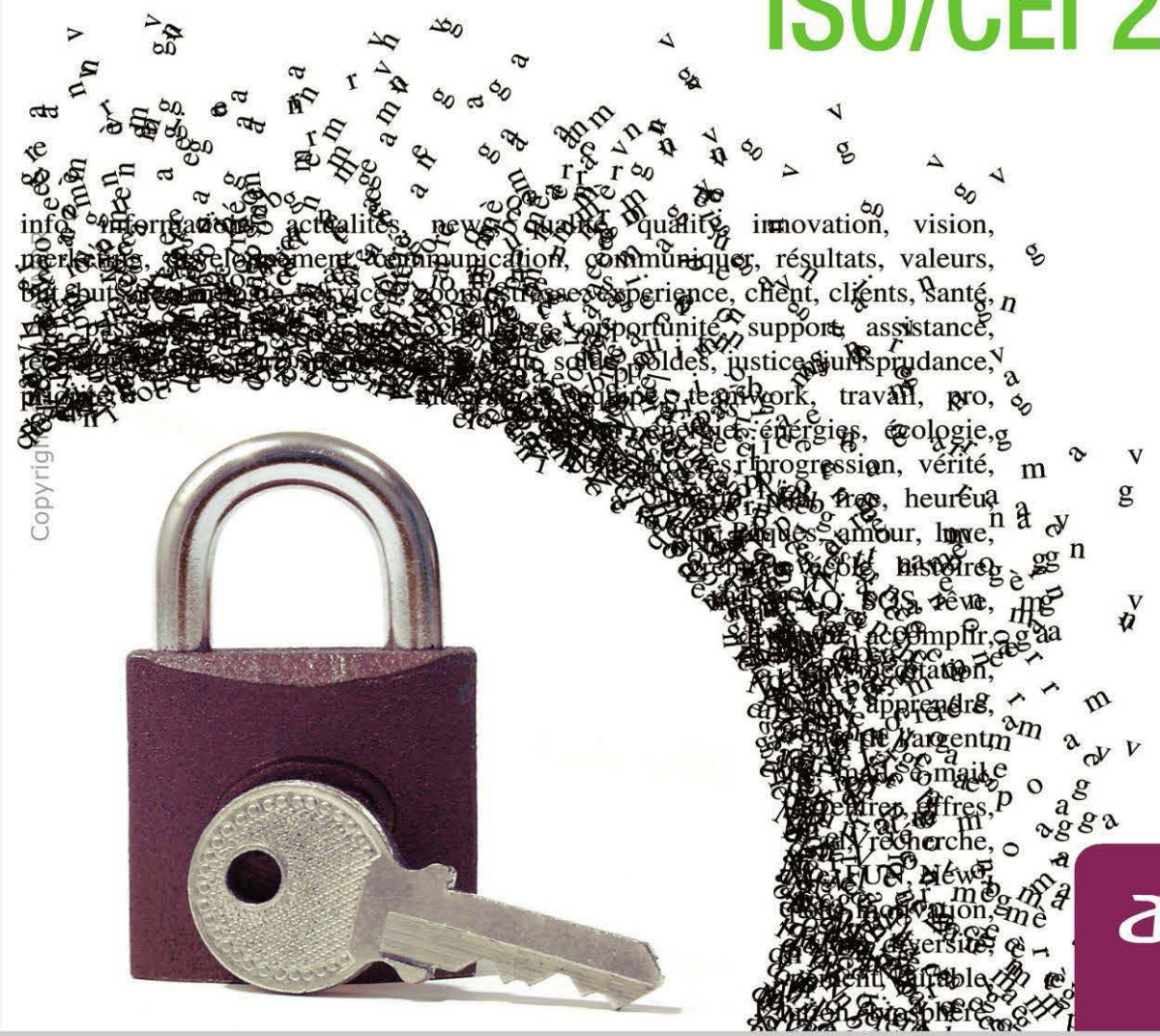
www.afnor.org/editions

Claude Pinet

10 clés pour la sécurité de l'information

ISO/CEI 27001

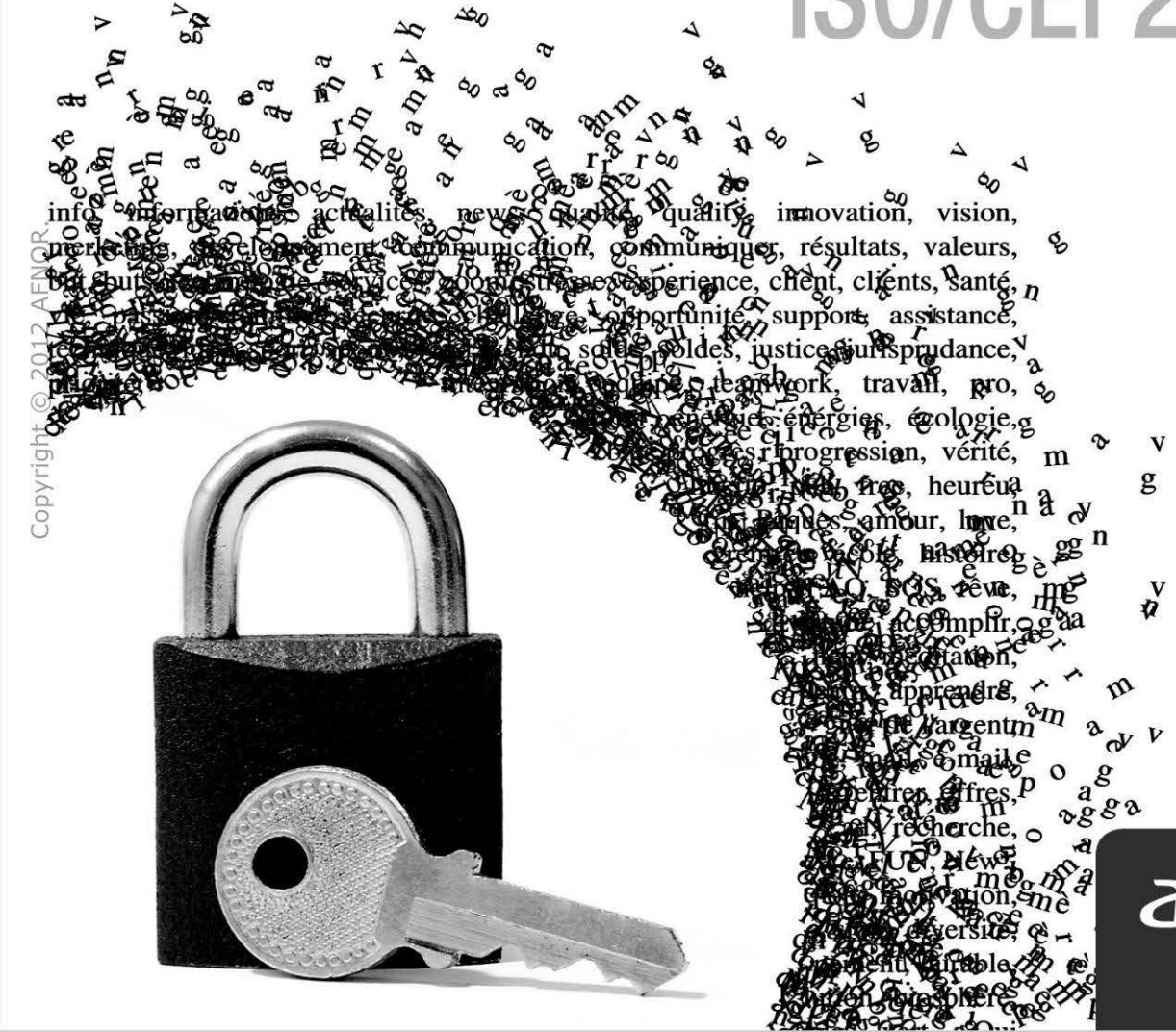


afnor ÉDITIONS

Claude Pinet

10 clés pour la sécurité de l'information

ISO/CEI 27001



afnor ÉDITIONS

Du même auteur chez AFNOR Éditions

Basic easy, Découverte de la qualité, 2010.

10 clés pour réussir sa certification ISO 9001 – Version 2008, 2009.

10 clés pour réussir sa certification QSE, ISO 9001, OHSAS 18001, ISO 14001, 2009.

10 clés pour la gestion des services, de l'ITIL à l'ISO 20000, 2007.

10 clés pour réussir sa certification IS0 9001, 2006.

Sous la direction de C. Pinet (Groupe des experts qualité du CNAM), *La Qualité du logiciel – Retour d'expériences*, 1998.

Couverture : création AFNOR Éditions – Crédit photo © 2012 Fotolia
ISBN 978-2-12-465381-2

AFNOR – 11, rue Francis de Pressensé, 93571 La Plaine Saint-Denis Cedex
Tél. : + 33 (0) 1 41 62 80 00 – www.afnor.org

Sommaire

Présentation de l'auteur

Claude Pinet[1], ingénieur **CNAM**, ingénieur européen (**EUR ING**®), est auditeur qualité certifié **IRCA**[2] sous le n° 1182803 depuis plus de quinze ans.

Ingénieur-conseil, il a accompagné de nombreux organismes ou entreprises de toute taille pour concevoir, formaliser et mettre en place leur système de management de la qualité et de systèmes de management des services. Ses nombreux retours d'expériences lui ont aussi permis d'assister des responsables qualité et les directions informatiques dans la mise en œuvre de méthodes et d'outils pour obtenir des améliorations efficientes.

Auditeur de certification NF EN ISO 9001, NF EN ISO 14001, NF ISO/CEI 20000-1, NF ISO/CEI 27000 pour le compte de plusieurs organismes de certification accrédité par le Comité français d'accréditation (COFRAC), il a audité de nombreux systèmes de management de la qualité et des systèmes de management des services. Il a recommandé l'obtention de certificats ISO dans des domaines d'activité économique diversifiés (de l'industrie, de l'administration publique, de la banque/assurance et d'entreprises de service).

À **AFNOR**, il participe aux groupes de travail internationaux qui contribuent à la rédaction, au vote et à l'évolution des normes ISO.

Ce capital d'expériences a permis à ce professionnel de la qualité des services et de la certification des systèmes d'information, de créer le cabinet **CPI Conseil**[3] qui est spécialisé dans la mise en œuvre des référentiels et des outils pour l'amélioration continue.

1 Adresse électronique : cpi.conseil@online.fr

2 International Register of Certificated Auditors : www.irca.org

3 http://cpi.conseil.free.fr

Avant-propos

Dans notre époque moderne, des techniques et des outils de plus en plus sophistiqués sont apparus et se sont développés. Il en résulte que notre environnement quotidien apparaît de plus en plus complexe et donc de plus en plus difficile à appréhender.

Toute activité humaine comporte intrinsèquement un certain nombre de risques. Avant d'entreprendre une action quelle qu'elle soit, il se pose la question de l'évaluation des conséquences que cette action est susceptible d'entraîner. Questionnement qui peut, dans certains cas, entraîner des blocages qui peuvent apparaître comme excessifs (principe de précaution).

En ce qui concerne une entreprise (ou tout organisme au sens plus général), les préoccupations sont du même ordre. Cette problématique décisionnelle choix/risque est applicable à tous les domaines : marketing, commerciaux, recherche et développement, production, logistique… Mais, compte tenu de sa nature immatérielle, c'est probablement dans le domaine de l'information que l'impact des décisions et des actions peut s'avérer le plus difficile à appréhender.

Une absence de maîtrise des risques inhérents à la sécurité de l'information peut entraîner des répercussions porteuses de très lourdes conséquences.

L'objectif de cet ouvrage est d'être utile :

- d'une part à tout intervenant dans les traitements de l'information, quel que soit son degré de responsabilité, afin d'améliorer la sécurité des activités ;
- d'autre part à tout utilisateur de l'information, afin d'améliorer la confiance dans les informations véhiculées.

La certification, si elle est recherchée, ne devant être considérée que comme un moyen et non une fin en soi.

Introduction

La notion de sécurité est une chose très vaste qui, en fonction du contexte ou des interlocuteurs concernés, recouvre des éléments bien différents.

Les hommes sont placés dans un environnement. Des interactions existent entre les individus que nous sommes et la nature (la terre, l'eau et l'air) qui nous entoure. Ces relations sont généralement régies par un certain équilibre. Mais l'équilibre peut être amené à basculer dans un sens ou dans l'autre. Parfois il peut être rompu brutalement, on parle alors de cataclysme naturel (tremblement de terre, inondation, éruption volcanique, tsunami, tornade, cyclone…). Parfois le phénomène est plus lent (tectonique des plaques, réchauffement climatique…).

L'équilibre peut aussi être mis en péril à la suite de l'activité humaine. Soit sournoisement (pollution, appauvrissement des sols, épuisement de ressources naturelles) ; soit brutalement, on parle alors d'accident (explosion, incendie, transport/circulation…).

Dans nos civilisations développées technologiquement, les sources de dangers réels ou potentiels sont accentuées du fait de l'utilisation de moyens (machines faites par la main de l'homme) qui, par exemple, augmentent la vitesse ou impactent un plus grand nombre de personnes. Le moindre accident, qu'il soit le résultat de phénomènes naturels ou le résultat de l'intervention humaine, peut entraîner des conséquences importantes. À tel point que c'est même développé un principe dit « de précaution » qui peut aller jusqu'à refuser des actions, par peur des conséquences.

De plus en plus, nous recherchons un besoin de sécurité qui rassure et donne la force d'agir. Sinon, c'est l'immobilisme et le refus d'avancer qui conduit à la mort.

Dans le domaine des technologies de l'information nous sommes dans le domaine de l'immatériel et du virtuel. Les objets manipulés étant invisibles, les dangers sont plus difficiles à appréhender. Par contre les conséquences sont bien réelles et souvent plus lourdes de conséquences que dans le monde réel. Les mesures de précaution à imaginer et à mettre en œuvre nécessitent un niveau d'abstraction important.

Pour répondre à ces besoins de « confiance », des méthodes et des normes sont apparues, gage de maturité. La démarche méthodologique proposée dans cet ouvrage contribue à cet objectif d'amélioration de la sécurité de l'information.

Le présent ouvrage comporte deux parties :

- La première partie développe les éléments clés qui permettent de comprendre les mécanismes de la norme internationale ISO/CEI 27001. Puis, de mettre en place dans votre organisation les réponses aux exigences de la norme et de son annexe A normative. Et ensuite d'aller jusqu'à la certification si tel est votre projet.
- La deuxième partie comporte 28 fiches techniques qui accompagnent la démarche méthodologique et sont autant d'outils pratiques pour une mise en œuvre efficace.

Partie I
Sécurité et information

Cette partie de l'ouvrage nous servira à positionner les principaux concepts relatifs à l'information et à la sécurité.

Ensuite, nous détaillerons les exigences contenues dans l'ensemble des normes ISO qui traitent de ce sujet, notamment la série 27000.

Enfin, nous dresserons l'inventaire des composantes du système de management de la sécurité de l'information (SMSI) que tout organisme candidat à la certification doit définir, mettre en œuvre et améliorer en permanence.

1
Clé n° 1 – La sécurité, qu'est-ce que c'est ?

Cette première clé ouvre la porte décrivant les concepts de la sécurité.

Le terme sécurité est employé pour s'appliquer à de nombreux domaines : civil, industriel, financier, transport, militaire, sanitaire, au travail, juridique… et informatique.

La sécurité correspond à une situation qui présente un minimum de risques. Donc, elle suscite un sentiment de confiance.

1.1 La définition de la sécurité

Ce mot vient du terme latin securitas, et signifie « sûr ». Le dictionnaire *Le Robert* en donne la définition suivante :

État d'esprit confiant et tranquille d'une personne qui se croit à l'abri du danger. Situation tranquille qui résulte de l'absence réelle de danger (absence d'accident).

Et un danger, c'est une menace qui pèse sur l'existence de quelqu'un ou de quelque chose. Les conséquences de cette menace pourront avoir des impacts plus ou moins importants. En cas extrême, ces conséquences peuvent entraîner des dommages irrémédiables pouvant aller jusqu'à la mort.

Le fascicule de documentation FD X 50-252 nous donne la définition suivante pour le danger :

> **C'est une substance, un objet, une situation ou un phénomène pouvant être à l'origine d'un dommage ou d'un préjudice.**

Exemples de dangers : produit toxique, virus, inondation, incendie…

Dans toute activité humaine, personnelle ou professionnelle, il existe une multitude de dangers qui planent sur le cours du temps. Ces dangers représentent un risque d'altération de notre sécurité. Afin de contrer le sentiment d'insécurité qui va en résulter, il nous appartient de prendre conscience de ces dangers, d'en identifier les faits générateurs et de trouver des remèdes efficaces pour les contrer.

Les solutions de type « parades » (ou mesures de sécurité) doivent nous permettre d'en réduire les effets, voire d'en éliminer les causes.

Nous pourrons remarquer qu'en matière de sécurité de nombreux rapprochements peuvent être faits avec le domaine de la qualité. Les problématiques sont complexes. Les solutions à mettre en œuvre sont souvent de nature transverse. Il est aussi possible de faire une distinction entre la qualité/sécurité réelle et la qualité/sécurité perçue.

