E 24v13

Préparation à l'ISO 27001 version 2013

Objectif

Objectif du module : Préparation à la mise en œuvre, la certification, le maintien et l'amélioration de votre système de management de la sécurité de l'information (ISO 27001) pour pouvoir :

- garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information
- réduire les risques liés à la sécurité de l'information
- saisir des opportunités d'amélioration continue

1 Sécurité de l'information

1.1 Historique

Les informations, le matériel informatique et les logiciels que possède une organisation est un investissement précieux qu'il faut protéger. Une des meilleures façons de prendre soin de ce trésor est de mettre en place un système de management de la sécurité de l'information (SMSI).

En 1989 sort le code de pratique des utilisateurs (*User's Code of Practice*), basé sur la politique de sécurité de Shell, à la demande du gouvernement britannique *(Department of Trade and Industry).*

En 1995, la norme britannique BS 7799 est publiée.

En 1996 est publiée la norme ISO 13335 qui après sa dernière version de 2004 sera remplacée par l'ISO/CEI 27001.

L'ISO (Organisation internationale de normalisation) a été créée en 1947. ISO vient du grec « isos » (égal). Pour + de simplicité nous utilisons ISO à la place d'ISO/CEI.

L'historique des transformations et versions de la famille des normes ISO 27000 est montré dans la figure 1-1.

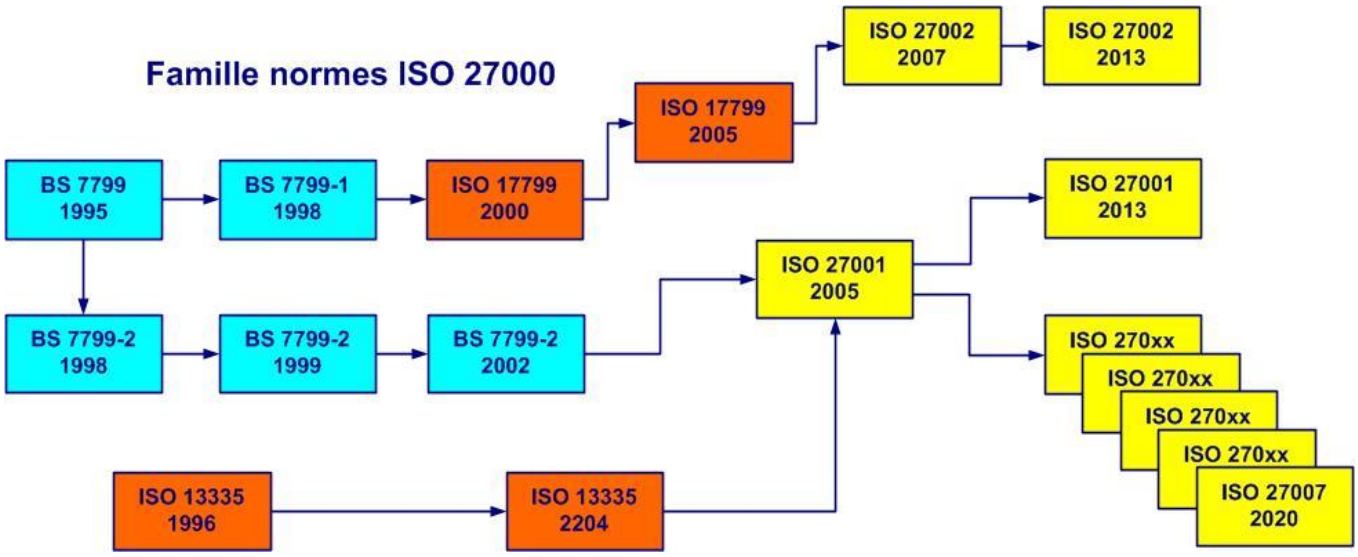


Figure 1-1. Historique des normes de la famille ISO 27000

Depuis 2005 l'ISO/CEI 27001:2005 offre la possibilité de certification d'un système de management de la sécurité de l'information.

En 2013, sortent les normes ISO/CEI 27001:2013 et ISO/CEI 27002:2013. Suivent une grande quantité de normes qui forment la famille ISO/CEI 27000. Pour plus de détails voir le paragraphe 2.2.

1.2 Application

La sécurité de l'information est l'affaire de tous

La norme ISO 27001 (**Technologies de l'information – Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences**) est générique car elle

s'applique au système de management de toute organisation, sans aucune contrainte relative à la taille, l'activité ou le type. C'est une norme volontaire internationale qui permet la certification par un organisme accrédité (de certification).

La mise en place d'un système de management de la sécurité de l'information est toujours :

- issue d'une décision stratégique de la direction
- en accord avec :
  - les objectifs de l'organisation
  - la culture d'entreprise
  - les processus métier

L'application de la norme ISO 27001 et le respect de ses exigences permet de préserver la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information.

Le respect des exigences liées à l'appréciation et au traitement des risques (en se basant sur la norme ISO 31000) permet de rassurer les parties intéressées sur la gestion de la sécurité de l'information.

1.3 Principes et étapes

La sécurité est un processus. John Mallery

La démarche sécurité de l'information (SI) est un état d'esprit qui part de la direction comme décision stratégique prioritaire et s'étend à l'ensemble du personnel. La direction définit la politique de sécurité de l'information, dans laquelle sont fixés les objectifs de sécurité de l'information, qui sont applicables à toutes les activités. L'outil utilisé pour atteindre les objectifs est le système de management de la sécurité de l'information. La prévention est le concept essentiel du système de management de la sécurité de l'information.

Les trois propriétés essentielles de la sécurité de l'information sont la confidentialité, l'intégrité et la disponibilité comme montré dans la figure 1-2.

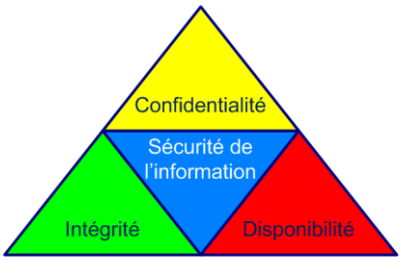


Figure 1-2. Propriétés de la sécurité de l'information

Prenons comme exemple votre compte en banque. L'information sur le compte doit être protégée :

- sa confidentialité – l'information doit rester secrète
- son intégrité – l'information du total doit être exacte et ne doit pas changer
- sa disponibilité – l'information doit rester accessible en temps voulu

Tout système de management de la sécurité de l'information comprend trois démarches distinctes et interdépendantes :

- l'approche processus
- l'approche par les risques (*risk-based thinking*)
- l'amélioration continue

Les sept principes de management de la qualité (cf. figure 1-3) nous aiderons à obtenir des performances durables (cf. ISO 9000 : 2015, § 2.3).

