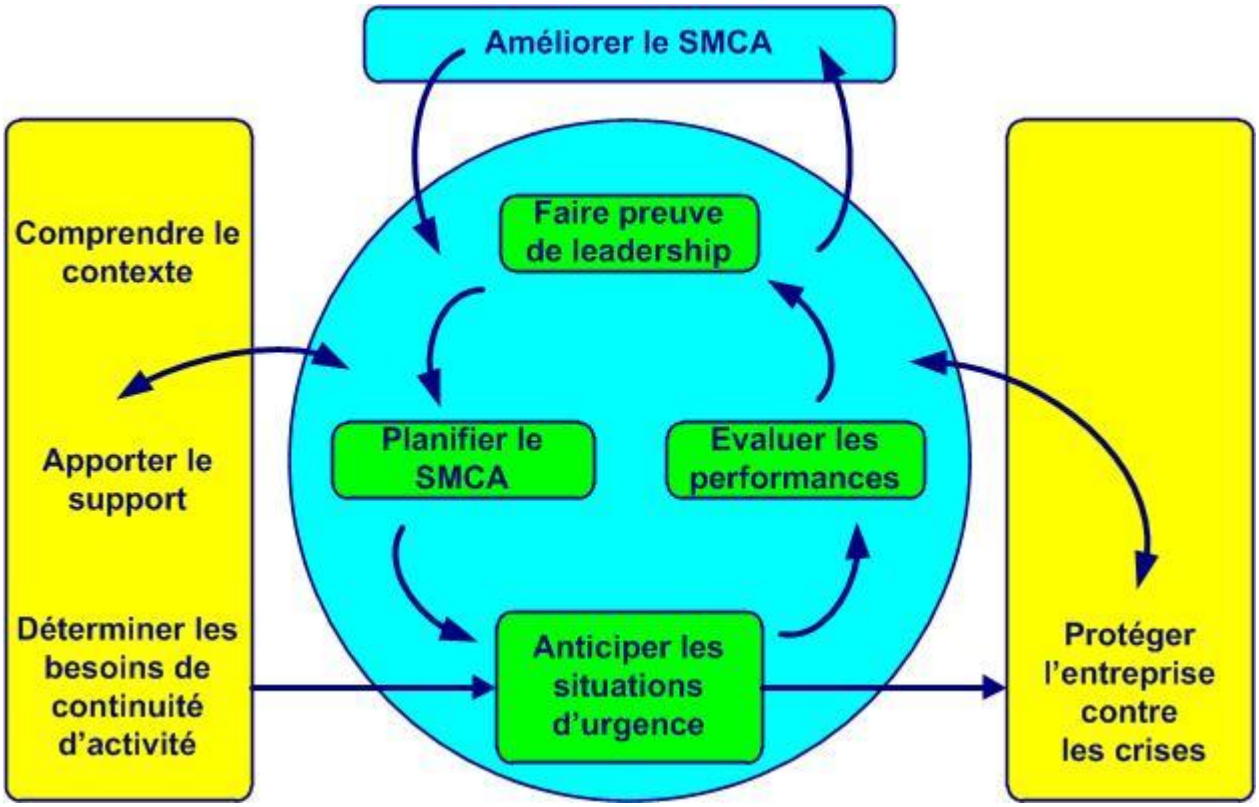


Figure 3-4. Modèle d'un SM basé sur l'approche processus et l'amélioration continue

L'approche processus (cf. annexe 05) :

- souligne l'importance :

    - de comprendre et de satisfaire les exigences de continuité d'activité
    - de la prévention pour réagir sur les éléments non voulus comme :
        - incidents
        - crises
        - catastrophes
    - de mesurer la performance des processus
    - d'améliorer en permanence ses objectifs sur la base de mesures objectives
    - de la valeur ajoutée des processus
- repose sur :
    - l'identification méthodique
    - les interactions
    - la séquence et
    - le management des processus qui consiste à :
        - déterminer les objectifs et leurs indicateurs
        - piloter les activités associées
        - analyser les résultats obtenus
        - entreprendre des améliorations en permanence
- permet :
    - de mieux visualiser les données d'entrée et de sortie et leurs interactions
    - de clarifier les rôles et responsabilités exercées
    - d'affecter judicieusement les ressources nécessaires
    - de faire tomber des barrières entre les départements
    - de diminuer les coûts, les délais, les gaspillages
- et assure à long terme :
    - la maîtrise
    - la surveillance et
    - l'amélioration continue des processus