1.2 Les acteurs de la sécurité

La sécurité se situe dans un environnement qui correspond à un échange entre deux ou plusieurs acteurs. La norme les appelle « les parties prenantes ».

Nous proposons de nous reporter aux deux définitions normées ci-dessous :

Les parties intéressées, selon la norme ISO 9000:2005 – *Vocabulaire et définitions* :

> **C'est une personne ou un groupe de personnes (ou un autre organisme) ayant un intérêt dans le fonctionnement ou le succès d'un organisme.**

Exemples de parties prenantes : les clients, propriétaires, personnes d'un organisme, fournisseurs, banques, syndicats, partenaires ou société.

Les parties intéressées selon la norme ISO 14001:2004 – *Système de management environnemental* :

> **C'est un individu ou un groupe concerné ou affecté par la performance environnementale d'un organisme.**

Par ailleurs, la norme NF EN ISO 9001 nous donne la définition d'un **organisme** :

> **C'est un ensemble (généralement structuré) d'installations et de personnes avec des responsabilités, pouvoirs et relations.**

Un organisme peut être public ou privé (compagnie, société, firme, entreprise, institution, œuvre de bienfaisance, travailleur indépendant, association, ou parties ou combinaison de ceux-ci).

1.3 Les composantes de la sécurité

Pour décrire la sécurité, deux aspects sont souvent utilisés :

- La sécurité passive : cette notion fait appel au domaine de la prévention (actions préventives). Son rôle consiste à réduire les facteurs de survenance ou de déclenchement de l'accident.
- La sécurité active : cette notion fait appel au domaine de la résolution (actions correctives). Son rôle consiste à déployer des mesures de protection à l'encontre des conséquences dommageables lorsque l'accident survient.

1.4 Monsieur Sécurité

Pour définir, mettre en œuvre et suivre la démarche sécurité au sein de l'entreprise, il importe de désigner un « monsieur Sécurité[4] ». Un peu comme le « monsieur Qualité », représentant de la direction, exigé par la norme NF EN ISO 9001, ce monsieur Sécurité est investi par la direction de la responsabilité de la gestion de la sécurité de l'information.

4 En anglais, cette fonction est appelée *risk manager*. Une description sommaire de la fonction est donnée dans la fiche technique n° 24.

Les objectifs de monsieur Sécurité sont à la fois stratégiques et opérationnels. Il doit notamment :

- participer à la définition de la politique et les objectifs de sécurité ;
- établir un plan de gestion des risques ;
- obtenir de la direction les ressources nécessaires ;
- établir le système de management de la sécurité de l'information ;
- développer les outils permettant de suivre, et de tracer l'activité ;
- entretenir un esprit de gestion des risques ;
- mettre en place un suivi.

Comme monsieur Qualité, monsieur Sécurité doit être rattaché hiérarchiquement à la direction générale qui lui donne autorité et à laquelle il doit rendre compte de sa mission.

Pour réussir, monsieur Sécurité devra faire preuve de sérieuses capacités de communication. D'abord en interne pour faire prospérer la notion de sécurité. Ensuite, à l'extérieur avec les fournisseurs pour leur faire adopter le même état d'esprit.

Il devra aussi gérer tous les processus :

- d'évaluation et de gestion des risques ;
- de gestion de surveillance et de contrôle du SMSI ;
- de réponse aux incidents de sécurité.

Il devra être capable d'anticiper et de fournir des recommandations adaptées.

Concevoir, déployer, gérer, maîtriser, dialoguer, anticiper, évoluer, former, communiquer… telles sont les qualités requises pour réussir la mission d'un « monsieur Sécurité ».

2
Clé n°2 – L'information, qu'est-ce que c'est ?

Cette deuxième clé ouvre la porte décrivant les concepts de l'information.

Il est souhaitable de faire une distinction de sémantique entre les deux mots « information » et « donnée ». En effet, ces deux mots ne recouvrent pas les mêmes concepts.

2.1 La définition de l'information

Le terme information vient du latin *informare* qui signifie mettre en forme. En fait le même mot désigne à la fois le message (communication, média) et les symboles codés (signes, alphabet) qui sont contenus dans le message. La notion d'information est étroitement liée à la relation des individus que nous sommes avec notre environnement. Ces messages, échangés sous la forme de signaux, sont véhiculés à notre niveau par nos cinq sens (vision, toucher, ouïe, goût, odorat). Dans notre civilisation technologique, les moyens de communication biologiques sont prolongés par des outils qui en accélèrent la vitesse de transmission et réduisent les limites espace/temps. Il en résulte que toute perturbation (distorsion, déformation, incomplète, perte) de la qualité et de la sécurité de cette information peut avoir de lourdes conséquences sur nos relations, donc sur notre vie. Au regard de la sécurité, il importera donc de prendre en compte ces deux aspects de l'information et d'intervenir à la fois :

- sur le message et sa transmission ;
- sur le contenu du message.

2.2 La définition de la donnée

Le terme « donnée » correspond à une représentation de l'information selon des règles codées, généralement pour en faire le traitement.

La norme ISO/CEI 2382-1:1993 nous donne la définition suivante :

> **Représentation ré interprétable d'une information sous une forme conventionnelle convenant à la communication, à l'interprétation ou au traitement.**

Les données sont conservées sur différents types de supports (papier, magnétique, numérique).

Pour transmettre un message, il faut le coder. Le code utilisé est dépendant de la nature du canal de transmission.

Par exemple :

- l'écriture ;
- la parole ;
- le code morse ;
- le code binaire ;
- …

Dans le domaine des systèmes de traitement de l'information, les données sont gérées séparément des traitements.

2.3 Le traitement de l'information

Le traitement de l'information constitue une part importante de l'activité humaine. Il est aussi ancien que l'homme lui-même.

Pour communiquer entre eux, les hommes utilisent essentiellement le langage parlé ou écrit. Tous les messages échangés comportent :

- un contenu sémantique qui décrit les idées à transmettre ;
- des règles de structure linguistiques qui portent sur :
- un dictionnaire (définition des mots) ;
- une grammaire (règles de conjugaison, d'accord…).

Ainsi, deux messages décrivant les mêmes idées, mais rédigés l'un en français et l'autre en chinois, seront considérés comme deux messages totalement distincts.

De façon plus générale, le traitement de l'information s'intéresse aux règles permettant de combiner entre eux les différents éléments d'information.

2.4 Le traitement automatisé de l'information

La collecte, le traitement, la diffusion et la conservation de l'information peuvent utiliser des moyens technologiques modernes pour en généraliser l'utilisation, accélérer les processus et réduire les coûts de fonctionnement.

Ainsi, la mécanisation – grâce aux machines développées par l'homme –, puis l'automatisation – grâce aux outils électroniques –, a permis d'amplifier le rôle et l'importance du traitement de l'information. Décupler la puissance des moyens permet à l'homme de concentrer son attention sur les aspects méthodologiques et sur le développement des connaissances. L'informatique change de dimension pour devenir « les technologies de l'information » (*information technologies*) et se développe dans tous les secteurs d'activités économiques (gestion, industrie, médecine, enseignement…).

3
Clé n° 3 – Structure des normes ISO 27000

Cette troisième clé ouvre la porte découvrant le contenu de la famille ISO/IEC 27000.

La famille des normes ISO/IEC 27000 comprend plusieurs documents normatifs. Tous ne servent pas de référence pour une certification. Toutefois, nous en listons l'ensemble afin de disposer d'une large vision des documents consultables pour y trouver de nombreuses bonnes pratiques.

Un premier document traitait des techniques de sécurité, l'ISO/IEC 17799:2005, *Information technology –Security techniques – Code of practice for information security management*. Ces recommandations de mise en œuvre sont reprises dans l'annexe A, normative, de la norme NF ISO/CEI 27001.

3.1 Structure normative

Cette série de normes appartient à la catégorie des « Technologies de l'information » dans la partie « Techniques de sécurité ».

Elle comporte les documents suivants :

- NF ISO/CEI 27000 (publiée en février 2011) *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*.
- NF ISO/CEI 27001 (publiée en décembre 2007) *Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences*.
- ISO/CEI 27002:2005 (publiée en juin 2005) *Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de sécurité de l'information (ISO/CEI 17799:2005 et rectificatif 1 de 2007)*.
- ISO/CEI 27003:2010 (publiée en février 2010) *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information*.
- ISO/CEI 27004:2009 (publiée en décembre 2009) *Technologies de l'information – Techniques de sécurité – Management de la sécurité de l'information – Mesurage*.
- NF ISO/CEI 27005 (publiée en juin 2011) *Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.
- ISO/CEI 27006:2011 (publiée en mars 2007 et un projet de nouvelle norme en septembre 2011) *Technologies de l'information – Techniques de sécurité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*.
- ISO/CEI 27011:2008 (publiée en décembre 2008) – *Technologies de l'information – Techniques de sécurité – Lignes directrices pour le management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002*.

À ces normes sécurité de l'information, il faut ajouter la norme ISO 19011 – *Lignes directrices pour l'audit des systèmes de management* – dont la dernière version date de 2011 (version française NF ISO 19011, janvier 2012, indice de classement X50-136). Cette norme définit les exigences pour l'audit des systèmes de management quels qu'ils soient. Cette norme sert de cadre de référence pour les audits de certification et défini les exigences relatives aux compétences des auditeurs de certification.

La figure 3.1 donne une image du positionnement des documents ISO.

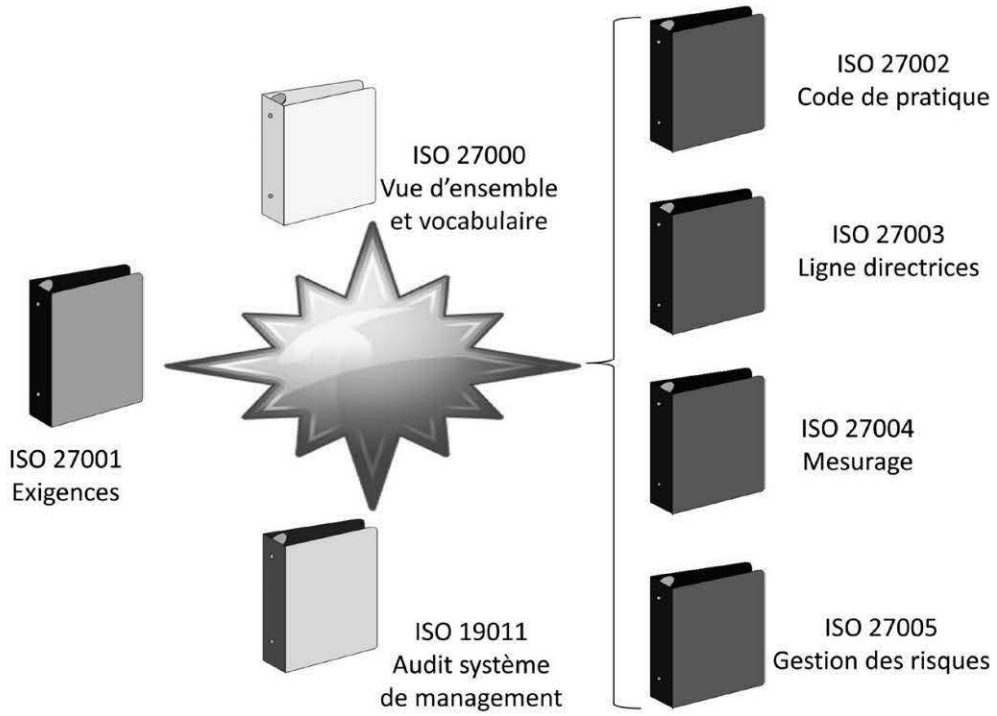


Figure 3.1 La ligne de produits normatifs ISO

3.2 NF ISO/CEI 27000

Cette norme qui a pour titre *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité des informations – Vue d'ensemble et vocabulaire* a été publiée par l'ISO en mai 2009 avec le statut de norme internationale.

Elle a été reprise à l'identique par AFNOR sous le même titre en tant que NF ISO/CEI 27000 et publiée en février 2011 (indice de classement Z74-220).

Le paragraphe 2 de cette norme détaille les termes et définitions. Dans cet ouvrage, nous faisons référence à nombre de ces définitions normées.

Le paragraphe 3 de cette norme décrit :

- les composantes d'un système de management de la sécurité de l'information (SMSI) ;
- les raisons de l'importance d'un SMSI ;
- l'établissement, la surveillance, la mise à jour et l'amélioration d'un SMSI.

Le paragraphe 4 de cette norme décrit la famille de normes et les relations entre elles. Enfin, dans son annexe A (informative), cette norme précise le degré d'interprétation à prendre en compte dans les expressions verbales utilisées :

- **Exigence** : qui doit être strictement respecté ; ce qui est permis (doit) ou interdit (ne doit pas) pour être conforme.
- **Recommandation** : qui n'est pas exigé mais souhaitable (il convient/ne convient pas de…).
- **Permission** : qui est une conduite à tenir (peut/n'a pas besoin).
- **Possibilité** : qui a une possibilité d'apparition (peut/ne peut pas).

3.3 NF ISO/CEI 27001

Cette norme intitulée *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité des informations – Exigences* a été publiée par l'ISO en octobre 2005 avec le statut de norme internationale.

Elle a été reprise à l'identique par AFNOR sous le même titre en tant que NF ISO/CEI 27001 et publiée en décembre 2007 (indice de classement Z74-221).

Le contenu de cette norme décrit (thèmes repris et détaillés dans la clé n° 4) :

- le domaine d'application ;
- les références normatives ;
- le rappel des termes et définitions ;
- le SMSI ;
- la responsabilité de la direction ;
- les audits internes du SMSI ;
- la revue de direction du SMSI ;
- l'amélioration du SMSI.

Cette norme comporte trois annexes :

- Annexe A (normative), très importante et qui décrit les objectifs et les mesures de sécurité.

- Annexe B (informative), qui reprend les principes de l'OCDE :
  - Sensibilisation
  - Responsabilité
  - Réaction
  - Évaluation des risques
  - Conception et mise en œuvre de la sécurité
  - Gestion de la sécurité
  - Réévaluation
  - Annexe C (informative), qui indique les correspondances par rapport à l'ISO 9001 (qualité) et l'ISO 14001 (environnement).

3.4 ISO/CEI 27002:2005

Cette norme qui a pour titre *Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de la sécurité de l'information* a été publiée par l'ISO en juin 2005 avec le statut de norme internationale.

Un document rectificatif n° 1 a été publié en 2007. Ce rectificatif technique concerne le remplacement, par renumérotation dans tout le texte de la norme, du numéro de code 17799 par le numéro de code 27002.

En effet, cette norme ISO/CEI 27002:2005 reprend le texte d'une ancienne norme 17799 publiée en 2000, qui décrivait des mesures et des facteurs cruciaux de réussite pour la sécurité de l'information pouvant être appliqués à la plupart des organismes.

Dans chacune des rubriques principales de sécurité, cette norme décrit :

- un objectif de sécurité avec un but à atteindre ;
- une ou plusieurs mesures pouvant être appliquées pour atteindre l'objectif de sécurité.

Pour chaque mesure la description :

- spécifie la mesure adaptée à l'objectif de sécurité ;
- propose des préconisations détaillées de mise en œuvre ;
- présente des compléments d'information ou des références à d'autres normes.

Les principaux thèmes traités dans cette norme concernent :

- Appréciation et traitement du risque.
- Politique de sécurité.
- Organisation de la sécurité de l'information.
- Gestion des biens.
- Sécurité liée aux ressources humaines.
- Sécurité physique et environnementale.
- Gestion de l'exploitation et des télécommunications.
- Contrôle d'accès.
- Acquisition, développement et maintenance des systèmes d'information.
- Gestion des incidents liés à la sécurité de l'information.
- Gestion du plan de continuité de l'activité.
- Conformité.

3.5 ISO/CEI 27003:2010

Cette norme intitulée *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information* a été publiée par l'ISO en février 2010 avec le statut de norme internationale. Cette norme décrit :

- les phases d'un projet de mise en œuvre ;
- l'approbation de la direction pour le lancement d'un projet ;
- la définition du champ du projet, de ses limites et de sa politique ;
- la conduite de l'analyse des exigences de sécurité de l'information ;
- la conduite de l'évaluation du risque et du plan de traitement des risques ;
- la conception du système de management de la sécurité de l'information (SMSI).

Cette norme comporte cinq annexes :

- Annexe A (informative) : *Liste type d'activités.*
- Annexe B (informative) : *Les rôles et responsabilités.*

- Annexe C (informative) : *Des informations pour les audits internes.*
- Annexe D (informative) : *Des informations sur les politiques.*
- Annexe E (informative) : *Le pilotage et la mesure.*

3.6 ISO/CEI 27004:2009

Cette norme qui a pour titre *Technologies de l'information – Techniques de sécurité – Management de la sécurité de l'information – Mesurage* a été publiée par l'ISO en décembre 2009 avec le statut de norme internationale.