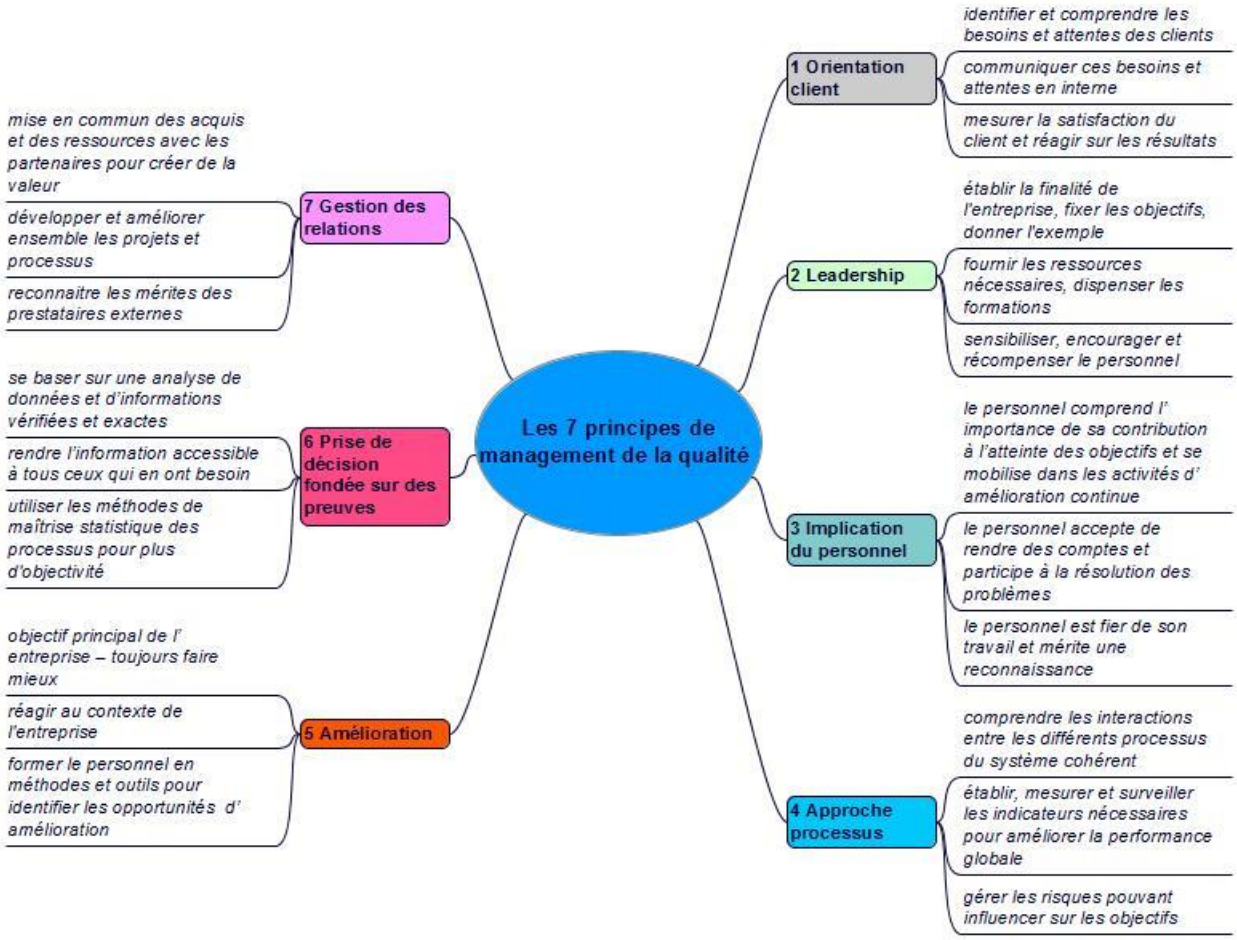


Figure 1-3. Les 7 principes de management de la qualité

Une démarche bien préparée est à moitié réussie

La démarche pour mettre en œuvre un système de management de la sécurité de l'information passe par plusieurs étapes. Un exemple de préparation est montré en figure 1-4.

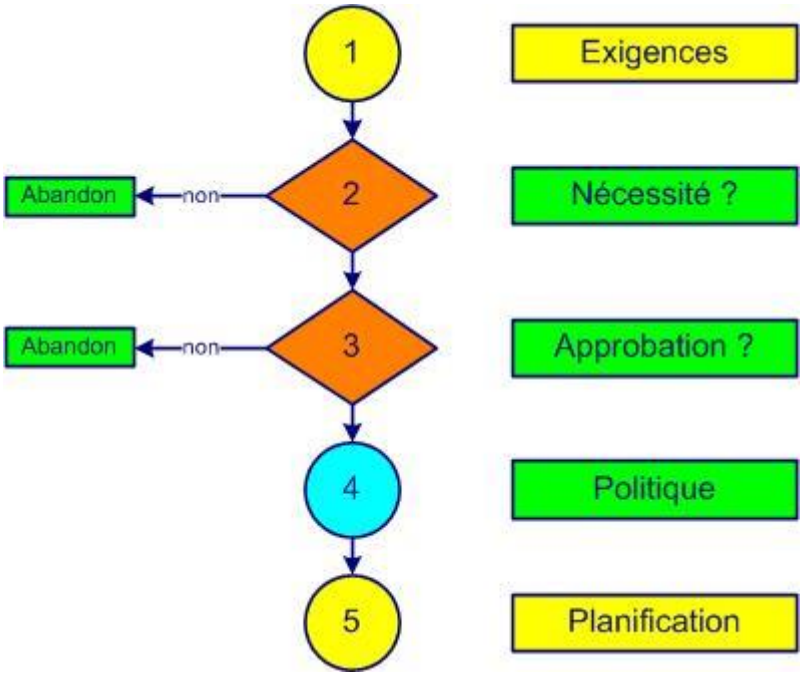


Figure 1-4. Préparation d'un SMSI

L'**étape 1** comporte la détermination des besoins et attentes (**exigences**) des parties intéressées :

- personnel
- clients, consommateurs
- concurrents
- actionnaires, investisseurs
- prestataires externes (fournisseurs, sous-traitants, partenaires)
- organisations et associations de branche
- autorités légales et réglementaires

L'implication de la direction à son plus haut niveau est réellement indispensable. Les conseils d'un consultant sont souvent sollicités. C'est le moment pour réaliser un état des lieux du système de management (ou de ce qui existe). Choisir un organisme externe de certification.

Une des questions clés qui vient très vite (**étape 2**) est la **nécessité** de cette décision. Si cela n'est vraiment pas nécessaire ou si l'estimation des coûts de la démarche de certification dépasse les ressources disponibles ou la valeur des actifs à protéger, on fera mieux d'abandonner tout de suite.

Les bénéfices de la mise en place d'un système de management de la sécurité de l'information sont souvent :

- sécurité augmentée des systèmes de l'information
- résistance renforcée aux menaces et logiciels malveillants
- l'information est disponible uniquement aux personnes qui ont l'autorisation
- l'information est protégée contre toute modification par du personnel non autorisé
- protection améliorée :
  - des informations opérationnelles
  - des secrets d'entreprise
  - de la propriété intellectuelle
  - des données personnelles
- responsabilités et obligations mieux définies
- vraisemblance d'apparition diminuée d'incidents de sécurité de l'information

- niveau de maîtrise des risques élevé
- ruptures d'activité évitées
- coûts d'assurance réduits
- implication active du personnel dans l'amélioration de la sécurité de l'information
- obligations légales à jour
- forte intégration de la sécurité de l'information aux processus métier
- culture d'amélioration continue de la sécurité de l'information
- vous laisse dormir plus tranquillement 

Les bénéfices de la certification d'un système de management sont souvent :

- image de l'organisation améliorée
- un pas devant la concurrence
- nouveaux clients
- confiance améliorée des parties intéressées
- part de marché accrue
- hausse des ventes
- meilleure performance financière

Plus d'un million et demi d'entreprises dans le monde entier ne peuvent pas se tromper !

La **troisième étape** doit déterminer si cette démarche reçoit l'**approbation** du personnel. Une campagne de communication en interne est lancée sur les objectifs du système de management de la sécurité de l'information (SMSI). Le personnel est sensibilisé et comprend que sans sa participation le projet ne pourra aboutir.

Ayez confiance, le succès viendra avec l'implication et l'effort de tout le personnel !

Définir la vision (ce que nous voulons être), la mission (pourquoi nous existons) et le plan stratégique de l'organisation. L'**étape suivante** (**4**) comprend l'établissement d'une ébauche de la **politique de sécurité de l'information** et des objectifs de sécurité de l'information. Si vous ne possédez pas encore un exemplaire de la norme ISO 27001, c'est le moment de l'obtenir (cf. § 2.1 du présent module).

La **planification** est la dernière **étape** (**5**) de la préparation du projet d'obtention de la certification ISO 27001. Une période raisonnable se situe entre 12 à 24 mois (chaque organisation est spécifique et unique). Les ressources (financières et en personnel) sont confirmées par la direction. L'engagement de la direction est formalisé par écrit et communiqué à l'ensemble du personnel. Une personne est nommée chef du projet d'obtention du certificat ISO 27001.

L'établissement et la mise en place du système de management de la sécurité de l'information ISO 27001 sont montrés dans la figure 1-5.