L'approche processus **ce n'est pas** :

- la gestion de crise (« On ne résout pas les problèmes en s'attaquant aux effets »)
- blâmer le personnel (« La mauvaise qualité est le résultat d'un mauvais management ». Masaaki Imai)
- la priorité aux investissements (« Utilisez vos méninges, pas votre argent ». Taiichi Ohno)

4 Contexte

4.1 L'entreprise et son contexte *(exigence 1, voir aussi le quiz)*

Les deux choses les plus importantes n'apparaissent pas au bilan de l'entreprise : sa réputation et ses hommes. Henry Ford

Pour mettre en place avec succès un système de management de la continuité d'activité il faut bien comprendre et évaluer tout ce qui peut influer sur la raison d'être et la performance de l'entreprise pendant et après une perturbation. Il convient d'engager une réflexion approfondie après quelques activités essentielles :

- dresser un diagnostic approfondi du contexte unique dans lequel se trouve votre entreprise en prenant en compte les enjeux :
  - externes comme l'environnement :
    - social
    - réglementaire
    - économique
    - technologique
  - internes comme :
    - les aspects spécifiques de la culture d'entreprise :
      - vision
      - raison d'être, finalité, mission
      - valeurs essentielles
    - le personnel
    - les produits et services
    - les infrastructures
- surveiller et passer en revue régulièrement toute information relative aux enjeux externes et internes
- analyser les facteurs pouvant influer sur l'atteinte des objectifs de l'entreprise

Les analyses PESTEL et SWOT peuvent être utiles pour une analyse pertinente du contexte de l'entreprise (cf. annexe 07).

Une liste des enjeux externes et internes est réalisée par une équipe pluridisciplinaire. Chaque enjeu est identifié par son niveau d'influence et de maîtrise. La priorité est donnée aux enjeux très influents et pas du tout maîtrisés.

Bonnes pratiques

- *le diagnostic du contexte comprend les principaux enjeux externes et internes*
- *les valeurs essentielles comme la culture d'entreprise sont prises en compte*
- *les résultats de l'analyse du contexte sont largement diffusés*
- *l'analyse SWOT aide à l'identification des principales menaces et opportunités*

Écarts à éviter

- *des enjeux du contexte de l'entreprise comme l'environnement réglementaire ne sont pas pris en compte*
- *dans certains cas la culture d'entreprise n'est pas prise en compte*
- *les menaces et faiblesses identifiées dans l'analyse SWOT restent sans actions*

4.2 Besoins et attentes des parties prenantes *(exigences 2 à 6)*

Il n'y a qu'une seule définition valable de la finalité de l'entreprise : créer un client.
Peter Drucker

Pour bien comprendre les besoins et attentes des parties prenantes il faut commencer par déterminer tous ceux qui peuvent être concernés par le système de management de la continuité d'activité comme par exemple les :

- salariés
- clients
- prestataires externes
- propriétaires
- actionnaires
- banquiers
- distributeurs
- concurrents
- citoyens
- voisins
- organisations sociales et politiques

Chaque partie prenante est identifiée par son niveau d'influence et de maîtrise. La priorité est donnée aux parties prenantes très influentes et pas du tout maîtrisées. Une liste des parties prenantes est réalisée par une équipe pluridisciplinaire, cf. annexe 08.