Cette norme décrit :

- les objectifs de la mesure de la sécurité de l'information (efficacité, performance) ;
- le programme de mesurage selon le cycle du PDCA avec :
  - les entrées du cycle ;
  - les sorties du cycle.
  - les facteurs de succès ;
  - le modèle de mesurage avec :
  - attributs ;
  - méthode ;
  - indicateurs ;
  - résultats ;
  - critères de décision.
- la gestion des responsabilités notamment en matière de :
  - formations ;
  - connaissances ;
  - compétences.
  - mise en œuvre des mesures et du mesurage ;
  - production du mesurage ;
  - analyse des données et des résultats ;
  - évaluation et amélioration du programme de mesurage.

Cette norme comporte deux annexes :

- Annexe A (informative) : Modèle de mesurage de sécurité de l'information.
- Annexe B (informative) : Exemples de construction de mesurage.

3.7 NF ISO/CEI 27005

Cette norme intitulée *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information nouvelle version* a été publiée par l'ISO en juin 2011 avec le statut de norme internationale.

La version précédente a été reprise à l'identique par AFNOR sous le même titre en tant que NF ISO/CEI 27005 et publiée en novembre 2010 (indice de classement Z74-225).

Cette norme présente le processus général de gestion des risques en sécurité de l'information.

Le document décrit tout d'abord les critères d'évaluation des risques. Le processus d'analyse des risques comprend :

- l'identification des actifs ;
- l'identification des menaces ;
- l'identification des mesures de sécurité ;
- l'identification des vulnérabilités ;
- l'identification des conséquences.

Puis, le processus d'appréciation des risques comprend :

- l'appréciation des impacts ;
- la prise en compte des conséquences ;
- la vraisemblance des scénarios d'incident ;
- l'estimation du niveau de risque.

Ensuite, l'évaluation du risque permet de comparer le niveau des risques aux critères d'évaluation des risques et aux critères d'acceptation des risques.

Le processus de traitement des risques consiste à choisir des mesures de sécurité pour réduire, maintenir, éviter ou transférer les risques et définir un plan de traitement des risques.

Après, il convient de prendre la décision d'accepter les risques et les responsabilités de cette décision. Alors, les informations relatives aux risques doivent être communiquées afin de partager ces informations avec les autres parties prenantes.

Pour permettre l'amélioration de la gestion des risques, des activités de surveillance et de revue des facteurs de risques doivent être mises en place.

3.8 ISO/CEI 27011:2008

Cette norme intitulée *Technologies de l'information – Techniques de sécurité – Lignes directrices pour le management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002* a été publiée par l'ISO en décembre 2008 avec le statut de norme internationale.

Cette norme est orientée métier. Elle décrit :

- les conditions de sécurité en télécommunications ;
- la politique sécurité ;
- l'organisation de la sécurité de l'information ;
- la gestion des actifs (biens) ;
- la sécurité des ressources humaines ;
- la sécurité physique et environnementale ;
- la gestion de l'exploitation et des communications ;
- le contrôle des accès ;
- l'acquisition, le développement et la maintenance des systèmes d'information ;
- la gestion des incidents de sécurité ;
- la gestion de la continuité de l'activité ;
- la conformité.

Cette norme comporte deux annexes :

- Annexe A (qui représente une partie intégrante des recommandations de la norme) : *Ensemble de contrôles étendus aux communications.*
- Annexe B (qui ne représente pas une partie intégrante des recommandations de la norme) : *Guide d'implémentation complémentaire.*

4
Clé n° 4 – Exigences de la norme NF ISO 27001

Cette quatrième clé ouvre la porte découvrant le contenu de l'ISO/IEC 27001. Cette norme constitue le référentiel pour la certification.

La norme NF ISO/IEC 27001 est une norme d'exigences. Elle constitue le référentiel pour l'élaboration et la certification d'un système de management de la sécurité de l'information (SMSI).

Cette norme est alignée sur les référentiels NF ISO 9001 (qualité) et NF ISO 14001 (environnement) ou ISO/CEI 20000 (prestations de services technologies de l'information). Aussi, lorsque c'est opportun, il est recommandé de réaliser des économies d'échelles en procédant à une certification multiple. Par exemple 9001-27001 ou 20000-27001.

4.1 L'organisation de la norme

Comme toutes les normes ISO, cette norme comporte deux premiers paragraphes relatifs au domaine d'application et aux références normatives.

Ensuite, dans le paragraphe 3 sont données des définitions précises de vocabulaire qui permettent de lever toute ambiguïté sur les termes utilisés.

Le lecteur pourra se reporter à la fiche technique n° 1 pour retrouver les principaux éléments de vocabulaire et leurs définitions normées.

Les paragraphes suivants sont consacrés aux exigences applicables à un système de management de la sécurité de l'information (SMSI).

- Le paragraphe 4 – *Le SMSI*.
- Le paragraphe 5 – *Responsabilité de la direction*.
- Le paragraphe 6 – *Audits internes du SMSI*.
- Le paragraphe 7 – *Revue de direction du SMSI*.
- Le paragraphe 8 – *Amélioration du SMSI*.

Pour obtenir une certification, aucune exclusion n'est autorisée sur l'ensemble de ces paragraphes. Toutes les exigences de la norme doivent être satisfaites par l'organisme candidat à la certification.

La fiche technique n° 2 présente le sommaire de la norme NF ISO/CEI 27001.

4.2 Le SMSI (§ 4 de la norme)

Les articles de ce paragraphe dressent l'inventaire des exigences normatives à satisfaire pour une certification d'un système de management de la sécurité de l'information (SMSI).

La norme NF ISO/CEI 27001 nous donne la définition suivante du SMSI :

> **Partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information.**

On remarquera que les processus exigés pour le SMSI doivent respecter le principe du modèle PDCA. À savoir :

- Établissement du SMSI (*Plan*), avec les processus d'appréciation des risques, d'élaboration du plan de traitement des risques et d'acceptation des risques.
- Mise en œuvre et fonctionnement du SMSI (*Do*), avec le processus de gestion du plan de traitement des risques.
- Surveillance et réexamen du SMSI (*Check*), avec le processus de revue des risques.
- Mise à jour et amélioration du SMSI (*Act*), avec amélioration du processus de gestion des risques en sécurité de l'information.

La figure 4.2 résume graphiquement les processus du SMSI.

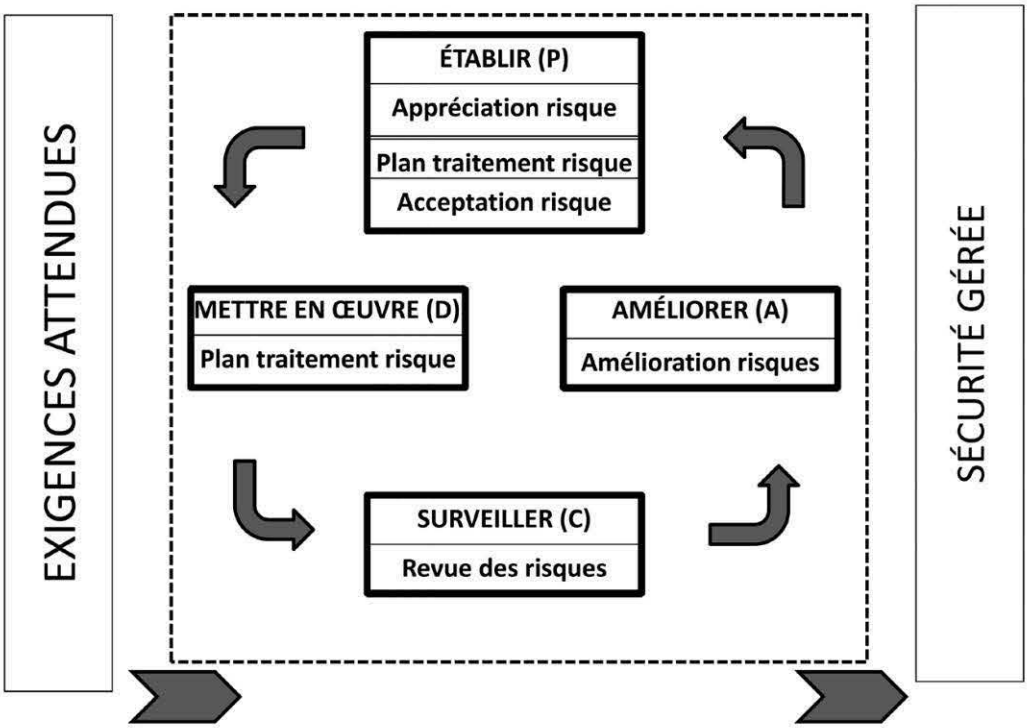


Figure 4.1 Cartographie des processus de la norme NF ISO/IEC 27001

4.2.1 Établir le SMSI

Dans le cadre de cette phase d'établissement du SMSI, l'organisme doit effectuer un certain nombre de travaux :

- définir le domaine d'application (*cf.* fiche technique n° 3) ;
- définir la politique sécurité ;
- définir l'approche d'appréciation du risque ;
- identifier les risques ;
- analyser et évaluer les risques ;
- identifier et évaluer les choix de traitement des risques ;
- sélectionner les objectifs de sécurité ;
- faire approuver par la direction les risques résiduels ;
- préparer la déclaration d'applicabilité (DdA). Les principaux thèmes de la DdA sont exposés dans la fiche technique n° 4 et dans le chapitre « Clé n° 5 »).

4.2.2 Mettre en œuvre le SMSI

Dans le cadre de cette phase de mise en œuvre du SMSI, l'organisme doit effectuer un certain nombre de travaux :

- élaborer un plan de traitement du risque ;
- mettre en œuvre le plan de traitement du risque ;
- mettre en œuvre les mesures de sécurité ;
- définir la méthode d'évaluation de l'efficacité des mesures ;
- mettre en œuvre des programmes de formation et sensibilisation ;
- gérer les opérations du SMSI ;
- gérer les ressources ;
- mettre en œuvre les procédures.

4.2.3 Surveiller le SMSI

Dans le cadre de cette phase de surveillance du SMSI, l'organisme doit effectuer un certain nombre de travaux :

- exécuter les procédures de surveillance ;
- exécuter les procédures de réexamen ;
- réaliser les réexamens réguliers de l'efficacité du SMSI ;
- évaluer l'efficacité des mesures ;
- réexaminer les appréciations des risques ;
- mener des audits internes ;
- effectuer une revue de direction périodique ;
- mettre à jour les plans de sécurité ;
- consigner les événements et les actions.

4.2.4 Améliorer le SMSI

Dans le cadre de cette phase d'amélioration du SMSI, l'organisme doit effectuer un certain nombre de travaux :

- mettre en œuvre les améliorations identifiées ;
- entreprendre les actions correctives et préventives ;
- informer les parties prenantes ;
- s'assurer que les améliorations permettent d'atteindre les objectifs.

4.3 La responsabilité de la direction (§ 5 de la norme)

La direction de l'organisme doit être particulièrement impliquée. Cette implication s'exprime dans :

- la formulation de la politique sécurité ;
- la détermination des objectifs de sécurité ;
- la définition des rôles et responsabilités ;
- la fourniture et la mobilisation des ressources nécessaires au bon fonctionnement du SMSI ;
- l'assurance que les audits internes sont menés ;
- la réalisation des revues de direction.

Les ressources humaines sont un élément important. Elles doivent faire l'objet d'une attention toute particulière afin de garantir l'efficacité des activités liées à la sécurité de l'information. Les compétences doivent être soigneusement sélectionnées. Elles doivent assurer le soutien des procédures de sécurité de l'information et des exigences métier. L'objectif étant de maintenir une sécurité adéquate par une application correcte de toutes les mesures mises en œuvre.

La direction de l'organisme doit aussi s'assurer que le personnel ayant des responsabilités dans le SMSI a les compétences nécessaires pour exécuter les tâches de fonctionnement. L'inventaire des compétences du personnel fait apparaître des lacunes ou besoins de montée en compétence. Pour satisfaire à ces besoins deux catégories d'actions doivent être mis en œuvre :

- Soit des actions de sensibilisation qui ont pour objet de diffuser les connaissances de base nécessaire. Toute personne ayant un rôle de près ou de loin dans le SMSI doit connaître les fondamentaux du système et leur positionnement respectif dans le fonctionnement de ce système organisationnel.
- Soit des actions de formation qui ont pour objet de transférer aux catégories de personnels qui en ont besoin, des compétences techniques indispensables afin d'exercer convenablement leur métier avec le niveau de qualité requis.

Dans tous les cas, toutes les actions entreprises, de formation comme celles de sensibilisation, doivent faire l'objet d'une évaluation de l'efficacité des résultats. Cette évaluation a pour objectif de vérifier le bien-fondé de chaque action, notamment le niveau des résultats obtenus par rapport au niveau des résultats attendus. Dans le cas où ces résultats attendus ne sont pas au rendez-vous, des actions de correction doivent être mises en œuvre, puis suivies, évaluées… afin d'atteindre la cible définie.

En outre, il est de la responsabilité de la direction de l'organisme de s'assurer que toutes informations relatives aux personnels sont « enregistrées ». Un enregistrement, au sens de la gestion de la qualité, est une preuve qui est conservée quel que soit le support d'archivage. Ces enregistrements concernent notamment :

- la formation initiale (diplômes) ;
- la formation professionnelle (stages) ;
- les qualifications ;
- les parcours professionnels ;
- les savoir-faire acquis ;
- les expériences ;
- …

4.4 Audits internes du SMSI (§ 6 de la norme)

Comme pour la norme NF EN ISO 9001 et pour tout système de management, la conduite d'audits internes à intervalles planifiés est une garantie de la conformité du fonctionnement du SMSI mis en place.

La norme NF EN ISO 9000 nous donne la définition suivante :

> **Processus méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit (enregistrements énoncés de faits ou autres informations pertinents et vérifiables) et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit (ensemble de politiques, procédures ou exigences utilisés comme référence) sont satisfaits.**

Le rôle des audits internes consiste à vérifier la conformité au référentiel de certification. Ce référentiel de certification est défini par les exigences de la norme NF ISO/CEI 27001, le contenu du système de management de l'organisme avec ces processus, procédures et instructions.

Cette vérification de la conformité doit s'exercer selon plusieurs directions :

1. Tout d'abord sur le plan de sa définition et de sa construction.
2. Puis, sur sa mise en œuvre de ses pratiques.
3. Ensuite, sur son exécution telle qu'elle était prévue.
4. Mais aussi sur sa mise à jour permanente afin de le conserver efficace pour atteindre, conserver et améliorer le niveau de sécurité de l'information souhaité.

Pour mémoire, comme pour les autres systèmes de management (par exemple pour la qualité telle que définie dans la norme NF EN ISO 9001) la mise en œuvre opérationnelle des audits internes implique les opérations suivantes :

- La définition et la planification des audits internes doivent être définies au préalable. Cette préparation est matérialisée par un programme (ou plan d'audit).
- La formalisation d'une procédure organisationnelle définissant le mode opératoire des audits internes, les critères, le champ, la fréquence et les méthodes d'audit.
- Le choix d'un certain nombre de personnes formées et compétentes pour être auditeurs internes dans l'organisme. Ces auditeurs doivent être objectifs, impartiaux et ne doivent pas auditer leur propre travail.
- Des enregistrements (rapports d'audit, fiches d'écarts) doivent être conservés à titre de preuves des audits internes réalisés.

Le lecteur pourra se reporter à la norme NF EN ISO 19011 qui définit les exigences pour mener des audits dans les systèmes de management.

4.5 Revue de direction du SMSI (§ 7 de la norme)

Comme pour la norme NF EN ISO 9001 et pour tout système de management, la réalisation de réexamens (revue de direction) à intervalles planifiés (au moins une fois par an) est une garantie du contrôle du fonctionnement du SMSI mis en place. Cette vérification contribue aussi à la révision et à l'amélioration du SMSI. La norme NF EN ISO 9000 nous donne la définition suivante :

> **Examen entrepris pour déterminer la pertinence, l'adéquation et l'efficacité de ce qui est examiné à atteindre les objectifs définis.**

La norme nous donne une liste des éléments d'entrée nécessaires à la conduite d'une revue de direction. À savoir :

- les résultats des audits et réexamens du SMSI ;
- les retours des parties intéressées ;
- l'état des actions correctives et préventives ;
- les vulnérabilités et menaces restant à traiter ;
- les résultats des mesures de l'efficacité ;
- les recommandations d'amélioration ;
- …

La norme nous donne une liste des éléments de sortie résultant de la conduite d'une revue de direction. À savoir :

- les évaluations de l'efficacité du SMSI ;
- la mise à jour du plan de traitement du risque ;
- les procédures à modifier ou à faire évoluer ;
- les besoins en ressources ;
- l'amélioration de la méthode d'évaluation de l'efficacité ;
- …

4.6 Amélioration du SMSI (§ 8 de la norme)

Comme pour la norme NF EN ISO 9001 et pour tout système de management, la mise en œuvre de l'amélioration continue est une exigence de l'efficacité du SMSI mis en place. Les non conformités doivent être traitées. Des actions correctives et préventives doivent être mises en œuvre et leurs résultats doivent être consignés avec évaluation de leur efficacité.