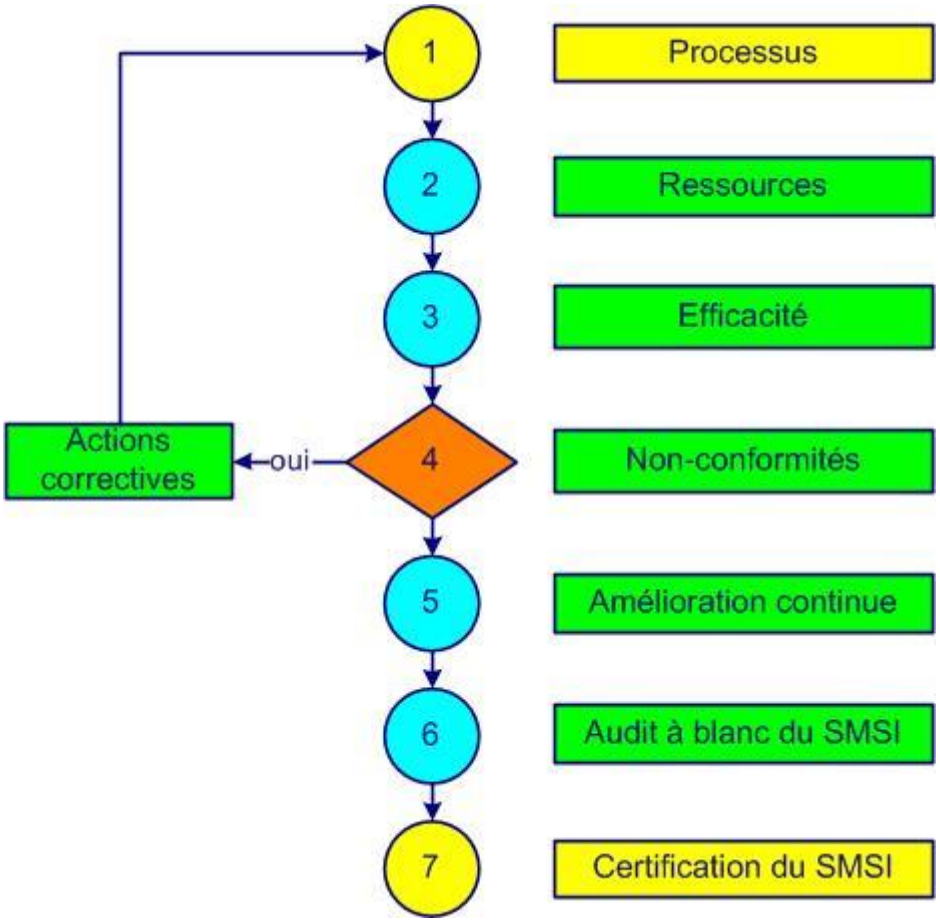


Figure 1-5. Mise en œuvre d'un SMSI

L'**étape 1** consiste à identifier et définir les **processus**, les interactions, les pilotes, les responsabilités et les brouillons de certaines informations documentées. Avec la participation du maximum de personnes disponibles sont rédigés les premières versions des fiches de processus, des descriptions de fonction et des instructions de travail.

Dans l'**étape 2** sont fixées les **ressources** nécessaires pour atteindre les objectifs de sécurité de l'information. 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. Des audits internes permettent d'évaluer le degré de la mise en place du système.

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

Une première appréciation des outils et domaines 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 saisies. Une approche de prévention des non-conformités et d'élimination des causes est établie. La communication en interne et en externe est établie et formalisée.

Pour effectuer l'**audit à blanc du SMSI** (**étape 6**) les informations documentées sont vérifiées et approuvées par les personnes appropriées. Une revue de direction permet d'évaluer le respect des exigences applicables. La politique de sécurité de l'information et les objectifs sont finalisés. Un responsable sécurité de l'information d'une autre organisation ou un consultant pourra fournir de précieuses remarques, suggestions et recommandations.

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

Un exemple de plan de projet de certification 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 sécurité de l'information 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 1-6) 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.

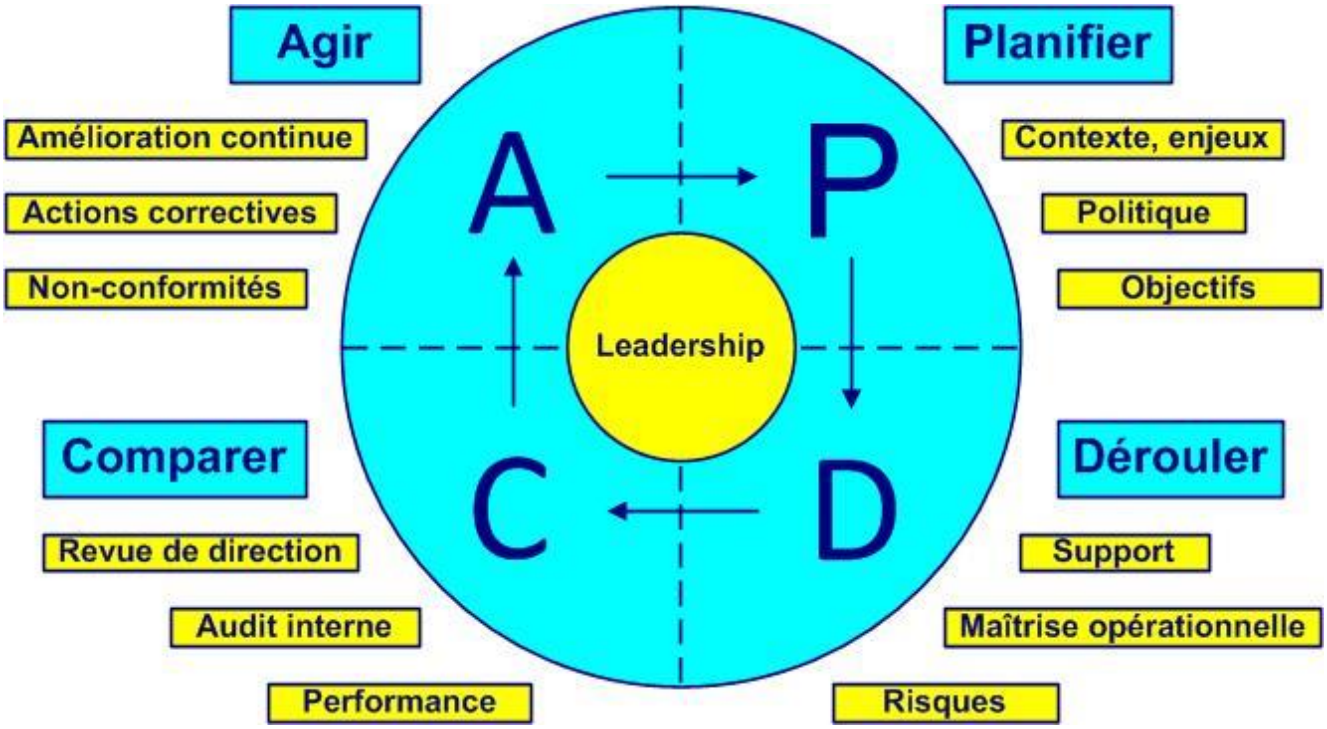


Figure 1-6. Le cycle de Deming

- Plan – Planifier, définir le contexte, les enjeux et les processus, faire preuve de leadership, établir la politique et les objectifs (articles 4, 5 et 6)
- Do – Dérouler, traiter les risques, développer, mettre en œuvre et maîtriser les processus, faire preuve de leadership, apporter le support (articles 5, 7 et 8)
- Check – Comparer, vérifier, évaluer les risques, la performance, inspecter, analyser les données, réaliser les audits et revues de direction, faire preuve de leadership (articles 5 et 9)
- Act – 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.

2 Normes, définitions, livres

2.1 Normes

Prévoir pour ne pas subir

La famille ISO 27000 comprend un grand nombre de normes. Une partie des normes les plus utilisées est montrée dans la figure 2-1 :