Histoire vraie

Le client est roi mais on peut quand même lutter contre l'impolitesse. Exemple du restaurant niçois La petite Syrah et les prix du café :

Anticiper les besoins et attentes raisonnables et pertinentes des parties prenantes c'est :

- satisfaire aux exigences légales et réglementaires
- se préparer à faire face aux menaces
- saisir des opportunités d'amélioration

Le processus Identifier les exigences légales de continuité d'activité permet de prendre en compte les exigences obligatoires et de les respecter.

Les exigences peuvent concerner :

- la réponse aux incidents (gestion des urgences)
- la continuité d'activité (plan de continuité d'activité, programme d'exercices)
- la gestion du risque
- la gestion des dangers (matières chimiques)

Quand une exigence applicable est acceptée celle-ci devient une exigence interne du SMCA.

Bonnes pratiques

- *la liste des parties prenantes est à jour*
- *les besoins et attentes des parties prenantes sont établis au moyen de rencontres sur place, enquêtes, tables rondes et réunions (mensuelles ou fréquentes)*
- *l'application des exigences légales et réglementaires est une démarche de prévention et non une contrainte*

Écarts à éviter

- *des exigences réglementaires et légales ne sont pas prises en compte*
- *les attentes des parties prenantes ne sont pas déterminées*
- *la liste des parties prenantes ne contient pas leur domaine d'activité*

4.3 Domaine d'application du SMCA *(exigences 7 à 15)*

Dans beaucoup de domaines, le gagnant est celui qui est le mieux renseigné. André Muller

Le domaine d'application (ou autrement dit le périmètre) du présent module s'applique au système de management de la continuité d'activité (ou autrement dit à la gestion du risque de crise) dans l'entreprise et concerne :

- la localisation
- les produits et services
- les activités et processus
- les ressources

Le domaine d'application du SMCA est disponible aux parties prenantes, cf. annexe 09.

Quand une exigence ne peut pas être appliquée, une justification est incluse dans le document.

Le domaine d'application du SMCA de l'entreprise est établi en tenant compte :

- de sa raison d'être
- de ses produits et services
- de son contexte (enjeux internes et externes)
- des exigences des parties prenantes
- de la complexité de sa structure

Questions qui demandent des réponses :

- quel est l'activité de l'entreprise la plus vulnérable ?
- quel est le niveau maximal tolérable de perturbation ?
- quelles sont les obligations réglementaires applicables ?
- quels sont les risques prioritaires ?
- quelle crise peut nous surprendre ?
- l'équipe de crise est-elle préparée ?
- comment protéger le personnel et l'outil de travail ?
- quel est le plan pour maintenir une partie de l'activité ?
- comment rétablir l'activité normale dans les meilleurs délais ?

Dans ce module ne sont pas inclus spécifiquement les risques comptables et les risques extrêmes liés :

- aux crises financières
- à l'assurance
- à la fraude fiscale
- aux pièces de contrefaçon
- à la corruption

Exemple d'un domaine d'application

Pour un cirque les risques susceptibles de provoquer des soucis d'une représentation comprennent une coupure de courant, une tempête, l'absence de plusieurs acteurs ou techniciens (maladie ou conflit social), des problèmes de transport importants pour le public.

Après avoir identifié, analysé et évalué les risques qui pourraient perturber la représentation, la direction doit décider quelles actions appliquer pour réduire les chances d'annulation.

La continuité d'activité concerne de nombreux domaines et risques :

- le personnel
- la réputation de l'entreprise
- les produits et projets
- l'assurance
- la rupture d'approvisionnement
- le manque de compétences
- les menaces terroristes
- les catastrophes naturelles

Pour bien déterminer le domaine d'application du SMCA sont pris en compte les spécificités du contexte de l'entreprise comme :

- les enjeux (cf. paragraphe 4.1)
- les produits et services
- la culture d'entreprise
- l'environnement :
    - social
    - financier
    - technologique
    - économique
- les exigences des parties prenantes (cf. paragraphe 4.2)

- les processus externalisés

Bonnes pratiques

- *le domaine d'application est pertinent et disponible sur simple demande*
- *les exigences non applicables sont justifiées par écrit*