4.6.1 Action corrective

L'organisme doit mener des actions pour éliminer les causes de non-conformités avec les exigences du SMSI afin d'éviter qu'elles ne se reproduisent. La norme NF EN ISO 9000 nous donne la définition suivante :

> **Action visant à éliminer la cause d'une non-conformité ou d'une autre situation indésirable détectée.**

Une procédure documentée doit être formalisée. Elle doit préciser :

- l'identification des non-conformités ;
- la détermination des causes des non-conformités ;
- l'évaluation du besoin d'entreprendre des actions entreprises ;
- la détermination et la mise en œuvre des actions correctives ;
- la consignation des résultats de l'action ;
- le réexamen de l'action corrective entreprise pour son évaluation.

4.6.2 Action préventive

L'organisme doit mener des actions pour éliminer les causes de non conformités potentielles avec les exigences du SMSI afin d'éviter qu'elles ne surviennent. La norme NF EN ISO 9000 nous donne la définition suivante :

> **Action visant à éliminer la cause d'une non-conformité potentielle ou d'une autre situation potentielle indésirable.**

Une procédure documentée doit être formalisée. Elle doit préciser :

- l'identification des non-conformités potentielles ;
- l'évaluation du besoin d'entreprendre des actions ;
- la détermination et la mise en œuvre des actions préventives ;
- la consignation des résultats de l'action entreprise ;
- le réexamen de l'action préventive entreprise pour son évaluation.

4.7 Documentation

La documentation du SMSI sera fonction de la taille et des activités de l'organisme concerné. Elle constitue la formalisation du système de management mis en place. Elle doit inclure :

- la politique sécurité ;
- les objectifs ;
- les procédures documentées ;
- la méthodologie d'appréciation du risque ;
- le rapport d'appréciation du risque ;
- la déclaration d'applicabilité ;
- les enregistrements à titre de preuves.

4.7.1 Maîtrise des documents

La norme NF EN ISO 9000 nous donne la définition suivante d'un document :

Support d'information et l'information (données signifiantes) qu'il contient.

Les différents documents constituant la documentation doivent être protégés et maîtrisés. Comme pour l'ISO 9001, une procédure documentée de maîtrise documentaire est requise.

4.7.2 Maîtrise des enregistrements

La norme NF EN ISO 9000 nous donne la définition suivante d'un enregistrement :

> **Document spécifiant les résultats obtenus ou apportant la preuve des activités réalisées.**

Les différents enregistrements (preuves) doivent être établis, conservés, lisibles, protégés et maîtrisés. Comme pour la norme NF EN ISO 9001, une procédure documentée de maîtrise des enregistrements est requise.

5
Clé n° 5 – La déclaration d'applicabilité

Cette cinquième clé ouvre la porte sur les engagements et les mesures répondant aux exigences de la norme.

Ce thème correspond à l'annexe A de la norme NF ISO 27001. Cas très rare dans le domaine normatif, cette annexe est normative et non informative. C'est-à-dire que tout organisme qui prétend à l'obtention d'un certificat doit obligatoirement répondre à tous les objectifs de sécurité de cette annexe. L'organisme doit aussi décrire les mesures appropriées qu'il a prises et qui sont applicables à son système de management de la sécurité de l'information (SMSI).

Cette réponse doit être formalisée dans un document appelé « Déclaration d'Applicabilité » (en abrégé DdA).

5.1 Rôle de la DdA

La norme NF ISO 27001 nous donne la définition suivante :

> **Déclaration documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées applicables au SMSI d'un organisme.**

Ce document recense les objectifs de sécurité et les mesures de sécurité afférents aux meilleures pratiques. Toutefois, si l'organisme le souhaite, il peut ajouter des objectifs et des mesures complémentaires.

5.2 Thèmes sécurité imposés

Une liste de onze thèmes (plus les sous-thèmes) de la DdA correspond aux recommandations de mise en œuvre de l'ISO/CEI 17799:2005.

À savoir :

- La politique de sécurité de l'information.
- L'organisation de la sécurité de l'information.
- La gestion des actifs.
- La sécurité liée au RH.
- La sécurité physique et environnementale.
- La gestion de l'exploitation et des télécommunications.
- Les contrôles d'accès.
- Les acquisitions, développement et maintenance des systèmes d'information.
- La gestion des incidents liés à la sécurité de l'information.
- La gestion de la continuité de l'activité.
- La conformité.

5.3 Les sous-thèmes sécurité imposés

Les thèmes listés au paragraphe précédent se subdivisent en sous thèmes. Une liste de 133 thèmes de la DdA correspond aux recommandations de mise en œuvre de l'ISO/CEI 17799:2005. Le tableau 5.1 liste l'ensemble des thèmes et sous thèmes de la DdA (et fiche technique n° 4).

5.4 Comment y répondre ?

Pour chacune des 133 exigences détaillées dans les thèmes et sous-thèmes de l'annexe A de la norme, l'organisme candidat à la certification devra présenter à l'auditeur une « Déclaration d'Applicabilité » (DdA) formalisé. Dans ce document, l'ensemble des actions définies et mises en place par l'organisme doit être formalisé et vérifiable.

Dans les cas très rares ou une exigence ne serait pas applicable à l'organisme, ce dernier doit en apporter la preuve tangible (par exemple : pour un organisme qui ne pratiquerait pas de commerce électronique).

Tableau 5.1 Liste des thèmes de la DdA

Thèmes	Sous thèmes
Politique de sécurité de l'information	–
Organisation de la sécurité de l'information	Organisation interne
	Tiers
Gestion des actifs	Responsabilités relatives aux actifs
	Classification des informations
Sécurité liée aux RH	Avant le recrutement
	Pendant la durée contrat de travail
	Fin ou modification du contrat de travail
Sécurité physique et environnementale	Zones sécurisées
	Sécurité du matériel
Gestion de l'exploitation et des télécommunications	Procédures et responsabilités liées à l'exploitation
	Gestion de la prestation de service conclue avec un tiers
	Planification et acceptation du système
	Protection contre les codes malveillant et mobile
	Sauvegarde
	Gestion de la sécurité des réseaux
	Manipulation des supports
	Échange des informations
	Services de commerce électronique
	Surveillance

Thèmes	Sous thèmes
Contrôles d'accès	Exigences métier relatives au contrôle d'accès
	Gestion des accès des utilisateurs
	Responsabilités de l'utilisateur
	Contrôle d'accès réseau
	Contrôle d'accès au système d'exploitation
	Contrôle d'accès aux applications et à l'information
	Informatique mobile et télétravail
Acquisition, développement et maintenance des systèmes d'information	Exigences de sécurité applicables aux systèmes d'information
	Bon fonctionnement des applications
	Mesures cryptographiques
	Sécurité des fichiers système
	Sécurité en matière de développement et d'assistance technique
	Gestion des vulnérabilités techniques
Gestion des incidents liés à la sécurité de l'information	Remontée des événements et des failles liés à la sécurité de l'information
	Gestion des incidents liés à la sécurité de l'information et des améliorations
Gestion de la continuité de l'activité	–
Conformité	Conformité aux exigences légales
	Conformité avec les politiques et normes de sécurité
	Conformité technique
	Prise en compte de l'audit du système d'information

6
Clé n° 6 – La gestion des actifs

Cette sixième clé ouvre la porte sur la gestion des actifs et d'identification des risques.

Ce thème correspond :

- tout d'abord à l'identification des actifs (les biens) de l'organisme ;
- Puis à l'identification et à l'appréciation des risques tel que demandé par la norme internationale ISO/IEC 27001.

La notion de risque, et surtout les conséquences qui en résultent, sont bien présentes à notre esprit lorsque nous entreprenons une activité. Par contre, très souvent, nous ne disposons pas d'une méthode qui nous permette d'appréhender les événements qui surviennent, notamment les aléas qui génèrent de l'incertitude sur l'atteinte des résultats attendus. La démarche développée dans ce chapitre permet de retrouver une certaine confiance et un sentiment de sécurité sur les informations d'un organisme.

6.1 Qu'est ce qu'un actif ?

Les éléments importants d'un organisme sont les composants de son capital (au sens large) et qui lui permettent d'exercer son activité. On les appelle communément les **actifs** ou les **biens**.

La norme NF ISO/CEI 27001 définit un actif comme :

> **Tout élément qui représente de la valeur pour l'organisme.**

Bien connue en matière de gestion comptable, l'importance des actifs (éléments patrimoniaux) est clairement identifiée puisque ces actifs nécessitent une gestion minutieuse. Au regard de la sécurité de l'information, il est important que les éléments patrimoniaux immatériels soient aussi ajoutés dans l'inventaire des actifs de l'organisme.

Une liste non exhaustive d'actifs est donnée dans le tableau 6.1 (voir des exemples dans la fiche technique n° 5).

Tableau 6.1 Liste des actifs/biens (non exhaustive)

Actifs/biens
Bâtiments – Locaux
Personnels – Compétences
Équipements
Matériels informatiques
Réseaux
Logiciels
Données
Documentation
Fournisseurs – Sous-traitants
Valeurs immatérielles
…

6.2 Comment identifier un actif ?

Il convient d'identifier clairement tous les biens de l'organisme. Lors de cet inventaire, un soin tout particulier sera consacré aux actifs qui ont une importance significative pour le fonctionnement de l'activité de l'organisme. Un propriétaire, responsable de la gestion, est désigné pour chaque actif.

Le tableau 6.2 propose un cadre type pour l'inventaire des actifs (voir quelques exemples dans la fiche technique n° 6).

Tableau 6.2 Cadre pour l'inventaire des actifs/biens

Classe d'actif	Identifiant	Nom	Propriétaire	Description

L'annexe B, informative, de la norme NF ISO/CEI 27005 nous fournit des éléments de guides pratiques pour aider dans les travaux d'identification des actifs. Elle recommande notamment d'aborder tout d'abord les actifs primordiaux. Ces actifs supportent les informations relatives aux activités métier de l'organisme et à ses processus dont la dégradation impacte la réalisation des missions de l'entreprise. Sur le domaine d'application, il importe d'identifier les informations concernées par le plan de continuité de l'activité. Ensuite, l'inventaire doit s'intéresser aux actifs de type support. C'est notamment le cas :

1. des différents matériels et équipements de toutes catégories ;
2. de tous les composants logiciels qui contribuent au fonctionnement du système d'information :
   - ▼ systèmes d'exploitation ;
   - ▼ progiciels ;
   - ▼ applications métiers.
3. de tous les composants réseau :
   - ▼ supports de communication ;
   - ▼ ponts, routeurs, concentrateurs…
   - ▼ protocoles.
4. de toutes les catégories de personnel :
   - ▼ décideurs ;
   - ▼ utilisateurs ;
   - ▼ développeurs ;
   - ▼ …

Sans oublier les actifs relatifs aux sites, emplacements géographiques, et tous les composants de l'organisation.

6.3 Comment gérer un actif ?

Pour chaque actif, un « propriétaire » est désigné. Ce terme de propriétaire peut concerner soit une personne, soit une entité. Être propriétaire d'un actif ne signifie pas nécessairement jouir des droits juridiques de propriété. La responsabilité du propriétaire consiste à assurer la gestion, le contrôle, la mise à jour et la protection de l'actif concerné.

De ce fait, le propriétaire d'un actif est en charge des données attachées à cet actif. Notamment les éléments de vulnérabilité de cet actif ainsi que les évaluations des impacts et toutes les caractéristiques de risques qui seront abordées dans le chapitre 7 suivant relatif à la gestion des risques.

7
Clé n° 7 – Les processus de gestion des risques

Cette septième clé ouvre la porte décrivant les dispositions pour traiter les risques.

La notion de risque correspond à un événement dont l'apparition n'est pas certaine mais dont la manifestation est susceptible d'entraîner des conséquences plus ou moins dommageables. Les termes « aléas » ou « imprévu » sont quelques fois utilisés à la place du mot « risque ». Lorsque l'événement s'est déjà produit on emploie souvent le terme « problème ».

La gestion des risques a pour objectif de réduire les dangers et de minimiser leurs effets, donc de développer la notion de sécurité.

7.1 Qu'est ce qu'un risque ?

La démarche méthodologique de recensement des actifs (biens), développée au chapitre précédent, a pour seul objectif d'appréhender les différents facteurs de risques qui peuvent venir se greffer sur ces actifs de l'organisme.

Le document ISO GUIDE 73 défini le risque comme l'effet de l'incertitude sur l'atteinte des objectifs. Cet effet correspond à un écart positif et/ou négatif par rapport à une attente. Ces objectifs pouvant être de différents niveaux et d'ordre métier, financiers, environnementaux…

Un risque est souvent caractérisé en faisant référence à des événements et des conséquences potentielles ou une combinaison des deux.

Un événement, appelé parfois incident ou accident, correspond à une occurrence ou un changement d'un ensemble particulier de circonstances. Lorsqu'un événement est sans conséquence néfaste il pourra être qualifié de « succès ».

Les conséquences (appelées aussi impacts) correspondent aux effets d'un événement qui affectent les objectifs. Un événement peut engendrer une série de conséquences et déclencher des réactions en chaîne. Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs. Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

L'ISO/CEI 27002:2005 définit le risque comme :

> **La combinaison de la probabilité d'un événement et de ses conséquences.**

Tous les risques ne se ressemblent pas. À titre d'exemple, lorsqu'un événement désagréable n'a que peu de chance de se produire et si les conséquences n'ont qu'un impact limité, on pourra dire que le risque est faible. C'est l'intérêt de la suite de ce chapitre de décrire les bonnes pratiques permettant de gérer les risques qui pèsent sur la sécurité de l'information.

7.2 Comment identifier un risque ?

Lorsque les actifs (biens) sont inventoriés, il importe de déterminer quels sont leurs points faibles (les vulnérabilités) et les menaces susceptibles d'apparaître sur ces actifs et de les endommager.

Afin d'identifier les risques, après l'identification des actifs, la norme NF ISO/CEI 27001 exige d'identifier d'abord les menaces auxquelles sont confrontés les actifs puis d'identifier les vulnérabilités qui pourraient être exploitées par les menaces.

7.2.1 Les menaces

L'ISO/CEI 27002:2005 définit la menace comme :

> **La cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.**

Une menace peut provenir de l'intérieur ou de l'extérieur de l'organisme. Elle peut être accidentelle ou délibérée. Voici quelques exemples de type de menaces :

- les actions non autorisées ;
- les catastrophes naturelles ;
- les pertes de services ;
- les dommages physiques ;
- les défaillances techniques ;
- …

L'annexe C de la norme NF ISO/CEI 27005 donne une liste plus détaillée des types de menaces. La fiche technique n° 7 donne une liste des menaces générales. La fiche technique n° 8 donne une liste des menaces à caractère humain.

7.2.2 Les vulnérabilités

Au regard des menaces répertoriées, il importe d'identifier les points faibles, les vulnérabilités, pouvant nuire à chacun des actifs ou à l'organisation.

L'ISO/CEI 27002:2005 définit la vulnérabilité comme :

> **La faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace.**

Les vulnérabilités peuvent être liées à certaines conditions d'utilisation d'un actif ou à son environnement.

Voici quelques exemples de type de vulnérabilités :

- l'organisation ;
- le personnel ;
- le matériel ;
- le logiciel ;
- le réseau ;
- …

L'annexe D de la norme NF ISO/CEI 27005 donne une liste plus détaillée des type de vulnérabilités. La fiche technique n° 9 dresse un tableau avec des exemples de relations entre vulnérabilités et menaces pour :

- des actifs de type matériel informatique ;
- des actifs de type logiciel ;
- des actifs de type réseau ;
- des actifs de type personnel.

7.3 Typologie d'impacts sur les actifs – Notion de « DIC »

Après l'inventaire des menaces et des vulnérabilités qui concernent les actifs, la norme NF ISO/CEI 27001 exige d'identifier les impacts sur ces mêmes actifs.

La norme a retenu trois facteurs principaux pour ces impacts. Ils sont contenus dans la définition de la sécurité de l'information. À savoir :

> **Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information.**

Ces facteurs permettent de déterminer la force des impacts (conséquences) subis par chacun des actifs. La figure 7.1 matérialise les trois propriétés impactées.

D'autres propriétés intéressantes sont conseillées (mais non imposées par la norme). Éventuellement, elles peuvent venir compléter les attributs DIC. Notamment :

- l'authenticité ;
- l'imputabilité ;
- la non-répudiation ;
- la fiabilité.

7.3.1 La disponibilité

La norme NF ISO/CEI 27001 définit la disponibilité comme :

> **La propriété d'être accessible et utilisable à la demande par une entité autorisée.**

La disponibilité d'un équipement, d'un système ou d'un service est obtenue en faisant le ratio entre la durée pendant laquelle l'actif/bien est opérationnel et la durée totale pendant laquelle on souhaite qu'il soit accessible.