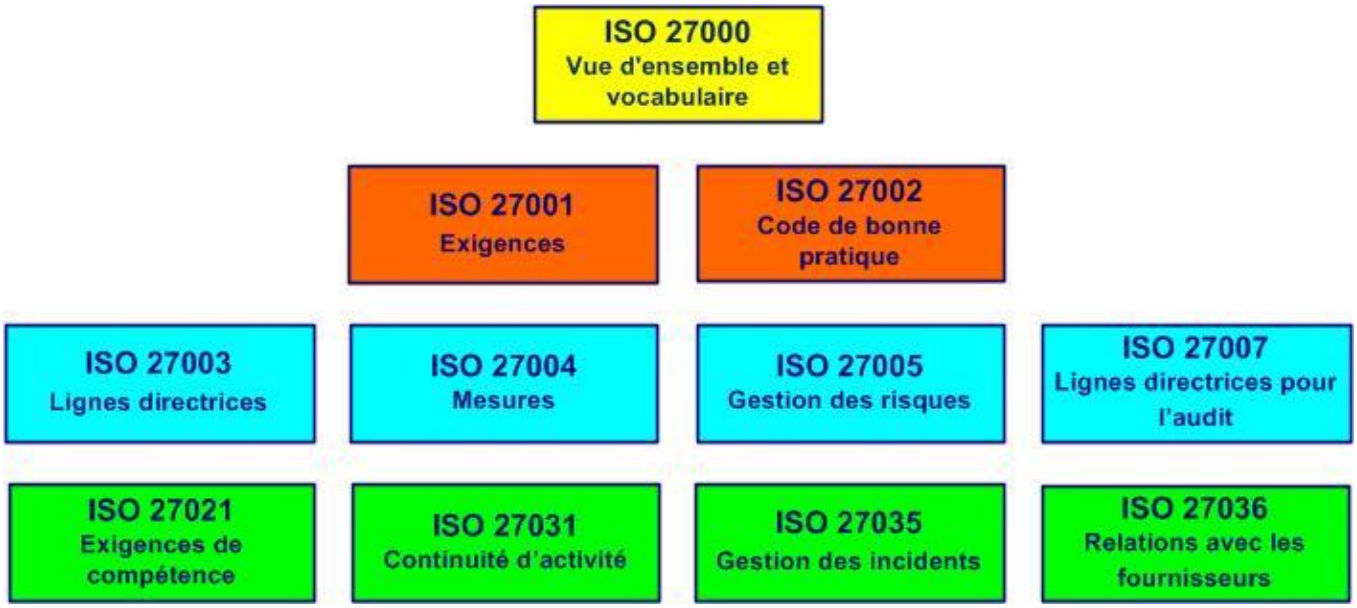


Figure 2-1. Normes de la famille ISO 27000

- **ISO 27000:2018** - Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information (gratuit – PAS - Spécifications publiquement disponibles) — Vue d'ensemble et vocabulaire
- **ISO 27001:2013** – Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
- **ISO 27002:2013** Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information
- **ISO 27003:2017** – *Information technology — Security techniques — Information security management systems — Guidance* **(**Technologies de l'information — Techniques de sécurité —Systèmes de management de la sécurité de l'information — Lignes directrices)
- **ISO 27004:2016** – *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation* (Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation)
- **ISO 27005:2018** – Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information
- **ISO 27007:2020** - *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing* (Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information)
- **ISO 27008 :2019** - *Information technology — Security techniques — Guidelines for the assessment of information security controls* (Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information)

- **ISO 27021:2017** – *Information technology — Security techniques — Competence requirements for information security management systems professionals* (Technologies de l'information — Techniques de sécurité — Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité)
- **ISO 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 27035-1:2016** - *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management* (Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information — Partie 1: Principes de la gestion des incidents)
- **ISO 27035-2:2016** - *Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response* (Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information — Partie 2: Lignes directrices pour planifier et préparer une réponse aux incidents)
- **ISO 27035-3:2020** - *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations* (Technologies de l'information — Gestion des incidents de sécurité de l'information — Partie 3: Lignes directrices relatives aux opérations de réponse aux incidents TIC)
- **ISO 27036-1:2014** - *Information technology — Security techniques (gratuit – PAS - Spécifications publiquement disponibles) — Information security for supplier relationships — Part 1: Overview and concepts* (Technologies de l'information - Techniques de sécurité - Sécurité de l'information dans les relations avec les fournisseurs - Partie 1 : Vue d'ensemble et concepts)
- **ISO 27036-2:2014** - *Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements* (Technologies de l'information - Techniques de sécurité - Sécurité de l'information dans les relations avec les fournisseurs - Partie 2 : Exigences)

Remarque : certaines versions « plus récentes » (exemple pour l'ISO 27001 et l'ISO 27002 version 2017), incluent des correctifs mineurs et reprennent la version en vigueur intégralement (dans ce cas celles de 2013).

La norme sur l'audit est :

L'ISO 19011 (2018) : Lignes directrices pour l'audit des systèmes de management

La norme ISO 31000 : 2018 Management du risque – Lignes directrices établit les principes et le processus de management du risque, l'appréciation et le traitement du risque.

Le rapport technique ISO/TR 31004 : 2013 Management du risque — Lignes directrices pour l'implémentation de l'ISO 31000 permet de mieux comprendre les principes et le cadre organisationnel de management du risque.

La norme sur la continuité d'activité est : ISO 22301 (2019) Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences.

Deux documents français liés aux processus avec des explications, recommandations et exemples :

- AC X50-178 (accord, 2002) Management de la qualité – Management des processus – Bonnes pratiques et retours d'expérience
- FD X50-176 (fascicule de documentation, 2005) Outils de management – Management des processus

Les normes ISO (plus de 21 000) sont utilisées dans d'innombrables domaines et sont reconnues dans le monde entier.

Tous ces référentiels et beaucoup d'autres peuvent être commandés (sous format électronique ou papier) sur le site de l'AFNOR (Association française de normalisation) dans la rubrique boutique, catalogue, normes.

Plus de 28 000 normes (en anglais et autres langues) sont disponibles gratuitement sur le site Public.resource.Org.

2.2 Définitions

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

Certains termes spécifiques :

Actif : *tout élément ayant de la valeur pour l'organisation*
Action corrective : *action pour éliminer les causes d'une non-conformité ou tout autre événement indésirable et empêcher leur réapparition*
Appréciation du risque : *processus d'identification, d'analyse et d'évaluation du risque*
Client : *celui qui reçoit un produit*
Compétence : *aptitudes, connaissances et expériences personnelles*
Confidentialité : *propriété d'une information d'être dévoilée aux seules personnes autorisées (voir aussi ISO 27000, 3.10)*
Conformité : *satisfaction d'une exigence spécifiée*
Cryptographie : *activités de protection de la confidentialité d'une information à l'aide de codification et de décodification*
Déclaration d'applicabilité (DdA) : *document décrivant les objectifs et les mesures de sécurité*
Direction : *groupe ou personnes chargées de la gestion au plus haut niveau de l'entreprise*
Disponibilité : *propriété d'une information d'être accessible en temps voulu aux seules personnes autorisées (voir aussi ISO 27000, 3.7)*
Efficacité : *capacité de réalisation des activités planifiées avec le minimum d'efforts*
Efficience : *rapport financier entre le résultat obtenu et les ressources utilisées*
Exigence : *besoin ou attente implicite ou explicite*
Incident (de sécurité de l'information) : *événement indésirable et inattendu qui peut compromettre la sécurité de l'information (voir aussi ISO 27000, 3.31)*
Indicateur : *valeur d'un paramètre, associé à un objectif, permettant de façon objective d'en mesurer l'efficacité*
Information documentée : *tout support permettant le traitement d'une information*
Intégrité : *propriété d'une information d'être non altérée (voir aussi ISO 27000, 3.36)*
Non-conformité : *non-satisfaction d'une exigence spécifiée*
Objectif : *but mesurable à atteindre*
Organisation (entreprise) : *structure qui satisfait un besoin*
Partie intéressée : *personne, groupe ou organisation pouvant affecter ou être affecté par une entreprise*
Prestataire externe (fournisseur) : *celui qui procure un produit*
Processus : *activités qui transforment des éléments d'entrée en éléments de sortie*
Produit (ou service) : *tout résultat d'un processus ou d'une activité*
Qualité : *aptitude à satisfaire aux exigences*
Risque résiduel : *risque accepté (voir aussi ISO Guide 73, 3.8.1.6)*
Risque : *vraisemblance d'apparition d'une menace ou d'une opportunité*
Satisfaction du client : *objectif prioritaire de chaque système de management*
Sauvegarde: *copie de données afin d'archiver et protéger contre la perte*

Sécurité de l'information (SI) : *mesures permettant de protéger la confidentialité, l'intégrité et la disponibilité de l'information (voir aussi ISO 27000, 3.28)*
SI : *sécurité de l'information*
SMSI : *système de management de la sécurité de l'information*
Système de management : *ensemble de processus permettant d'atteindre les objectifs*
Traçabilité : *aptitude à mémoriser ou restituer tout ou partie d'une trace des fonctions exécutées*
Traitement du risque : *activités de modification du risque (voir aussi ISO Guide 73, 3.8.1)*
VLAN : *Virtual Local Area Network*, *Réseau local virtuel*
Vulnérabilité : *faiblesse d'un actif pouvant conduire à un accès non autorisé (voir aussi ISO 27000, 3.77)*

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, défaut, défaillance, dysfonctionnement, gaspillage, non-conformité et rebut :
  - l'anomalie est une déviation par rapport à ce qui est attendu
  - le défaut est la non-satisfaction d'une exigence liée à une utilisation prévue
  - la défaillance c'est quand une fonction est devenue inapte
  - le dysfonctionnement est un fonctionnement dégradé qui peut entraîner une défaillance
  - le gaspillage c'est quand il y a des coûts ajoutés mais pas de valeur
  - 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 produit
  - l'audité est celui qui est audité
  - l'auditeur est celui qui réalise l'audit
- 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
- 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
- incident et non-conformité
  - l'incident est un événement indésirable
  - la non-conformité est le non-respect d'une exigence
- 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
- 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
- programme d'audit et plan d'audit
    - le programme d'audit est la planification annuelle des audits
    - le plan d'audit est le descriptif des activités d'un audit
- sécurité et sureté
    - la sécurité (*security*) est la prévention contre les risques d'origine involontaire
    - la sureté (*safety*) est la prévention contre les risques malveillants
- 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

Les informations sont stockées de multiples façons comme :

- numérique (données stockées électroniquement)
- forme matérielle (sur papier ou autres)
- connaissances (le savoir-faire du personnel)

Les informations sont transmises de différentes manières comme :

- numérique (courrier électronique)
- physiquement (poste)
- verbalement (réunions)

Remarque 1 : le mot anglais « control » a plusieurs sens. Il peut être traduit par maîtrise, mesure, autorité, commande, gestion, contrôle, surveillance, inspection. Pour éviter des malentendus notre préférence est pour maîtrise, mesure et inspection au détriment de contrôle.