Écarts à éviter

- *certains ateliers sont en dehors du domaine d'application du SMCA sans justification*
- *le domaine d'application est obsolète (la nouvelle filiale n'est pas incluse)*

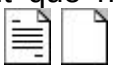
4.4 Système de management de la continuité d'activité *(exigence 16)*

Mieux vaut prévenir que guérir

Les exigences de la norme ISO 22301 concernent :

- le contexte de l'entreprise
- la politique et les objectifs de continuité d'activité
- la réponse aux perturbations
- l'évaluation de la performance du SMCA
- l'amélioration continue du SMCA

Pour cela :

- le système de management de la continuité d'activité est :
  - établi
  - documenté (un système documentaire simple et suffisant est mis en place)
  - mis en œuvre et
  - amélioré en continu
- la politique continuité d'activité, les objectifs, les ressources et l'environnement du travail sont déterminés
- les menaces sont identifiées et les actions pour les réduire sont établies (cf. paragraphe 6.1)
- les processus essentiels nécessaires au SMCA sont maîtrisés :
  - les ressources correspondantes assurées
  - les éléments d'entrée et de sortie déterminés
  - les informations nécessaires disponibles
  - les pilotes nommés (responsabilités et autorités définies)
  - les séquences et les interactions déterminées
  - chaque processus est mesuré et surveillé (critères établis), les objectifs sont établis et les indicateurs de performance analysés
  - les performances des processus sont évaluées
  - les changements nécessaires sont introduits pour obtenir les résultats attendus
  - les actions pour obtenir l'amélioration continue des processus sont établies
- le strict minimum nécessaire (« autant que nécessaire ») des documents sur les processus est tenu à jour et conservé ()

Pièges à éviter :

- faire de la sur-qualité :
  - une opération inutile est réalisée sans que cela ajoute de la valeur – c'est un gaspillage, cf. les outils qualité E 12
- faire écrire toutes les procédures par le responsable du PCA :
  - la sécurité est l'affaire de tous, « le personnel a conscience de la pertinence et de l'importance de chacun à la contribution aux objectifs », ce qui est encore plus vrai pour les chefs de départements et les pilotes de processus
- oublier les spécificités liées à la culture d'entreprise :
  - innovation, luxe, secret, management autoritaire (Apple)
  - culture forte liée à l'écologie, à l'action et la lutte, tout en cultivant le secret (Greenpeace)
  - culture d'entreprise fun et décalée (Michel&Augustin)
  - entreprise libérée, l'homme est bon, aimer son client, rêve partagé (Favi, cf. F 50)

Les exigences de la norme ISO 22301 sont montrées en figure 4-1 :