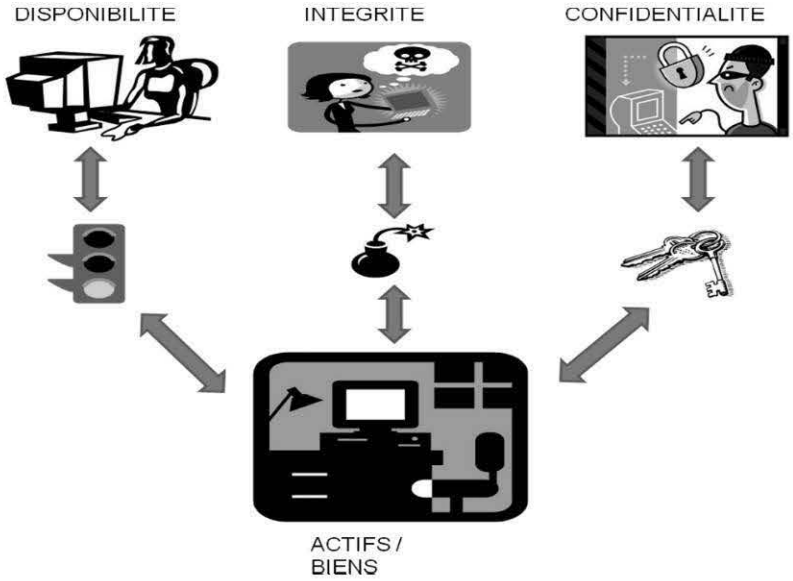


Figure 7.1 Les trois facteurs fondamentaux d'impact sur les actifs

La disponibilité n'a pas forcément la même importance pour l'utilisateur en fonction de la tranche horaire de mise à disposition d'un matériel ou d'un service. En effet, nous pouvons citer l'exemple d'une disponibilité mesurée à 99,9 % à la sortie d'un *data center* (plateau technique d'un prestataire de services technologiques de l'information). Par contre l'utilisateur pourra constater une dégradation de la disponibilité au niveau de son poste de travail en raison de perturbations liées au réseau de transmission. Un autre exemple est souvent constaté lors des dysfonctionnements ou des ruptures d'accès à un équipement ou à un service IT (*information technology*). Ces perturbations ou interruptions surviennent fréquemment pendant une période où l'utilisateur est particulièrement chargé et sollicite abondamment l'accès au service. C'est notamment le cas en présence de phénomènes dégradés dans des plages de forte activité de bureau (exemple 10 heures-midi et 14-17 heures). Dans de telles conditions, l'utilisateur accepte très difficilement tout dysfonctionnement qui a un impact très fort sur son métier. Son ressenti correspond à une mauvaise image de la disponibilité. Ce type de situation est à rapprocher avec les notions de qualité réelle et de qualité perçue.

La fiche technique n° 10 fournit des éléments pour le calcul de la disponibilité. Cette fiche est extraite de notre livre *10 clés pour la gestion des services de l'ITIL à l'ISO 20000*[5].

En effet, la notion de gestion de la disponibilité a été mise en avant dans le cadre des bonnes pratiques ITIL®[6]. La gestion de la disponibilité fait parties des exigences de l'ISO/CEI 20000 relatives à la certification des prestations de services des technologies de l'information.

7.3.2 L'intégrité

La norme NF ISO/CEI 27001 définit l'intégrité comme :

> **La propriété de protection de l'exactitude et de l'exhaustivité des actifs.**

L'intégrité d'un équipement, d'un système ou d'un service est obtenue lorsque celui-ci demeure intact et ne subit aucune altération ou destruction accidentelle ou volontaire.

L'intégrité de l'information doit être assurée à la fois lors du traitement de cette information, mais aussi lors de sa conservation et lors de sa transmission. La protection de l'intégrité doit être garantie contre toute agression accidentelle ou volontaire.

L'intégrité de l'information peut être abordée selon différents aspects :

- Aspect complétude : l'ensemble des éléments contenus dans l'information doit être entier, sans manquer de rien, donc sans être amputé d'une partie de ces éléments. L'information incomplète est un défaut pouvant être dû à une perte d'éléments ou à des éléments devenus illisibles ou irrécupérables.
- Aspect précision : tout ou partie des éléments contenus dans l'information qui est représentée par certaines valeurs (par exemple valeurs numériques). Le niveau de détail doit fournir une information sûre et non ambiguë. L'information imprécise n'est pas claire et peut être la conséquence d'altérations ou de pertes.

5 AFNOR Éditions, 2007.

6 ITIL® est une marque déposée de la Direction britannique du commerce (OGC). L'acronyme signifie *Information technology infrastructure library*, soit en français Bibliothèque de l'infrastructure des technologies de l'information.

- Aspect exactitude : tout ou partie des éléments contenus dans l'information doit conserver une fidélité et ne doit pas perdre dans leur degré de précision. C'est notamment le cas dans le domaine concerné par les appareillages de mesure qui doivent garantir une stabilité des mesures dans le temps. L'information inexacte n'est pas conforme à la réalité ou ne reproduit pas le modèle initial. Elle peut avoir été modifiée intentionnellement.
- Aspect validité : tout ou partie des éléments contenus dans l'information doit rester dans le cadre des règles prédéfinies. La conformité aux contraintes légales et réglementaires doit être maintenue quoiqu'il arrive. Une information valide est une information vraie ou vérifiée sur laquelle il est possible de s'appuyer en pleine confiance.

7.3.3 La confidentialité

La norme NF ISO/CEI 27001 définit la confidentialité comme :

> **C'est la propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés.**

La confidentialité d'un équipement, d'un système ou d'un service est obtenue lorsque son accès est réservé et protégé selon des règles définies.

Une information est déclarée confidentielle lorsqu'elle est limitée à un nombre restreint de personnes. Le terme confidentiel recouvre une notion de secret, c'est-à-dire une information qui doit être plus ou moins dissimulée ou cachée. Un peu comme un trésor qui est caché afin que les voleurs ne le trouvent pas. Pour y accéder, il faut justifier détenir le bon droit d'accès. En quelque sorte il faut posséder la bonne clé qui permet d'enlever l'écran qui cache, ou ouvrir la porte.

Il existe un équilibre à trouver entre la mise à disposition d'un grand nombre d'utilisateurs et la confidentialité. En effet, plus on souhaite ouvrir l'accès à un système d'information à un grand nombre de personnes et plus on augmente le risque que des personnes non autorisées puissent accéder intentionnellement ou non volontairement à ces informations. Par exemple, des informations personnelles nominatives, des informations financières, des informations concurrentielles, des informations stratégiques de développement, des brevets, des secrets de fabrication, des informations militaires… doivent être réservées aux seuls utilisateurs autorisés. Leur divulgation, notamment par des moyens frauduleux, peut nuire très

gravement au propriétaire de ces informations. D'autant qu'avec les moyens actuels de communication, cette information volée peut faire le tour de la planète en quelques secondes.

Il existe de nombreuses situations (ou des métiers spécifiques) pour lesquelles la législation ou des réglementations imposent des règles de confidentialité à respecter. Les systèmes d'information qui gèrent les données de ces situations doivent obligatoirement en tenir compte et en respecter les exigences.

Des outils tels que la cryptographie permettent d'augmenter les barrières de protection et de réserver l'accès à l'information exclusivement aux personnes ou entités qui disposent de la clé de décryptage.

7.4 Analyser et évaluer les risques

Au chapitre précédent, les impacts ont été identifiés au regard des trois facteurs disponibilité, intégrité, confidentialité. Il importe maintenant d'analyser la pondération qui en découle. Pour ce faire, la norme recommande d'en déterminer la criticité (*cf.* fiche technique n° 14).

Le fascicule de documentation FD X 50-117 définit la criticité comme :

> **(…) le niveau d'importance d'un risque résultant de la combinaison des caractéristiques quantifiées du risque, à savoir sa gravité, sa probabilité d'apparition et/ou sa probabilité de détection.**

L'analyse de cette criticité (ou l'importance d'un risque) consiste à étudier et évaluer les deux paramètres suivants :

- son impact ou sa gravité (les conséquences) ;
- sa probabilité (la fréquence d'apparition) ;

… et ensuite de combiner ces deux évaluations (conséquence et probabilité) pour déterminer la criticité de ce risque, c'est-à-dire les changements que le risque analysé peut faire subir à l'information.

7.4.1 Évaluer l'impact d'un risque (gravité)

Pour chaque couple de défaillance menace-vulnérabilité, l'importance des conséquences d'un défaut ou d'une perte doit être évaluée. L'évaluation de ces conséquences détermine la gravité du risque.

Le fascicule de documentation FD X 50-117 définit la gravité comme :

> **(…) l'ampleur des conséquences de l'événement redouté sur un actif.**

Derrière ce terme de « gravité » il y a une notion de dangerosité, de poids des conséquences supportées. D'où l'importance de définir une échelle faisant apparaître des différences de niveau d'appréciation de l'impact.

Le tableau 7.1 propose un exemple d'échelle d'impact (gravité). Voir un exemple des niveaux de gravité pour un projet dans la fiche technique n° 11.

Tableau 7.1 Exemple de pondération des niveaux de gravité

Type d'impact	Pondération
Très faible	0
Faible	1
Moyen	2
Élève	3
Très élevé	4

Bien évidemment, le niveau des impacts doit être apprécié pour chacun des trois facteurs : Disponibilité, Intégrité et Confidentialité des actifs sélectionnés.

7.4.2 Évaluer la probabilité d'apparition d'un risque (fréquence)

Pour chaque couple de défaillance menace-vulnérabilité, la probabilité d'apparition d'un défaut ou d'une perte doit être évaluée. L'évaluation de cette probabilité détermine la fréquence d'apparition du risque.

Le document *ISO Guide 73* définit la probabilité comme :

> **La mesure de la possibilité d'occurrence exprimée par un chiffre entre 0 et 1.**
> **0 indiquant une impossibilité.**
> **1 indiquant une certitude absolue.**

Le document *ISO Guide 73* définit la fréquence comme :

> **Le nombre d'événements ou d'effets par unité de temps donné.**

Qui dit « probabilité » sous-tend le caractère aléatoire de l'apparition des conséquences du risque. Lorsque ces conséquences du risque apparaissent, plus leur « fréquence » d'apparition est élevée, plus leurs effets nuisibles seront dommageables pour l'organisme. D'où l'importance de définir une échelle faisant apparaître des différences de niveau d'appréciation de l'impact. Le tableau 7.2 propose un exemple d'échelle de probabilité d'apparition (fréquence d'exposition au risque). Voir un exemple des niveaux de probabilité pour un projet dans la fiche technique n° 12.

Tableau 7.2 Exemple d'échelle de probabilité d'apparition

Type de fréquence	Pondération
Très peu probable	0
Peu probable	1
Possible	2
Probable	3
Fréquent	4

Bien évidemment, le niveau de cette fréquence d'exposition doit être apprécié pour chacun des trois facteurs : Disponibilité, Intégrité et Confidentialité des actifs.

7.5 Déterminer les risques acceptables

Pour l'ensemble des risques identifiés, analysés et évalués, il importe de déterminer ceux qui sont acceptables tel quel. Pour cela, des critères d'acceptation des risques doivent être définis en fonction des objectifs de sécurité définis par la direction générale de l'organisme. La fiche technique n° 13 fait apparaître dans un tableau les deux axes (gravité et probabilité) du risque avec leurs échelles respectives de notation. En fonction des critères d'acceptation des risques, qui sont propres à chaque organisme, le tableau permet de distinguer différents domaines d'acceptabilité :

- Risque acceptable.
- Risque à surveiller.
- Risque inacceptable.

Le tableau 7.3 propose l'inventaire des risques et des impacts sur les actifs.

Tableau 7.3 La criticité des risques sur les actifs/biens

Actif	Menace	Vulnérabilité	Disponibilité		Intégrité		Confidentialité	
			Impact	Fréquence	Impact	Fréquence	Impact	Fréquence

7.6 Traiter les risques

Pour les risques qui ne sont pas acceptables (mais aussi dans une moindre mesure pour les risques à surveiller), des mesures appropriées de parade ou de contournement vont devoir être mises en œuvre afin d'en rendre les effets acceptables. C'est le processus de traitement du risque.

La norme NF ISO/CEI 27001 définit le processus de traitement du risque comme :

> **Processus de sélection et de mise en œuvre des mesures visant à diminuer le risque.**

Il existe plusieurs options possibles afin de traiter un risque. Elles comprennent (*cf.* fiche technique n° 15) :

- la réduction par l'application de mesures appropriées (parades) ;
- l'acceptation de certains risques en connaissance de cause ;
- l'évitement ou le refus de certains risques ;
- le transfert de risques à des tiers (assureurs, fournisseurs…).

Dans le cadre d'un projet d'amélioration de la couverture des risques, en fonction des objectifs assignés par la direction, un plan de gestion des risques doit être formalisé. Un exemple de plan de traitement des risques figure dans la fiche technique n° 16. Dans ce plan, les différentes actions de progrès sont répertoriées et gérées. Leur efficacité doit être évaluée et rectifiée si besoin.

7.7 Approuver les risques résiduels

Après application des mesures de réduction des risques, de même que pour certains risques dont les impacts sont jugés non significatifs, il va rester un petit nombre de risques pour lesquels les conséquences ne justifient pas l'investissement de mesures supplémentaires. Ce sont les risques résiduels.

La norme NF ISO/CEI 27001 définit un risque résiduel comme :

> **Un risque qui subsiste après application du traitement à un risque.**

La liste de ces risques résiduels doit être établie et la direction de l'organisme doit obligatoirement approuver cette liste.

7.8 Le management des risques

Après avoir détaillé de manière précise tous ces concepts relatifs aux risques, il importe de donner une vue d'ensemble de ce qu'implique le management de ces risques qui menacent la sécurité de l'information.

La norme NF ISO/CEI 27001 définit le management du risque comme :

> **Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.**

En résumé, les principales activités sont schématisées dans la figure 7.1. Elles concernent :

- le recensement des actifs/biens avec identification des risques ;
- l'analyse du risque ;
- l'évaluation du risque ;
- le traitement du risque ;
- l'acceptation du risque ;
- la communication sur le risque.

La fiche technique n° 17 reproduit le processus de gestion des risques en sécurité de l'information tel que présenté par la norme NF ISO/CEI 27005.

Afin de s'inspirer d'autres documents plus génériques en matière de sécurité, nous conseillons au lecteur de se reporter aux fiches techniques suivantes qui reprennent des informations et les exemples du fascicule de documentation FD X 50-252.

À savoir :

- Fiche technique n° 18 – *Management du risque* ;
- Fiche technique n° 19 – *Exemple de pondération de probabilité d'un danger* ;
- Fiche technique n° 20 – *Exemple de pondération de la fréquence d'exposition à un danger.*

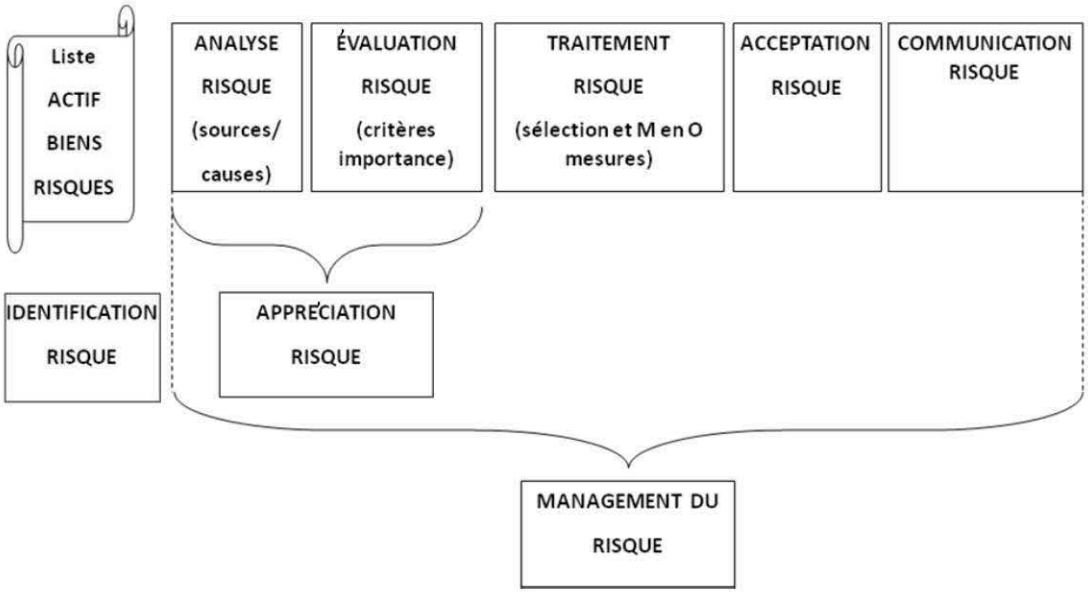


Figure 7.2 Schéma synoptique du management du risque

8
Clé n° 8 – Les incidents de sécurité

Cette huitième clé ouvre la porte pour gérer les incidents de sécurité.

Le système de management de la sécurité de l'information, comme tout système, est soumis à des événements intérieurs ou extérieurs qui sont susceptibles de venir en perturber le fonctionnement.