Remarque 2 : entre processus et procédé notre préférence est pour processus (en anglais « process »).

Remarque 3 : un actif est une notion large. Un actif peut être :

- *une information*
- *un document*
- *une archive*
- *une infrastructure*
- *un matériel technique*
- *un logiciel*
- *le personnel*
- *la renommée de l'organisation*
- *un processus*
- *un service*

Remarque 4 : l'utilisation des définitions de l'ISO 9000 et de l'ISO 27001 est recommandée. Le plus important est de définir pour tous dans l'organisation un vocabulaire commun et sans équivoque.

Remarque 5 : information documentée est toute information que l'on doit tenir à jour (procédure) ou conserver (enregistrement, instruction).

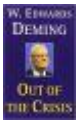
Pour d'autres définitions, commentaires, explications et interprétations que vous ne trouvez pas dans ce module et l'annexe 06 vous pouvez consulter :

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

2.3 Livres

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

Pour aller plus loin quelques livres sur la qualité et la sécurité de l'information :

- 

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

Hors de la crise, Economica, 1991)
- 

Eliyahu Goldratt, Jeff Cox, The Goal, A Process of Ongoing Improvement, North River Press, 1984 (

Le But, un processus de progrès permanent, AFNOR, 1986)
- 

Masaaki Imai, KAIZEN, The key to Japan's competitive success, McGraw-Hill, 1986 (
KAIZEN, La clé de la compétitivité japonaise, Eyrolles, 1989)
- 

Ulrich Beck, La Société du risque – Sur la voie d'une autre modernité, Flammarion, 2008
- 
Jean-François Zobrist, Un petit patron naïf et paresseux, Stratégie & Avenir, 2009
- 

Bernard Foray, La fonction RSSI : Guide des pratiques et retours d'expérience, Dunod, 2011
- 
Thierry Boileau, Iso 27001, un système de management de la sécurité de l'information, Univ Européenne, 2012

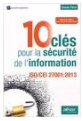
- 

Pascal Weber, Luc Villedieu, La sécurité de l'information: Mettre en pratique les exigences ISO 27001 : 2013, CreateSpace Independent Publishing Platform, 2014
- 

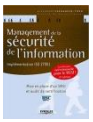
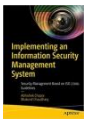
Edward Humphreys, Implementing the ISO/IEC 27001 2013 ISMS Standard, Artech House, 2016 (Mise en œuvre de la norme ISO/IEC 27001:2013 SMSI)
- 
Douglas Landoll, Information security policies, procedures, and standards, Auerbach Publications, 2016 (Politiques, procédures et normes en matière de sécurité de l'information)
- 
Alexandre Fernandez Toro, Comprendre et mettre en œuvre la norme ISO 27001: Conseils pratiques d'implémentation, CreateSpace Independent Publishing Platform, 2016
- 

Dejan Kosutic, Secure & simple, A small-business guide to implementing iso 27001 on your own, Advisera Expert Solutions, 2016 (Sécurisé et simple, Un guide pour les petites entreprises qui souhaitent mettre en œuvre l'ISO 27001 elles-mêmes)
- 
Dejan Kosutic, ISO 27001 Risk management in plain english, step-by-step handbook for information security practitioners in small businesses, Advisera Expert Solutions, 2016 (ISO 27001 Gestion des risques en bon anglais, Manuel par étapes à l'intention des praticiens de la sécurité de l'information dans les petites entreprises)
- 
Dejan Kosutic, ISO 27001 annex A controls in plain english, Step-by-step handbook for information security practitioners in small businesses, Advisera Expert Solutions, 2016 (Mesures de l'ISO 27001 Annexe A en bon anglais, Manuel par étapes à l'intention des praticiens de la sécurité de l'information dans les petites entreprises)
- 

Alexandre Fernandez Toro, Sécurité opérationnelle : Conseils pratiques pour sécuriser le SI, Eyrolles, 2016
- 
Alan Calder, Iso27001/Iso27002: Un guide de poche, It Governance, 2017
- 

Alan Calder, Neuf étapes vers le succès: Un aperçu de la mise en œuvre de la norme ISO 27001:2013, IT Governance, 2017
- 

Claude Pinet, 10 clés pour la sécurité de l'information: ISO/CEI 27001-2013, AFNOR, 2017

-  Jules Rémy, L'informatique maîtrisée dans ma PME, La ronde des Vivetières, 2017
-  Raphaël Hertzog et al, Kali Linux Revealed: Mastering the Penetration Testing Distribution, OFFSEC Press, 2017 (Kali Linux révélé : Maîtriser la distribution des tests de pénétration)
-  Michel Cattan, Guide des processus: Passons à la pratique ! - 3e édition entièrement révisée, conforme à la version 2015 de l'Iso 9001, AFNOR, 2018
-  Alexandre Fernandez-Toro, Management de la sécurité de l'information: Présentation générale de l'ISO 27001 et de ses normes associées - Une référence opérationnelle pour le RSSI, Eyrolles, 2018
-  Géraldine Sutra, Management du risque : une approche stratégique, AFNOR, 2018
-  Cees van der Wens, ISO 27001 handbook: Implementing and auditing an 'Information Security Management System' in small and medium-sized businesses, Brave New Books, 2020 (Mise en œuvre et audit d'un "système de gestion de la sécurité de l'information" dans les petites et moyennes entreprises)
-  Abhishek Chopra, Mukund Chaudary, Implementing an Information Security Management System, Apress , 2020 (Mise en œuvre d'un système de gestion de la sécurité de l'information)
-  Joseph Steinberg, La cybersécurité pour les nuls, First Interactive, 2020
-  Anne Lupfer, Gestion des risques en sécurité de l'information, Mise en œuvre de la norme ISO 27005, Eyrolles, 2021 (2010)

3 Approche processus

3.1 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 prestataires externes

Un processus est défini entre autres par :

- son intitulé et son type
- sa finalité (pourquoi ?)
- son bénéficiaire (pour qui ?)
- son domaine et activités
- ses déclencheurs
- ses informations documentées
- 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 conduite périodiquement par le pilote du processus (cf. annexe 02).

Revue : *examen d'un dossier, d'un produit, d'un processus afin de vérifier l'atteinte des objectifs fixés*

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

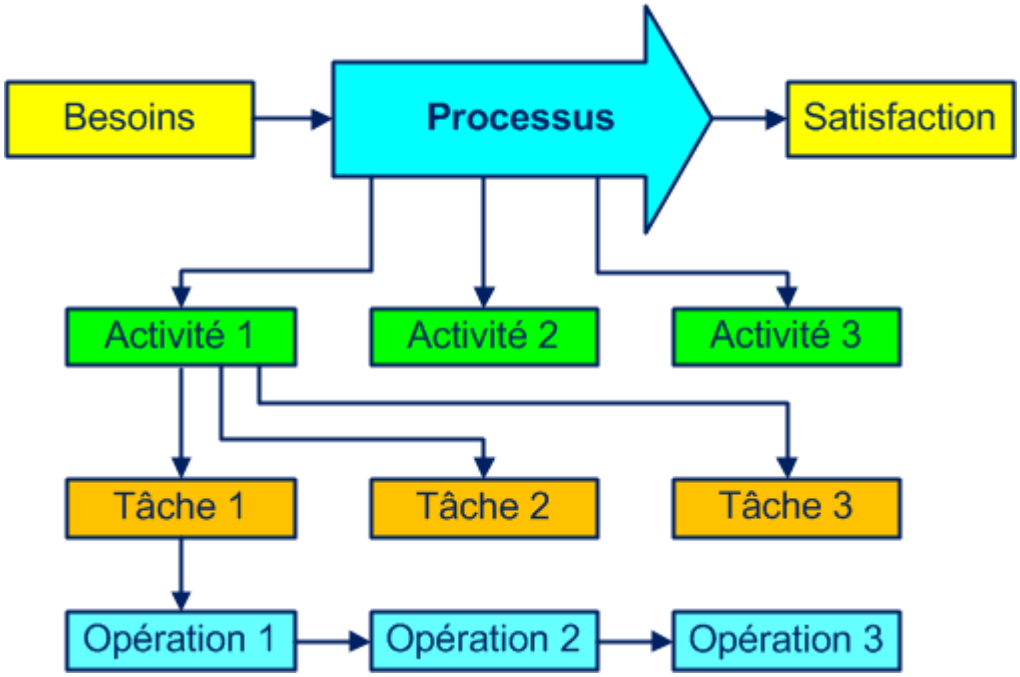


Figure 3-1. Les composantes d'un processus

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

- quelles matières, quelles informations documentées, quels outils ? (entrées)
- quel intitulé, quelle finalité, quelles activités, exigences, contraintes ? (processus)
- quels produits, quelles informations documentées ? (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)