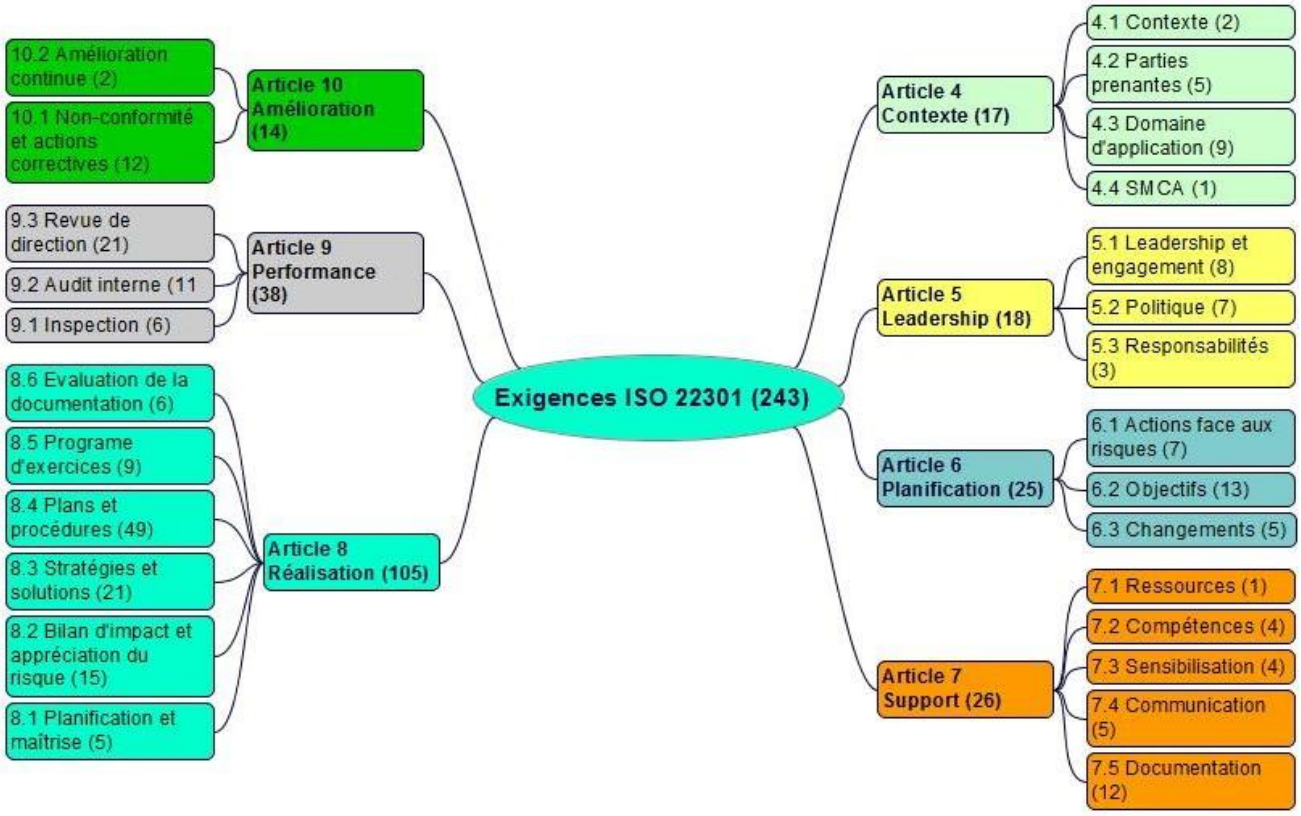


Figure 4-1. Les exigences de la norme ISO 22301

Un SMCA efficace est surtout orienté sur :

- les conséquences potentielles
- la capacité des activités critiques
- les exercices de simulation en équipe

- les réponses flexibles

N'hésitez pas à chercher des réponses dans l'ISO 22313 (« Lignes directrices sur l'utilisation de l'ISO 22301 ») quand vous ne les trouvez pas dans le présent module, cf. paragraphe 2.2.

Bonnes pratiques

- *la cartographie des processus contient assez de flèches pour bien montrer qui est le client (interne ou externe)*
- *beaucoup de flèches (plusieurs clients) sont utilisées pour les processus (aucun client n'est oublié)*
- *pendant la revue de processus la valeur ajoutée du processus est bien dévoilée*
- *l'analyse de la performance des processus est un exemple de preuve d'amélioration continue de l'efficacité du SMCA*
- *la direction surveille régulièrement les objectifs et les plans d'action*
- *les engagements de la direction relatifs à l'amélioration continue sont largement diffusés*
- *la finalité de chaque processus est clairement définie*

Écarts à éviter

- *certains éléments de sortie de processus ne sont pas correctement définis (clients non pris en compte)*
- *critères d'efficacité des processus non établis*
- *pilote de processus non formalisé*
- *processus externalisés non déterminés*
- *des activités bien réelles ne sont pas identifiées dans aucun processus*
- *maîtrise des prestations externalisées non décrite*
- *séquences et interactions de certains processus ne sont pas déterminées*
- *critères et méthodes pour assurer la performance des processus non définis*
- *surveillance de la performance de certains processus non établie*
- *les ressources du SMCA ne permettent pas d'atteindre les objectifs de continuité d'activité*
- *le SMCA n'est pas à jour (nouveaux processus non identifiés)*