Ces événements ayant une incidence sur la sécurité de l'information doivent faire l'objet d'un enregistrement comme incident ou faille, puis d'un traitement particulier.

8.1 Un incident, qu'est-ce que c'est ?

Le dictionnaire *Le Robert*[7] donne la définition générale d'un incident de la manière suivante :

« Incident : événement peu important en lui-même mais capable d'entraîner de graves conséquences. »

La notion d'incident a été abondamment développée dans l'ITIL® qui en donne la définition suivante :

« Événement qui ne fait pas partie du fonctionnement normal d'un service et qui entraîne, ou peut entraîner, une interruption de service ou une détérioration de sa qualité. »

7 *Le Robert pour tous*, édition de 1994.

Pour ce qui concerne la qualité des prestations de service dans les technologies de l'information, c'est la norme NF ISO/CEI 20000-1 qui en donne la définition suivante :

> **Tout événement qui sort du cadre d'exploitation normale d'un service et qui entraîne ou peut entraîner une interruption ou une baisse de la qualité de ce service.**

Dans notre ouvrage *10 clés pour la gestion des services, de l'ITIL à l'ISO 20000*, nous avons consacré un chapitre complet au processus de gestion des incidents.

Au niveau de la norme NF ISO/CEI 27001, la norme attache un intérêt tout particulier aux incidents qu'elle qualifie d'« incident de sécurité ». La norme en donne la définition suivante :

> **Un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événements indésirables ou inattendus présentant une probabilité de compromettre l'activité.**

Voici quelques exemples d'incidents de sécurité :

- perte de service ;
- perte de matériel ;
- dysfonctionnement ;
- erreur humaine ;
- …

8.2 Les facteurs déclenchant d'un incident

Des **événements** surviennent. Nous conviendrons de dire qu'un événement est un fait réel non prévu aux yeux de l'utilisateur, dont la venue a pour effet d'avoir un impact (forme, quantité, délai, qualité…) sur la perception que l'utilisateur a de la fourniture d'un service.

Ainsi, tout événement détecté par l'utilisateur et qui arrive chez le fournisseur de service va déclencher un processus de traitement. Chez le fournisseur de service, un point d'entrée unique de contact avec le client/utilisateur est mis en place. C'est le centre de service, entité *ad hoc* pour recueillir et enregistrer toutes les informations relatives aux événements.

Le terme gestion des incidents est générique. En effet, à l'étude du contenu de l'information événementielle recueillie, l'événement apparu pourra concerner :

- soit une demande d'information (DDS) ;
- soit une demande de travail particulier (DDS) ;
- soit une demande d'amélioration (DDS) ;
- soit un dysfonctionnement constaté par l'utilisateur (incident) ;
- soit un défaut constaté par un opérateur (incident).

Les trois premières catégories correspondent à une demande de service[8] DDS (*service request*) au sens de l'ITIL®. Il est utile de les différencier.

Par contre, l'incident est un dysfonctionnement par rapport à l'attente d'un utilisateur pour le service (matériel ou logiciel) qu'il utilise.

8.3 Les caractéristiques des incidents

Plusieurs causes peuvent être à l'origine d'un incident. Il est possible de classifier les incidents en fonction de la nature de leur origine.

◆ Nature

Nous pouvons citer ci-dessous quelques catégories :

- Une panne est survenue sur un matériel (PC, serveur, réseau…).
- Un défaut de fonctionnement d'un logiciel.
- Une attaque virale.
- Une tentative d'intrusion.

Tous les incidents ne présentent pas le même niveau de risque pour le client comme pour le fournisseur de services. La connaissance de ces caractéristiques va induire des procédures de traitement adaptées.

◆ Priorité

La priorité de résolution permet de donner l'ordre de traitement requis dans la résolution d'un incident. La priorité est déterminée en fonction de la combinaison de deux critères : la **criticité** et de la **sévérité**.

8 Une demande de service (DDS) correspond à toute requête adressée au centre de service et qui ne soit pas un incident.

Par exemple, on pourra convenir trois niveaux de priorité :

- Urgent (P1).
- Maximum (P2).
- Minimum (P3).

◆ Criticité

C'est un critère permettant d'apprécier le degré d'urgence du délai de résolution d'un incident (facteur temps). Cette appréciation est fondée sur la base des enjeux ou du contexte environnemental du métier de l'utilisateur.

◆ Niveau de sévérité (gravité)

C'est un critère qui est défini en fonction de l'impact sur l'organisation (facteur quantitatif). L'écart constaté par rapport au niveau normal de service sera différent s'il concerne le commercial, la logistique ou l'administratif. L'impact peut concerner peu ou beaucoup de personnes. Le facteur coût financier peut aussi intervenir.

Par exemple, on pourra convenir de trois niveaux de gravité/sévérité :

- Bloquant.
- Grave.
- Mineur.

Le tableau 8.1 donne un exemple de construction de grille de priorité.

Tableau 8.1 Exemple de grille de priorité

		Gravité (impact)		
		Haute	Moyenne	Faible
Criticité (urgence)	Haute	P1	P2	P3
	Moyenne	P2	P2	P3
	Faible	P3	P3	

8.4 Le traitement des incidents

Quelle qu'en soient la cause (nature) et la priorité (criticité, gravité), un incident va nécessiter le déclenchement d'un certain nombre d'actions pour y remédier et le résoudre. Le fournisseur de services doit définir et mettre en œuvre des procédures formalisées permettant de maîtriser le traitement complet (de bout en bout) d'un incident : depuis sa déclaration et son enregistrement jusqu'à la confirmation de sa résolution et sans oublier sa clôture.

Quoi qu'il en soit, la défaillance constatée doit être solutionnée avant l'expiration du délai maximum déterminé dans les engagements contractuels de service (SLA[9]). L'objectif est la restauration d'un service nominal et non la détermination de la cause.

Le processus général de traitement d'un incident comporte cinq phases :

- la détection et l'enregistrement ;
- la prise en compte et la classification ;
- l'analyse et le diagnostic ;
- la résolution et le rétablissement ;
- la clôture.

La fiche technique n° 21 donne une représentation schématique du processus général de traitement des incidents (logigramme).

8.4.1 L'enregistrement

Un utilisateur/client détecte un écart par rapport à son attente de service. Il formule son observation au moyen d'une demande par téléphone, fax ou e-mail. Cette demande arrive au centre de service, point d'entrée unique, désigné pour assurer toutes les relations avec les clients. Toutes les demandes doivent être enregistrées. L'enregistrement (dans la CMDB[10]) doit être effectué le plus tôt possible, dès l'apparition de l'événement. L'opérateur du centre de service doit saisir un maximum d'informations descriptives (qui, quoi, comment, quand, où).

9 SLA signifie *service level agreement*, soit en français : contrat/convention de service. Généralement, un contrat est signé avec un prestataire externe et peut contenir des clauses de pénalités financières alors qu'une convention de service sera signée entre des entités organisationnelles d'une même société ou groupe.

10 CMDB signifie *configuration management data base*, soit en français base de données de gestion de la configuration.

Lorsqu'un outil logiciel de gestion des incidents est utilisé on parle généralement d'ouverture et de saisie d'un « ticket ».

Une confirmation de l'enregistrement est fournie à l'auteur de la demande. L'utilisateur sera tenu informé de l'avancement du processus.

8.4.2 La prise en compte et la classification

Une fois l'enregistrement réalisé, la demande est prise en compte par le centre de service (accueil de niveau 1). Si l'événement correspond à une demande d'information, un traitement particulier ou à une demande d'amélioration, les réponses seront adaptées :

- soit information en retour et clôture de l'événement ;
- soit transmission de la demande à l'exploitation concernée ;
- soit transmission aux études pour analyse de la demande.

Si l'événement correspond à un dysfonctionnement, les informations saisies sont comparées avec les critères des grilles de priorité, de criticité et de gravité. Ainsi, l'impact et l'urgence de l'incident déterminent sa classification. Il faut remarquer que cette classification doit être menée sur la base de caractères objectifs. En effet, si l'on s'en tient uniquement aux dires de l'utilisateur, tout est urgent et il est bien difficile de prioriser. Par contre, le fait de disposer de grilles avec des critères précis est une garantie de professionnalisme.

En fonction de cette classification, l'incident, avec sa nature et sa priorité, est affecté à un acteur compétent pour l'analyser (niveau 2).

L'auteur de la demande est tenu informé du résultat de la classification et de l'état d'avancement de la suite qui est donnée. Si l'incident est classifié comme incident majeur ou comme incident de sécurité, celui-ci fera l'objet d'une procédure particulière (*cf.* § « Procédure à rédiger dans le SMSI »).

8.4.3 L'analyse et le diagnostic

L'incident classifié est transmis à un niveau supérieur (niveau 2) qui a la compétence technique pour étudier les caractéristiques de l'incident (support spécialisé). Cette analyse permet de diagnostiquer les causes du dysfonctionnement et d'en déduire la/les solutions qui conviennent. L'analyse va commencer par rapport aux expériences passées. La base de connaissance (CMDB) qui contient l'historique des incidents antérieurs

est utilisée afin de réutiliser les informations et les solutions des incidents similaires. Si l'incident ne correspond pas à une erreur connue, les investigations vont porter sur tout élément d'information susceptible d'aider à la recherche des causes potentielles. Une fois la cause identifiée, les experts techniques compétents vont proposer une ou plusieurs solution(s) pour la résolution. Les solutions possibles imaginées seront du type :

- soit modification de donnée(s) contenue(s) dans les bases ;
- soit une modification de configuration matérielle(s) ;
- soit modification de composant(s) logiciel(s) ;
- soit de solution(s) de contournement, à usage temporaire, dans l'attente d'une prochaine version de système.

L'auteur de la demande est tenu régulièrement informé par le centre de service de l'état d'avancement des travaux de diagnostic et de la solution préconisée lorsque celle-ci a été élaborée (ou choisie entre plusieurs).

8.4.4 La résolution

C'est l'activité qui va permettre de restaurer le service dès que possible. En fonction du résultat du diagnostic, les solutions possibles sont :

- Soit la mise en place d'un contournement temporaire dans l'attente d'une solution plus élaborée. Dans certains cas, la correction du dysfonctionnement nécessite plus de temps. La solution de contournement permet alors d'attendre les résultats d'une maintenance plus lourde et qui est pratiquée « à froid ».
- Soit une maintenance corrective « à chaud », qui a pour objectif de faire disparaître le dysfonctionnement et satisfaire aux fonctionnalités définies pour le service. La charge de travail de correction ne doit pas dépasser un certain nombre de jours. Au-delà de ce seuil, et si le degré d'urgence le permet, il faudra de préférence réaliser une maintenance « à froid » qui sera planifiée dans le temps.
- Soit la résolution de l'incident nécessite l'intervention d'un/expert(s) spécialisé(s). C'est la procédure d'escalade. Dans ce cas, au regard de la gravité de la situation ou de la non-efficacité du circuit de traitement normal, la situation nécessite une montée dans les niveaux hiérarchiques. Ce mode de traitement est considéré comme exceptionnel et doit être utilisé lorsque la procédure normale aura fait la preuve de son inefficacité.

- Il peut aussi arriver que l'incident soit dû à une fonctionnalité non couverte jusque-là par le système de traitement de l'information. Dans ce cas, l'incident est transformé en demande de nouvelle fonctionnalité ou d'évolution.
- Dans certaines situations particulièrement difficiles ou aiguës, il est nécessaire de faire face à une situation de crise (solution inefficace, trop longue, pas adaptée, inerte…). Une cellule spéciale avec un mode de fonctionnement exceptionnel est mise en place avec des circuits courts afin de trouver une solution rapide. Cette procédure permet de mobilier la hiérarchie et de dégager des moyens supplémentaires. C'est le mode ultime de la procédure d'escalade. À situation exceptionnelle, solution exceptionnelle.

Dans tous les cas, l'auteur de la demande initiale est tenu informé de l'état d'avancement et si possible de la date prévisionnelle de fin de résolution de l'incident, date à laquelle le service redeviendra normal.

8.4.5 L'escalade

Malgré toute la compétence et tous les efforts déployés par les experts techniques de niveau 2, il peut arriver que :

- soit la solution ne peut pas être trouvée car elle ne ressort pas de ce niveau d'expertise ;
- soit la solution préconisée par le niveau 2 et mise œuvre pour rétablissement s'est avérée insuffisante ou inopérante.

Dans ce cas, il y a escalade ; c'est-à-dire une montée de niveau. Ce passage du niveau 2 au niveau 3 nécessite le besoin de compétences en développement ou en architecture mobilisables moins facilement.

8.4.6 Remarque

Par souci de simplification nous avons retenu seulement trois niveaux d'escalade. Il peut y en avoir un quatrième. Ce niveau supplémentaire n'apporte rien de plus dans le processus. Le découpage et le positionnement seront ajustés en fonction de l'organisation, des moyens et des compétences des ressources dont dispose le fournisseur de service.

8.4.7 La clôture

La clôture d'un incident peut être prononcée seulement si l'auteur de la demande a pu constater que les actions entreprises pour résoudre l'incident ont été efficaces. C'est-à-dire que dans l'environnement de production, l'exploitation du service est revenue à la normale. L'enregistrement de cette validation du client doit être réalisé dans la base de connaissances (CMDB).

En l'absence d'information sur le retour à la normale du service, le fournisseur de services doit relancer son client/utilisateur jusqu'à obtention de cette confirmation. Alors, et alors seulement, le centre gestionnaire du service peut procéder à la clôture de l'incident déclaré.

8.5 Assurer la continuité de l'activité

Lorsqu'un incident, et notamment un incident de sécurité, se produit, un organisme – quel qu'il soit – doit être en mesure d'assurer la continuité de ses activités. Dans certains cas, les conséquences des risques peuvent être si fortes (par exemple accident/sinistre) que la survie de l'organisme peut être mise en cause.

Le dictionnaire *Le Robert*[11] donne la définition générale suivante :

Continuité : qui n'est pas interrompu dans le temps.

Il importe donc d'organiser l'entreprise afin qu'en cas de survenance d'une interruption, l'activité puisse continuer d'être exercée. Une rupture de continuité d'activité pénalise la disponibilité de l'information. Une mesure pertinente pour contrer le risque de défaillance des systèmes provoquant des interruptions d'activités consiste à prévoir :

- les conditions d'activation (facteurs de déclenchement) ;
- les services métier cruciaux ;
- les services qui peuvent supporter un mode dégradé ;
- les scénarios de sinistres ;
- les impacts sur l'exploitation, les effectifs, les matériels, les équipements… ;
- les travaux à conserver en priorité ;
- les responsabilités à mettre en place ;

11 *Le Robert pour tous*, édition 1994.

- les formations à effectuer ;
- les documentations à rédiger ;
- les ressources à mobiliser en remplacement des ressources défaillantes ;
- les niveaux de récupération satisfaisants ;
- les communications à mettre en œuvre ;
- l'organisation du « basculement » après coupure ;
- les procédures de reprise ;
- les procédures d'urgence ;
- les procédures de repli ;
- … et comment garantir la disponibilité, l'intégrité et la confidentialité de l'information.

L'organisation de l'ensemble de ces mesures de protection est formalisée dans un Plan de Continuité de l'Activité (PCA) et dans un Plan de Reprise d'Activité (PRA). Ces deux plans doivent s'insérer dans un cadre unique afin de garantir la cohérence entre eux.

La notion de processus de gestion de la continuité a été mise en avant dans le cadre des bonnes pratiques ITIL®. La gestion de la continuité fait partie des exigences de la norme NF ISO/CEI 20000-1 relatives à la certification des prestations de services des technologies de l'information.

La fiche technique n° 22 donne un exemple de sommaire type pour un plan de reprise d'activité. Cette fiche est extraite de notre livre *10 clés pour la gestion des services, de l'ITIL à l'ISO 20000*[12].

Il ne faut pas oublier qu'un plan de continuité ou de reprise d'activité doit toujours être opérationnel. Pour le vérifier, ces plans doivent être mis à l'essai (testés) périodiquement.

8.5.1 Incident courant

Un incident courant résulte d'un événement en production qui entraîne (ou peut entraîner) une interruption ou une dégradation du service rendu. Sa résolution ne nécessite pas l'activation du plan de reprise d'activité. Les solutions au dysfonctionnement sont connues. L'incident est maîtrisé.

12 Pour plus de détails sur la gestion de la continuité, le lecteur pourra se reporter à cet ouvrage paru chez AFNOR Éditions en 2007.

8.5.2 Incident majeur

Un incident majeur résulte d'un événement en production qui entraîne (ou peut entraîner) une interruption ou une dégradation importante du service rendu. Sa résolution nécessite l'activation du Plan de reprise d'activité (PRA) selon un scénario simple et connu. Les solutions au dysfonctionnement impliquent une bascule d'une ou plusieurs applications. Le délai de résolution n'est pas toujours maîtrisé.