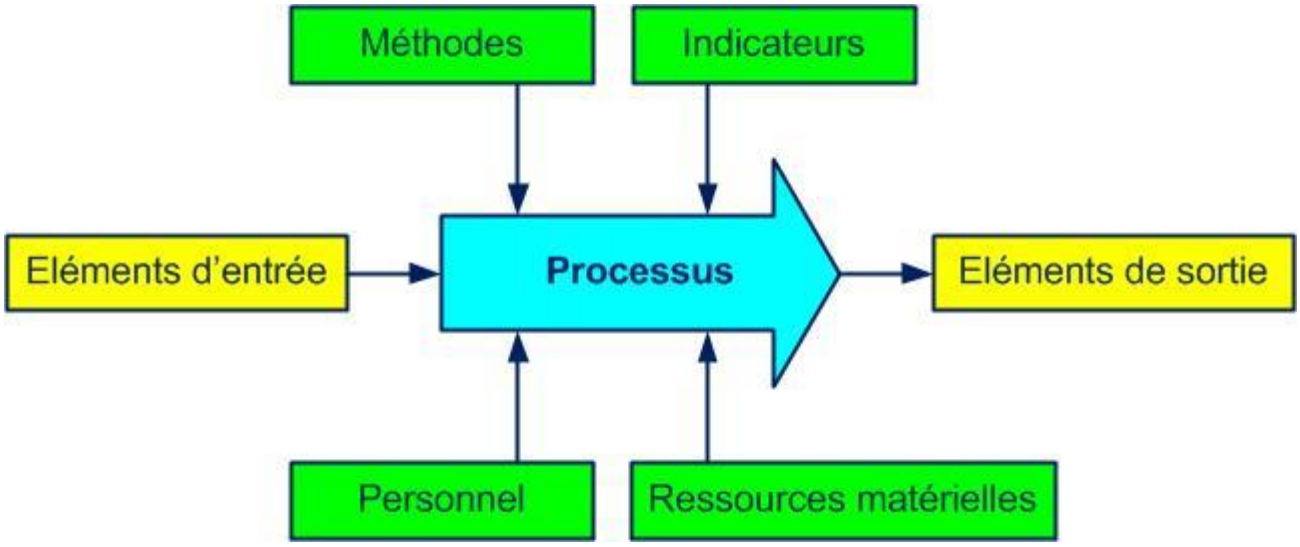


Figure 3-2. Certains éléments d'un processus

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

Vous pouvez trouver quelques exemples de fiches processus dans l'ensemble de documents E 02 et des exemples de processus dans l'annexe 03.

Toute organisation 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 aux exigences des clients).

Notre préférence pour déterminer 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'organisation ou de l'information documentée 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'organisation 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 (* obligatoires) :

- apprécier les risques*
- traiter les risques*
- communiquer*
- auditer*
- planifier le SMSI
- piloter les processus
- élaborer la stratégie
- développer la politique
- déployer les objectifs
- réaliser la revue de direction
- améliorer

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 (* obligatoires) :

- satisfaire aux exigences de la sécurité*
- maîtriser les processus externalisés*
- enregistrer et désinscrire*
- distribuer les accès*
- gérer l'authentification*
- développer et soutenir la sécurité*
- gérer la continuité de la sécurité*
- appliquer la sécurité*
- inspecter la sécurité*
- concevoir et développer
- acheter
- maintenir les équipements
- administrer les réseaux

- gérer les changements
- maîtriser les non-conformités
- 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 (* obligatoires) :

- appliquer la discipline*
- gérer le contrat de travail*
- tenir à jour la veille réglementaire
- acquérir et maintenir les infrastructures
- gérer les moyens d'inspection
- dispenser la formation
- fournir l'information
- gérer la documentation

3.2 Cartographie des processus

La cartographie des processus est par excellence un travail pluridisciplinaire. Ce n'est pas une exigence formelle de la norme ISO 27001 mais est toujours bienvenue.

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

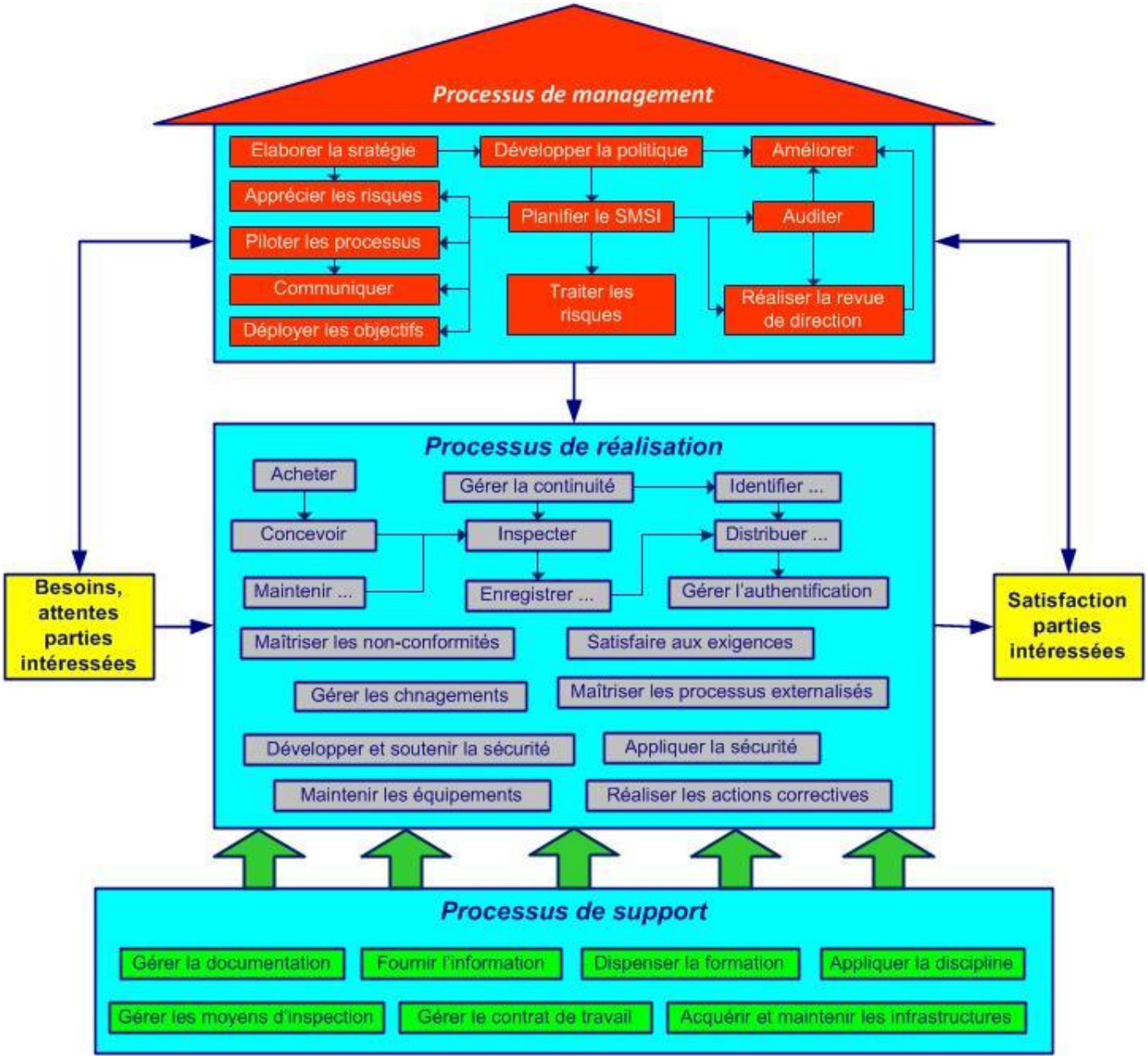


Figure 3-3. La maison des processus

Dans les éléments de sortie il ne faut pas sous-estimer les produits non voulus tels les déchets, nuisances, rejets.