8.5.3 Sinistre

Un sinistre résulte d'un événement en production qui entraîne (ou peut entraîner) une interruption ou une dégradation grave, en termes de conséquences, du service. Sa résolution nécessite l'activation du PRA selon un scénario complexe et pas toujours connu. Les solutions au dysfonctionnement impliquent une bascule de tout le site de production.

8.5.4 Gestion de crise

Une crise est une manifestation brutale ou une dégradation d'un état ou d'une situation consécutive à un incident majeur ou à un sinistre. La gestion de crise est un ensemble de trois phases qui s'enchaînent pour former un cycle de vie avec cinq processus. À savoir :

- Une phase de préparation avec un processus de prévention qui consiste à définir, rédiger les plans de continuité et les tester.
- Une phase de déroulé pendant une crise. Cette phase comprend trois processus :
- Un processus de réaction à la crise avec des tâches d'alerte, de diagnostic et d'activation du PRA.
- Un processus de gestion de crise avec des tâches de pilotage, d'organisation des moyens et de communication aux parties intéressées.
- Un processus de retour à la normale avec des tâches de réparation, de remplacement et de tests.
- Une phase de retour à la gestion opérationnelle avec les tâches de maintenance, de contrôle et de tests.

9
Clé n° 9 – Les exigences d'un système de gestion

Cette neuvième clé ouvre la porte sur la passerelle qui relie la norme ISO/IEC 27001 à la norme ISO 9001.

Avec ce thème apparaît une liaison de type imbrication entre la norme NF EN ISO 9001, qui est générique pour un système de management de la qualité (SMQ) quel que soit le domaine d'activité, et une norme sectorielle telle que la norme NF ISO/CEI 27001 qui est spécialisée pour la sécurité de l'information.

Il pourrait en être de même avec la norme NF ISO/CEI 20000-1 pour un système de management des prestations de service informatique, ou avec la norme NF EN ISO 14001 pour un système de management de l'environnement, ou avec l'OHSAS 18001 pour un système de management de la santé et de la sécurité au travail.

Dans notre cas précis de la sécurité de l'information, nous l'appellerons système de management de la sécurité de l'information (SMSI) si le référentiel est exclusivement la norme NF ISO/CEI 27001, ou système de management intégré (SMI) si les exigences d'un autre référentiel sont prises en compte.

9.1 Exigences d'un système de gestion

9.1.1 Pourquoi un SMSI ?

La norme NF ISO/CEI 27001 définit le SMSI comme :

> **Partie du système de management global, basé sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information.**
>
> **NOTE : Le système de management inclut l'organisation, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.**

Le système de gestion (de la sécurité de l'information) est en complémentarité parfaite avec les exigences de la norme NF EN ISO 9001 qui s'appliquent à la qualité. Ce système, qui pourra être certifié (*cf.* § « Clé n° 10 – Processus de certification »), matérialise la pérennité des engagements pris par l'organisme afin d'assurer la sécurité de l'information.

C'est pourquoi un organisme ayant déjà mis en place un système de management de la qualité (SMQ), ou obtenu une certification NF EN ISO 9001, aura un avantage certain sur la définition et la mise en œuvre des exigences normatives exposées dans les thèmes de ce chapitre.

L'organisation personnalisée du SMSI (ou du SMI dans le cas intégré) pour un organisme est décrite dans le document *Manuel de Management de la sécurité* (ou *Manuel Qualité et Sécurité*). Ce document doit répondre à chacune des exigences de la norme. Ainsi, nous y trouverons :

- L'établissement du SMSI/SMI avec :
  - l'engagement écrit de la direction du fournisseur de service ;
  - la définition du domaine d'application ;
  - la cartographie des processus ;
  - la politique sécurité ;
  - la méthodologie d'appréciation du risque ;
  - l'identification des risques ;
  - l'analyse des risques ;
  - l'identification et l'évaluation des choix de traitement des risques ;
  - les objectifs et les mesures de sécurité ;
  - la déclaration d'applicabilité (DdA) ;
  - la liste des procédures (description dans un document spécifique) ;

- la gestion de la documentation et des enregistrements ;
- la gestion des ressources humaines.

- La mise en œuvre du SMSI/SMI avec :
  - le plan de traitement des risques ;
  - la mise en œuvre des mesures de sécurité ;
  - l'évaluation de l'efficacité des mesures de sécurité ;
  - la mise en œuvre des programmes de formation et de sensibilisation ;
  - la gestion des opérations ;
  - la gestion des ressources ;
  - la gestion des ressources ;
  - la mise en œuvre des procédures et des mesures.
- La surveillance et le réexamen du SMSI/SMI avec :
  - l'exécution des procédures de surveillance et de réexamen ;
  - l'évaluation de l'efficacité des mesures ;
  - le réexamen des appréciations du risque ;
  - la réalisation des audits internes ;
  - la réalisation des revues de direction ;
  - la mise à jour des plans de sécurité ;
  - l'enregistrement des événements pouvant avoir un impact.
- La mise à jour et l'amélioration du SMSI/SMI avec :
  - la mise en œuvre des améliorations ;
  - la réalisation des actions correctives et préventives ;
  - l'information des parties prenantes ;
  - la vérification de l'atteinte des objectifs.

La fiche technique n° 23 propose un plan type de Manuel de Management.

9.1.2 Responsabilité de la direction

La direction de l'organisme doit fournir la preuve de son implication dans :

- la politique de sécurité ;
- les objectifs de sécurité à atteindre (pluriannuels et annuels) ;
- la définition des rôles et responsabilités pour la sécurité ;
- la fourniture de ressources suffisantes ;
- la détermination des critères d'acceptation des risques ;
- le contrôle des audits internes ;
- la réalisation des revues de direction.

La direction doit déterminer et fournir les ressources nécessaires pour maintenir une sécurité adéquate et une application correcte des mesures.

La direction doit s'assurer que le personnel a les compétences nécessaires. Dans le cas contraire, des actions de formation doivent satisfaire aux besoins. Des enregistrements doivent apporter la preuve de la formation initiale, des formations professionnelles, du savoir-faire, de l'expérience et des qualifications.

9.1.3 Exigences relatives à la documentation

Un système de management repose sur une gestion rigoureuse de la documentation. Cette gestion comporte des procédures précisant les règles d'identification, de rédaction, de validation, d'approbation, de diffusion et de retrait des documents. Des enregistrements[13] (au sens de la qualité) doivent pouvoir apporter la preuve des actions réalisées.

9.1.4 Compétence, sensibilisation et formation

Les rôles et responsabilités liées à la sécurité de l'information doivent être définis et tenu à jour. De même, les compétences nécessaires au bon fonctionnement de la sécurité de l'information doivent être définies et à jour.

Par rapport à ces besoins de compétences, la direction de l'organisme doit s'assurer en permanence de l'adéquation du niveau de compétences de son personnel par rapport aux besoins pour assurer le niveau de sécurité de l'information requis.

Lorsqu'il existe un écart entre besoins de compétences et disponibilités de compétences, l'organisme dispose de deux moyens pour réduire l'écart et permettre d'assurer le service.

a. Le **recrutement** : les renseignements fournis par un candidat permettront de vérifier si le candidat dispose des points forts nécessaires lui permettant de tenir le poste.
b. La **formation de perfectionnement** : les besoins en formation sont rassemblés dans un plan de formation et de perfectionnement.

La fiche technique n° 24 donne une description de fonction pour un responsable sécurité de l'information (monsieur Sécurité).

13 *Cf.* la définition d'un enregistrement dans la partie II, fiche technique n° 1.

10
Clé n° 10 – Le processus de certification

Cette dixième clé ouvre la porte qui mène à l'obtention de la récompense : le certificat attestant de la conformité du système de management mis en place.

Pour ce thème relatif à la certification, le lecteur pourra se reporter au livre *10 clés pour réussir sa certification ISO 9001* rédigé par le même auteur et publié par AFNOR Éditions en 2009. En effet, les aspects de certification de système de management sont, dans leurs principes, similaires quelle que soit la norme internationale de référence.

10.1 Accréditation et certification

Souvent, dans l'esprit du public, il y a confusion entre les deux termes. Il est utile de rappeler que :

- La **certification** est l'action de délivrer des certificats par un organisme de certification (lequel organisme a été au préalable accrédité).
- L'**accréditation** est l'habilitation donnée par le COFRAC[14] à un organisme pour qu'il devienne organisme de certification (certificateur) et qu'il ait la capacité de délivrer des certificats.

14 COFRAC : Comité français d'accréditation a été créé en 1994. Il est désigné par le décret n° 2008-1401 du 19 décembre 2008 relatif à l'accréditation et à l'évaluation de conformité pris en application de l'article 137 de la loi n° 2008-776 du 4 août 2008 de modernisation de l'économie (site web à l'adresse suivante : www.cofrac.fr).

La figure 10.1 matérialise la répartition des tâches et des responsabilités relevant de l'accréditation et de la certification en France.

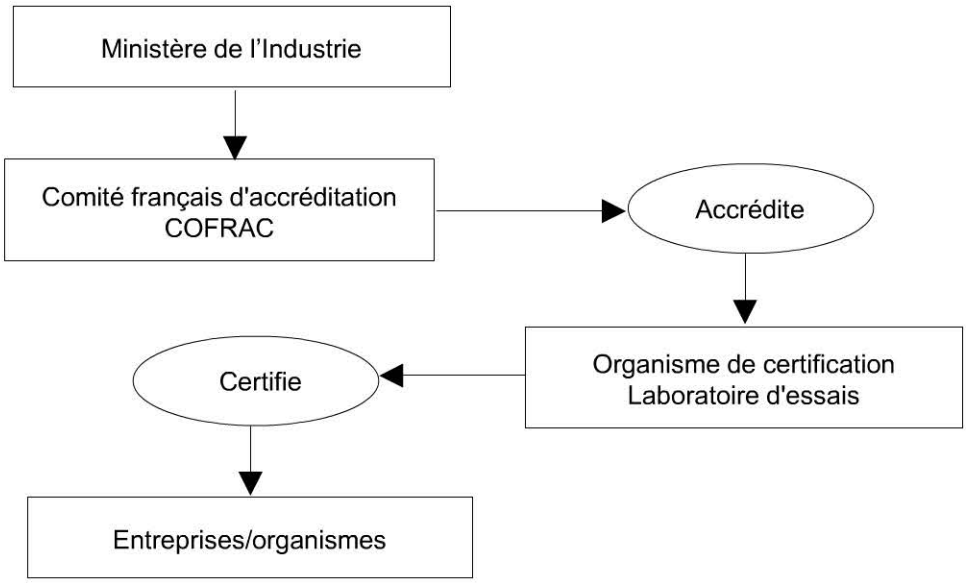


Figure 10.1 Répartition des rôles entre l'accréditation et la certification

10.2 Les acteurs les instances

10.2.1 L'ISO

L'ISO[15] (International Organization for Standardization) est une fédération internationale des organismes nationaux de normalisation.

Le travail de préparation des standards internationaux est normalement mené par les comités techniques ISO. Chaque organisme intéressé par un sujet pour lequel un comité technique a été établi, a le droit d'être représenté à ce comité.

10.2.2 CEI

La Commission Électronique Internationale[16] (CEI – en anglais IEC) s'occupe de tous les sujets qui concernent les standards électrotechniques.

15 ISO: International organization for standardization (site web à l'adresse : www.iso.ch).

16 CEI : Commission électronique internationale (site web à l'adresse : www.iec.ch).

Les standards internationaux réalisés et adoptés par les comités techniques sont distribués aux membres pour le vote. La publication en tant que standard international nécessite l'approbation d'au moins 75 % des membres participant au vote.

10.2.3 AFNOR

L'Association française de normalisation[17] est le représentant de l'ISO en France. Elle a pour mission d'animer, de coordonner l'élaboration des normes et de promouvoir leur utilisation.

10.2.4 Normes

Les normes internationales (en anglais : *standard*) sont réalisées et adoptées par les comités techniques, puis elles sont distribués aux membres pour le vote. La publication en tant que standard international nécessite l'approbation d'au moins 75 % des membres participant au vote.

10.3 Les catégories de certifications

En matière de certification, il existe trois catégories de certifications possibles que nous allons rapidement expliquer :

- la certification de produits/services ;
- la certification de personnes (certification de compétences) ;
- la certification de système.

10.4 La certification de produit/service

La certification de service a pour objectif de faire reconnaître les engagements qualité pour lequel un organisme, fournisseur de produits ou de services, s'engage à respecter vis-à-vis de ses clients/utilisateurs.

Conformément à l'article 115 du Code de la consommation, un référentiel spécifique définissant les exigences relatives au produit/service est élaboré, validé et publié au Journal Officiel.

17 AFNOR : Association française de normalisation (site web à l'adresse : www.afnor.fr).

Un audit de certification vérifie le respect des engagements et des modalités d'exécution. L'organisme de certification délivre un label qualité (par exemple NF Service). La satisfaction des clients est mesurée.

10.5 La certification de système

La certification de système atteste qu'un organisme a élaboré et mis en place un système de management. Ce système doit s'appuyer sur une volonté de la direction d'orienter les activités vers le client et la recherche de sa satisfaction. Tous les processus organisationnels de l'organisme sont formalisés et une démarche volontaire de progrès incite à rechercher l'amélioration.

Lorsque l'organisme fournisseur de produits ou de services est prêt, il demande à un organisme de certification (accrédité par le COFRAC) de venir vérifier sur place le respect des exigences édictées dans le référentiel. C'est l'audit initial de certification. Il porte sur la conformité de la documentation par rapport à la norme, et la conformité du fonctionnement par rapport au référentiel de l'organisme. Un rapport d'audit est établi qui permet de statuer à la commission de certification.

Le certificat est obtenu pour une durée de trois années.

Chaque année, un audit de suivi permet de vérifier le respect des exigences du référentiel et les améliorations réalisées.

La figure 10.2 schématise le déroulement d'une certification de système.

10.6 L'audit initial de certification

Lorsque l'organisme a déployé son système de management de la sécurité de l'information (SMSI), et qu'il s'estime prêt, il va demander à un organisme de certification accrédité sur le référentiel sécurité de l'information de procéder à un audit initial.

- Le référentiel :
  - NF ISO/CEI 27001, *Technologies de l'information – Techniques de sécurité – Système de gestion de la sécurité de l'information.*
  - NF EN ISO 19011, *Lignes directrices pour l'audit des systèmes de management.*

- Le champ de la certification :
  - Périmètre géographique : service, entreprise, domaine applicatif.
  - Possibilité d'audit combiné avec le référentiel NF EN ISO 9001 ou NF ISO/CEI 20000-1.
- Étape 1 – La préparation de l'audit :
  - un examen de la documentation en place ;
  - une visite du site ;
  - livrable : une revue documentaire ;
  - une préparation des activités d'audit ;
  - livrable : un plan d'audit.
- Étape 2 – La réalisation de l'audit sur le/les site(s) :
  - un délai de quelques jours ouvrés après la préparation ;
  - la durée d'audit sur site est fonction de la taille de l'entreprise ;
  - une réunion d'ouverture ;
  - la réalisation des interviews conformément au plan d'audit ;
  - une réunion de clôture ;
  - livrables : PV réunions d'ouverture/clôture et fiche des écarts.
- Après la réalisation de l'audit sur le/les site(s) :
  - un délai de cinq à dix jours ouvrés après la réalisation ;
  - rédaction d'un document rapport d'audit provisoire ;
  - envoi du rapport provisoire à l'entreprise auditée ;
  - réponses de l'entreprise ;
  - rédaction d'un document rapport d'audit définitif ;
  - diffusion du rapport définitif à l'entreprise auditée ;
  - délivrance du certificat pour une durée de validité de trois ans.