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 des 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 SMSI peuvent entrer les processus : 

- élaborer la stratégie
- développer la politique
- apprécier les risques
- traiter les risques

- planifier le SMSI
- déployer les objectifs
- piloter les processus
- améliorer

Un exemple de processus Concevoir est montré en figure 3-4) :

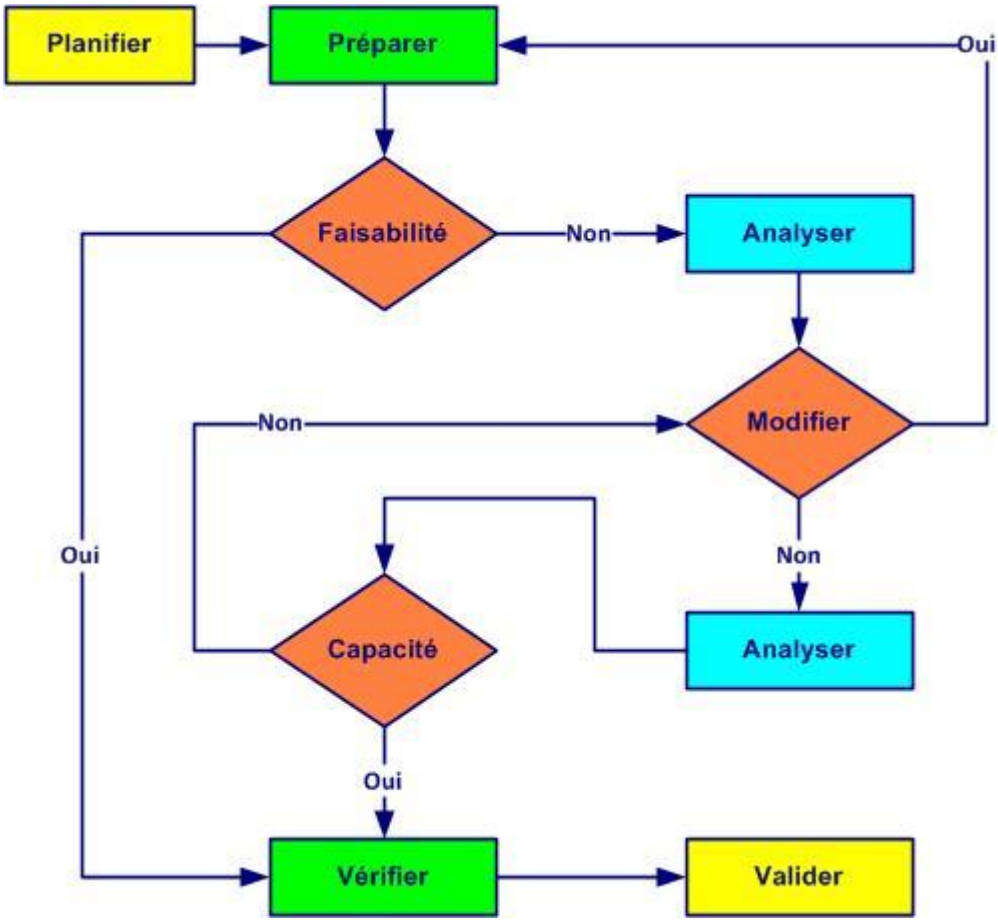


Figure 3-4. Un processus Concevoir

3.3 Approche processus

Les solutions simples pour maintenant, la perfection pour plus tard

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 contribue énormément à la gestion efficace de l'organisation (cf. annexe 04).

L'approche processus incluse au cours du développement, la mise en œuvre et l'amélioration continue d'un système de management de la sécurité de l'information permet d'atteindre les objectifs liés à la satisfaction des parties intéressées comme le montre la figure 3-5.

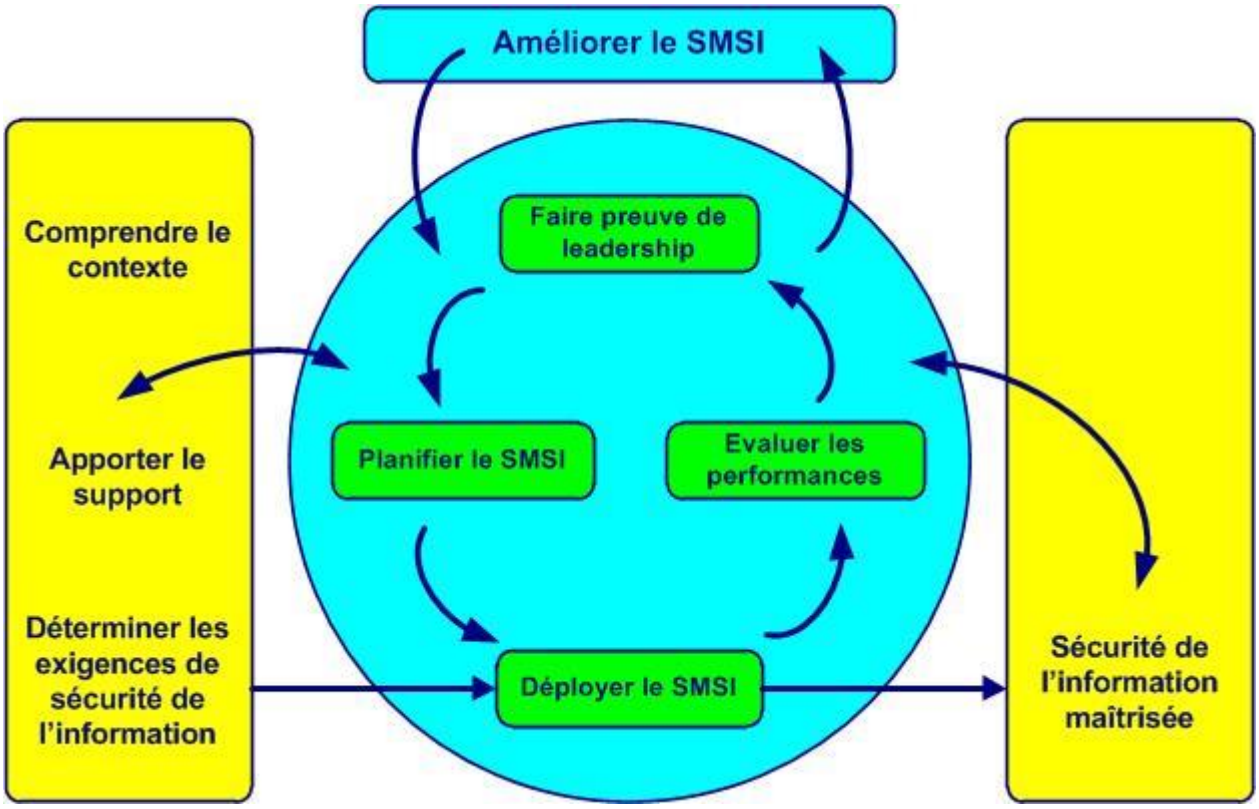


Figure 3-5. Modèle d'un SMSI basé sur l'approche processus et l'amélioration continue

L'approche processus :

- souligne l'importance :
  - de comprendre et de satisfaire aux exigences des parties intéressées
  - de la prévention pour réagir sur les éléments non voulus comme :
    - retours client
    - rebuts
  - de mesurer la performance, l'efficacité et l'efficience 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 continu
- permet :
  - de mieux visualiser les éléments 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'organisation et son contexte *(exigence 1)*

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

Intégrer les exigences du SMSI dans les processus métier permet de garantir aux parties intéressées (c'est-à-dire aux clients) une maîtrise des risques liés à la sécurité de l'information. Adopter ces exigences est une décision stratégique de la direction.

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

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

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. Enjeux externes et internes, cf. E 10v13.

Les analyses PESTEL et SWOT (nos forces et faiblesses, les opportunités et les menaces) peuvent être utiles pour une analyse pertinente du contexte de l'organisation (cf. annexe 05). L'analyse SWOT aide à comprendre notre environnement commercial. Elle nous permet également d'identifier les problèmes internes et externes, qui pourraient avoir un impact sur la sécurité de l'information.

Bonnes pratiques

- *le diagnostic du contexte comprend les principaux enjeux externes et internes*
- *les valeurs essentielles comme partie de la culture d'entreprise sont pris en compte dans le contexte de l'organisation*
- *les résultats de l'analyse du contexte sont largement diffusés*

- *l'analyse SWOT inclut beaucoup d'exemples pertinents*
- *l'analyse SWOT est un outil performant pour l'identification des principales menaces et opportunités*

Écarts à éviter

- *des enjeux du contexte de l'organisation comme l'environnement concurrentiel ne sont pas pris en compte*
- *dans certains cas la culture d'entreprise n'est pas prise en compte*
- *l'analyse des risques ne prend pas en compte les enjeux stratégiques*
- *manque de lien clair entre l'analyse SWOT et les actions entreprises*
- *la procédure domaine d'application du SMSI est classifiée comme confidentielle*

4.2 Besoins et attentes des parties intéressées *(exigences 2 à 3)*

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 intéressées il faut commencer par déterminer tous ceux qui peuvent être concernés par le système de management de la sécurité de l'information comme par exemple :

- salariés
- direction
- clients
- prestataires externes (fournisseurs, sous-traitants, consultants)
- propriétaires
- actionnaires
- banquiers
- distributeurs
- concurrents
- citoyens
- voisins
- organisations sociales et politiques

La liste des parties intéressées est réalisée par une équipe pluridisciplinaire. Chaque partie intéressée est identifiée par son niveau d'influence et de maîtrise. La priorité est donnée aux parties intéressées très influentes et faiblement maîtrisées. Liste des parties intéressées, cf. E 10v13.

Les exigences des parties intéressées qui changent avec le temps, sont revues régulièrement (cf. le processus Tenir à jour la veille réglementaire, annexe 03).

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 intéressées c'est :

- satisfaire aux exigences du SMSI
- se préparer à faire face aux menaces
- saisir des opportunités d'amélioration

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

Bonnes pratiques

- *la liste des parties intéressées est à jour*
- *les besoins et attentes des parties intéressées 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*
- *le délai de livraison n'est pas validé par le client*
- *les attentes des parties intéressées ne sont pas déterminées*
- *la liste des parties intéressées ne contient pas leur domaine d'activité*

4.3 Domaine d'application *(exigences 4 à 8)*

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 système de management de la sécurité de l'information est défini et validé par la direction.

La Déclaration d'applicabilité - DdA (cf. § 6.1.3 et annexe 07) permet :

- de déterminer ce qui fait partie ou ne fait pas partie du SMSI
- d'identifier et tenir à jour les mesures à appliquer
- de répondre pour chaque mesure aux questions :
  - qu'est-ce qui doit être fait ?
  - pourquoi ?
  - comment ?
  - quel est son statut ?
- de planifier et d'auditer le SMSI

Chaque mesure de la déclaration d'applicabilité est directement liée au traitement d'un risque.

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

- les enjeux (cf. § 4.1)
- les activités de l'organisation, y compris de support
- la culture d'entreprise
- l'environnement :
  - social
  - financier
  - technologique
  - économique
- les exigences des parties intéressées (cf. § 4.2)
- les processus externalisés

Le Domaine d'application du SMSI est disponible comme information documentée, cf. E 10v13.

Il inclut le domaine d'application (limites et interfaces) :

- de l'organisation :
  - produits
  - services
- de l'information et de la communication :
  - conception et développement de logiciels
  - maintenance
- physique :
  - siège social
  - filiales

Bonnes pratiques

- *le domaine d'application est pertinent et disponible sur simple demande*
- *les exigences non applicables sont justifiées par écrit*
- *le département non inclus dans le domaine d'activité est traité comme un fournisseur avec toutes les conséquences (contrat, accord de confidentialité, surveillance de la performance)*

Écarts à éviter

- *certains produits sont en dehors du domaine d'application du SMSI sans justification*
- *le domaine d'application est obsolète (la nouvelle filiale n'est pas incluse)*
- *le domaine d'application n'est pas validé par la direction*

4.4 Système de management de la sécurité de l'information *(exigence 9)*

Les exigences de la norme ISO 27001 sont liées à la maîtrise :

- de la sécurité de l'information et
- des processus de l'organisation

Pour cela :

- le système de management de la sécurité de l'information est :
  - planifié (cf. le processus Planifier le SMSI, annexe 03)
  - établi

    - documenté (un système documentaire simple et suffisant est mis en place)
    - mis en place et
    - amélioré en continu
- la politique de sécurité de l'information, les objectifs, les ressources et l'environnement de travail sont déterminés
- les menaces sont déterminées et les actions pour les réduire sont établies (cf. § 6.1)
- les processus essentiels nécessaires au SMSI sont maîtrisés (cf. le processus Piloter les processus, annexe 03)  :
    - 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 Informations documentées sur les processus est tenu à jour et conservé ()

Le manuel sécurité de l'information n'est pas une exigence de la norme ISO 27001 mais cela est toujours une possibilité de présenter l'organisation, son SMSI et ses procédures, politiques et processus (cf. annexe 08).

Le guide de l'ISO « *The integrated use of management system standards* » (L'utilisation intégrée des normes de systèmes de management) de 2018, en anglais, contient des recommandations pertinentes sur l'intégration des systèmes de management.

Pièges à éviter : 

- faire de la sur-qualité : 
    - une opération inutile est réalisée sans que cela ajoute de la valeur et sans que le client le demande – c'est un gaspillage, cf. les outils qualité E 12
- faire écrire toutes les procédures par le responsable sécurité de l'information : 
    - la sécurité de l'information est l'affaire de tous, « le personnel a conscience de la pertinence et de l'importance de chacun à la contribution aux objectifs de sécurité de l'information », 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 27001 sont montrées en figure 4-1 et sur la page dédiée :

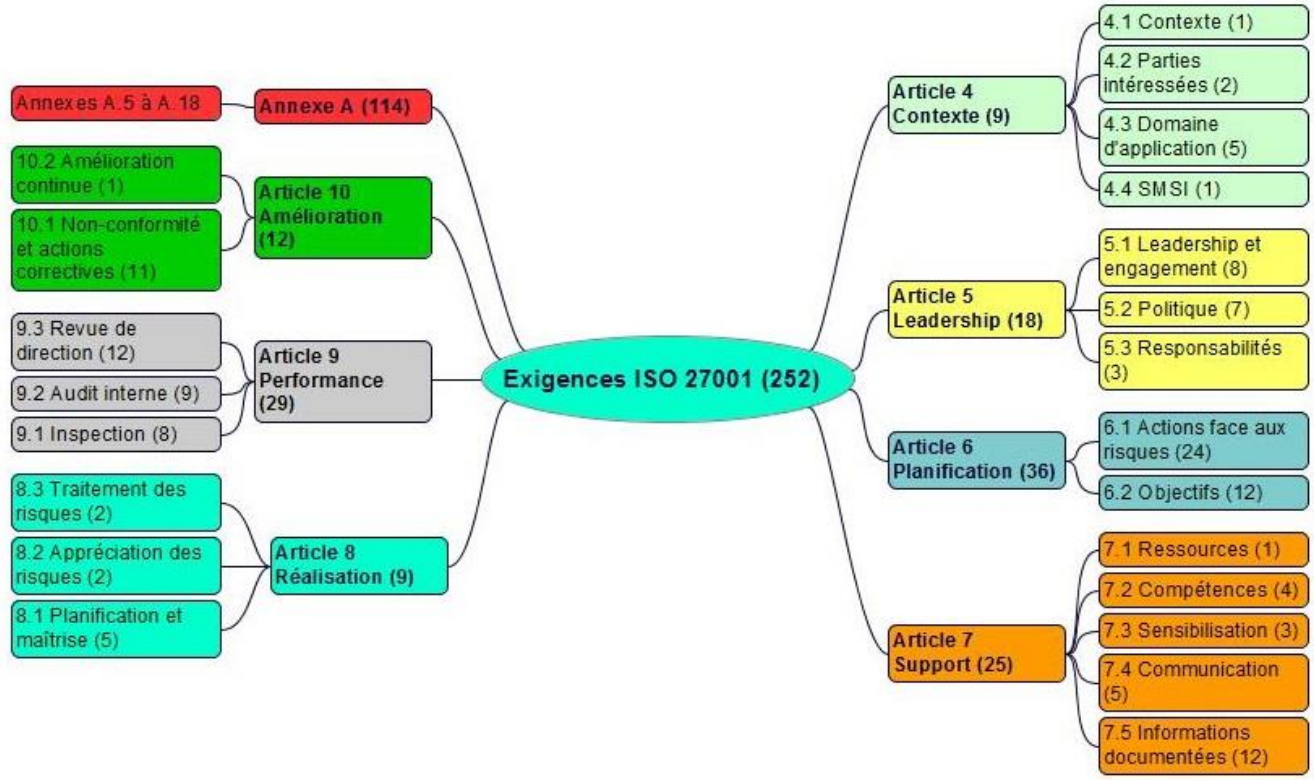


Figure 4-1. Les exigences de la norme ISO 27001 (2013)

Les exigences de sécurité de l'information concernent :

- les risques de l'organisation :
  - les menaces sur les actifs
  - la vulnérabilité et la vraisemblance d'apparition
  - les conséquences
- les exigences légales et contractuelles
- les principes, objectifs et obligations de maîtrise de l'information liés aux processus métier

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 SMSI*
- *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*
- *le potentiel innovation est confirmé par l'augmentation des ventes des nouveaux produits*

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 SMSI ne permettent pas d'atteindre les objectifs*
- *le SMSI n'est pas à jour (nouveaux processus non identifiés)*
- *les menaces et faiblesses identifiées dans l'analyse SWOT restent sans actions*