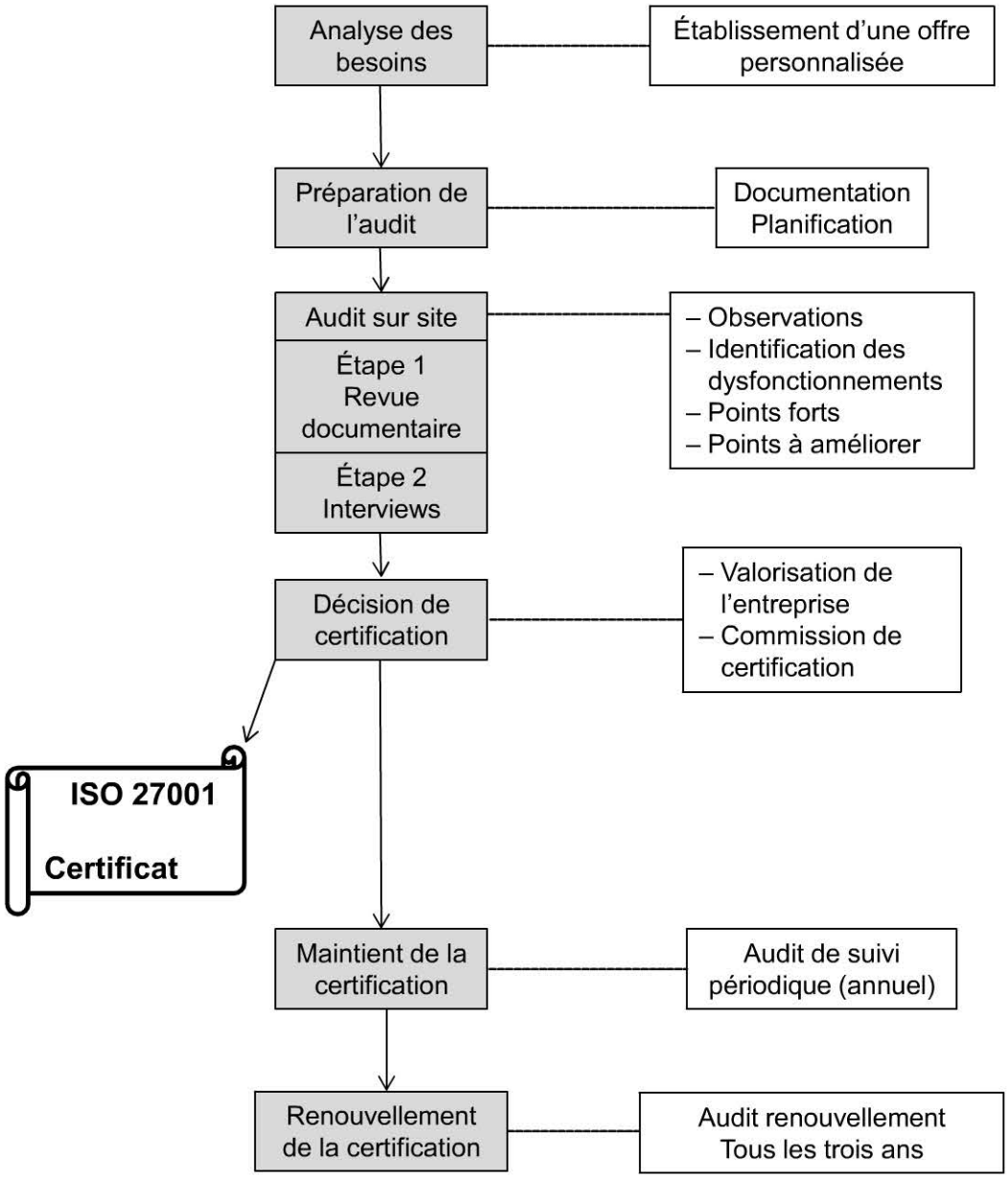


Figure 10.2 Le processus de certification de système

Conclusion

Toute organisation, quel que soit sa taille ou son domaine économique, est en permanence sujette à l'apparition d'événements. Qu'ils soient prévisibles ou inopinés, certain de ces événements ont des conséquences plus ou moins pénalisantes, voire dangereuses pour l'activité.

Ces aléas sont porteurs de risques dont la probabilité d'apparition et la force des impacts nécessitent de prendre des mesures de protection.

Dans le domaine de la sécurité de l'information, l'importance des conséquences réelles ou potentielles implique de mettre en œuvre une gestion des risques. Cette gestion des risques doit être supportée par un processus qui en garantit la maîtrise.

Le processus que nous venons d'étudier permet d'identifier les risques, d'évaluer les impacts possibles, de définir un plan de traitement de ces risques et de mettre en œuvre des actions.

Ainsi, le système de management de la sécurité de l'information déployé va permettre des actions en vue de réduire les risques jusqu'à les rendre acceptables. Et, dans le cas où un sinistre surviendrait quand même, les solutions de secours prévues et testées antérieurement permettent d'assurer une continuité (PCA) ou une reprise (PRA) de l'activité avec ses prestations de services associées.

La conformité du système de management de la sécurité de l'information (SMSI) aux exigences définies dans la norme NF ISO/CEI 27001 permet, après audit par un organisme accrédité, de délivrer un certificat qui atteste de cette conformité. Ensuite, le bénéficiaire du précieux certificat doit poursuivre l'amélioration du SMSI mis en place conformément aux principes vertueux du PDCA (*Plan*, *Do*, *Check*, *Act*). Ainsi est tracé le chemin qui conduit vers le progrès.

Partie II
Fiches techniques

Cette deuxième partie contient :

- le vocabulaire et les définitions des principaux termes normés du vocabulaire de la qualité, de la sécurité et de la certification relatifs aux technologies de l'information ;
- des fiches techniques, véritables outils complémentaires mis à la disposition du chef de projet qualité/sécurité/certification pour l'aider dans sa tâche.

Fiches techniques

◆ Fiche technique n° 1 : vocabulaire et définitions

Actif (d'après la norme NF ISO/CEI 27001)

> C'est tout élément qui représente de la valeur pour l'organisme.

Acceptation du risque (d'après la norme NF ISO/CEI 27001)

> Décision d'accepter un risque.

Analyse du risque (d'après la norme NF ISO/CEI 27001)

> Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

Appréciation du risque (d'après la norme NF ISO/CEI 27001)

> Ensemble du processus d'analyse du risque et d'évaluation du risque.

Action corrective (d'après la norme NF EN ISO 9000)

> Action visant à éliminer la cause d'une non-conformité ou d'une autre situation indésirable détectée.

Action préventive (d'après la norme NF EN ISO 9000)

> Action visant à éliminer la cause d'une non-conformité potentielle ou d'une autre situation potentielle indésirable.

Analyse du risque (d'après la norme NF ISO/CEI 27001)

> Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

Appréciation du risque (d'après la norme NF ISO/CEI 27001)

> Ensemble du processus d'analyse du risque et d'évaluation du risque.

Audit (d'après la norme NF EN ISO 9000)

> **Processus méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit (enregistrements énoncés de faits ou autres informations pertinentes et vérifiables) et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit (ensemble de politiques, procédures ou exigences utilisés comme référence) sont satisfaits.**

Confidentialité (d'après la norme NF ISO/CEI 27001)

> **C'est la propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés.**

Criticité (d'après le fascicule de documentation FD X 50-117)

> **Niveau d'importance d'un risque résultant de la combinaison des caractéristiques quantifiées du risque, à savoir sa gravité, sa probabilité d'apparition et/ou sa probabilité de détection.**

Danger (d'après le fascicule de documentation FD X 50-252)

> **Substance, objet, situation ou phénomène pouvant être à l'origine d'un dommage (ou préjudice dans certains domaines).**

Déclaration d'applicabilité – DdA (d'après la norme NF ISO/CEI 27001)

> **Déclaration documentée décrivant les objectifs de sécurité, ainsi que les mesures appropriées applicables au SMSI d'un organisme.**
>
> **NOTE : Les objectifs de sécurité et les mesures de sécurité proprement dites sont basés sur les résultats et les conclusions des processus de l'appréciation du risque et de traitement du risque, les exigences légales ou réglementaires, les obligations contractuelles et les exigences métier de l'organisme, relatives à la sécurité de l'information.**

Disponibilité (d'après la norme NF ISO/CEI 20000-1)

> **Aptitude d'un composant ou d'un service à remplir la fonction spécifiée à un moment fixé ou pendant une période de temps fixée.**

Disponibilité (d'après la norme NF ISO/CEI 27001)

> **Propriété d'être accessible et utilisable à la demande par une entité autorisée.**

Document (d'après la norme NF EN ISO 9000)

> **Support d'information et l'information (données signifiantes) qu'il contient.**

Efficacité (d'après la norme NF EN ISO 9000)

> **Niveau de réalisation des activités planifiées et d'obtention des résultats escomptés.**

Efficience (d'après la norme NF EN ISO 9000)

> **Rapport entre le résultat obtenu et les ressources utilisées.**

Enregistrement (d'après la norme NF EN ISO 9000)

> **Document spécifiant les résultats obtenus ou apportant la preuve des activités réalisées.**
>
> **Note 1 : La présente norme fait la distinction entre les enregistrements et les documents du fait que les premiers servent comme preuves des activités plutôt que comme preuves des intentions.**
>
> **Note 2 : Les rapports d'audit, les demandes de changement, les rapports d'incident, les enregistrements relatifs à la formation individuelle ainsi que les factures envoyées aux clients constituent des exemples d'enregistrements.**

Évaluation du risque (d'après la norme NF ISO/CEI 27001)

> **Processus de comparaison du risque estimé avec des critères de risque donnés pour en déterminer l'importance.**

Événement lié à la sécurité de l'information (d'après la norme NF ISO/CEI 27001)

> **Occurrence identifiée d'un état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité.**

Exigence (d'après la norme NF EN ISO 9000)

> **Besoin ou attente formulés, habituellement implicites, ou imposées.**

Gravité (d'après le fascicule de documentation FD X 50-117)

> **C'est l'ampleur des conséquences de l'événement redouté sur un actif.**

Impact (d'après la norme NF ISO/CEI 27005)

> **Changement radical au niveau des objectifs métiers atteints.**

Incident (d'après la norme NF ISO/CEI 20000-1)

> **Tout événement qui sort du cadre d'exploitation normale d'un service et qui entraîne ou peut entraîner une interruption ou une baisse de la qualité de ce service.**

Incident lié à la sécurité de l'information (d'après la norme NF ISO/CEI 27001)

> **Un ou plusieurs événements intéressant la sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information.**

Intégrité (d'après la norme NF ISO/CEI 27001)

> C'est la propriété de protection de l'exactitude et de l'exhaustivité des actifs.

Management du risque (d'après la norme NF ISO/CEI 27001)

> Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

Menace (d'après la norme ISO/CEI 27002:2005)

> Cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme.

Non-conformité (d'après la norme NF EN ISO 9000)

> Non-satisfaction d'une exigence.

Politique (d'après la norme ISO/CEI 27002:2005)

> Intentions et dispositions générales formellement exprimées par la direction.

Probabilité d'apparition (d'après le fascicule de documentation FD X 50-117)

> Degré de vraisemblance pour qu'un événement se produise.
>
> NOTE : On peut parfois utiliser la notion de « fréquence d'apparition ». Elle est tirée des expériences antérieures et correspond au nombre d'observations de la survenance d'un risque plus ou mois similaire.

Probabilité de détection (d'après le fascicule de documentation FD X 50-117)

> Degré de vraisemblance pour que les signes précurseurs liés à l'apparition de l'événement redouté puissent être détectés.

Procédure (d'après la norme NF EN ISO 9000)

> Manière spécifiée d'effectuer une activité ou un processus.

Processus (d'après la norme NF EN ISO 9000)

> Ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie.
>
> Produit/service = résultat d'un processus

Qualité (d'après la norme NF EN ISO 9000)

> Aptitude d'un ensemble de caractéristiques (trait distinctif) intrinsèques à satisfaire des exigences (besoin ou attente formulés, habituellement implicites ou imposées).

Revue (d'après la norme NF EN ISO 9000)

> **Examen entrepris pour déterminer la pertinence, l'adéquation et l'efficacité de ce qui est examiné à atteindre des objectifs définis.**

Risque (d'après la norme ISO/CEI 27002:2005)

> **La combinaison de la probabilité d'un événement et de ses conséquences.**
>
> **Risque de sécurité de l'information (d'après la norme ISO/CEI 27002:2005)**
>
> **Possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise à l'organisation.**
>
> **NOTE : Le risque est mesuré en termes de combinaison entre la vraisemblance d'un événement et de ses conséquences.**

Risque résiduel (d'après la norme NF ISO/CEI 27001)

> **Un risque résiduel est un risque qui subsiste après application du traitement à un risque.**

Sécurité de l'information (d'après la norme NF ISO/CEI 27001)

> **Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. D'autres propriétés telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.**
>
> **Système de management de la sécurité de l'information (d'après la norme NF ISO/CEI 27001)**
>
> **Partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information.**
>
> **NOTE : Le système de management inclut l'organisation, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.**

Traitement du risque (d'après la norme NF ISO/CEI 27001)

> **Processus de sélection et de mise en œuvre des mesures visant à diminuer le risque.**

Vulnérabilité (d'après la norme ISO/CEI 27002:2005)

> **La faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace.**

◆ Fiche technique n° 2 : sommaire de la norme NF ISO/CEI 27001

NF ISO/CEI 27001, *Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences* (décembre 2007)

1 – Domaine d'application

1.1 Généralités

1.2 Application

3 – Termes et définitions

2 – Références normatives

4 – SMSI

4.1 Exigences générales

4.2 Établissement et management du SMSI

4.2.1 Établissement du SMSI

4.2.2 Mise en œuvre et fonctionnement du SMSI

4.2.3 Surveillance et réexamen du SMSI

4.2.4 Mise à jour et amélioration du SMSI

4.3 Exigences relatives à la documentation

4.3.1 Généralités

4.3.2 Maîtrise des documents

4.3.3 Maîtrise des enregistrements

5 – Responsabilité de la direction

5.1 Implication de la direction

5.2 Management des ressources

5.3.1 Mise à disposition des ressources

5.3.2 Formation, sensibilisation et compétence

6 – Audits internes du SMSI

7 – Revue de direction du SMSI

7.1 Généralités

7.2 Éléments d'entrée du réexamen

7.3 Éléments de sortie du réexamen

8 – Amélioration du SMSI

8.1 Amélioration continue

8.2 Action corrective

8.3 Action préventive

◆ Fiche technique n° 3 : définition du domaine d'application

Voici des exemples d'extraits de l'annexe A de la norme NF ISO/CEI 27005 *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information* (parue en novembre 2010) :

- ▶ Présentation de l'organisme
  - ▼ Description de l'organisation.
  - ▼ Ses principaux objectifs.
  - ▼ Son activité.
  - ▼ Sa mission.
  - ▼ Ses valeurs.
  - ▼ Sa structure (organigramme).
  - ▼ Ses stratégies.
- ▶ Contraintes organisationnelles
  - ▼ Politique.
  - ▼ Stratégie.
  - ▼ Géographique.
  - ▼ Environnementale.
  - ▼ Économique.
  - ▼ Structurelle.
  - ▼ Fonctionnelle.
  - ▼ Technique.
  - ▼ RH.
  - ▼ Budgétaire.
  - ▼ …
- ▶ Références applicables
  - ▼ Législatives.
  - ▼ Réglementaires.
  - ▼ Contractuelles.
  - ▼ Autres.

◆ Fiche technique n° 4 : thèmes de la déclaration d'applicabilité

Tableau FT 4 Liste des thèmes de la déclaration d'applicabilité

Thèmes	Sous thèmes
Politique de sécurité de l'information	–
Organisation de la sécurité de l'information	Organisation interne
	Tiers
Gestion des actifs	Responsabilités relatives aux actifs
	Classification des informations
Sécurité liée aux RH	Avant le recrutement
	Pendant la durée du contrat de travail
	Fin ou modification du contrat de travail
Sécurité physique et environnementale	Zones sécurisées
	Sécurité du matériel
Gestion de l'exploitation et des télécommunications	Procédures et responsabilités liées à l'exploitation
	Gestion de la prestation de service conclue avec un tiers
	Planification et acceptation du système
	Protection contre les codes malveillants et mobiles
	Sauvegarde
	Gestion de la sécurité des réseaux
	Manipulation des supports
	Échange des informations
	Services de commerce électronique
	Surveillance
Contrôles d'accès	Exigences métier relatives au contrôle d'accès
	Gestion des accès des utilisateurs
	Responsabilités de l'utilisateur
	Contrôle d'accès réseau
	Contrôle d'accès au système d'exploitation
	Contrôle d'accès aux applications et à l'information
	Informatique mobile et télétravail

Thèmes	Sous thèmes
Acquisition, développement et maintenance des systèmes d'information	Exigences de sécurité applicables aux systèmes d'information
	Bon fonctionnement des applications
	Mesures cryptographiques
	Sécurité des fichiers système
	Sécurité en matière de développement et d'assistance technique
	Gestion des vulnérabilités techniques
Gestion des incidents liés à la sécurité de l'information	Remontée des événements et des failles liés à la sécurité de l'information
	Gestion des incidents liés à la sécurité de l'information et des améliorations
Gestion de la continuité de l'activité	–
Conformité	Conformité aux exigences légales
	Conformité avec les politiques et normes de sécurité
	Conformité technique
	Prise en compte de l'audit du système d'information

◆ Fiche technique n° 5 : exemples de catégories d'actifs

Tableau FT 5 Liste des actifs/biens (exemples)

Bâtiments – Locaux – Bureaux – Ateliers
Personnels – Compétences – Savoir-faire – Expériences
Équipements – Électrique – Climatisation – Éclairage
Matériels informatiques – Serveurs – Postes de travail
Réseaux – Matériels – Lignes – Protocoles
Logiciels – Système – Applicatifs
Bases de données – Fichiers
Documentation – Système – Applications, utilisation – Formation
Fournisseurs – Sous-traitants – Contrats
Valeurs immatérielles – Image – Réputation – Brevets
…

◆ Fiche technique n° 6 : exemple d'inventaire des actifs

Tableau FT 6 Inventaire des actifs/biens

Classe d'actif	Identifiant	Nom	Propriétaire	Description
Équipement	EQA001	Climatiseur	Services généraux	
Matériel informatique	INF 1A	Serveur A	Exploitation	
	INF 1B	Serveur B	Exploitation	
	INF 1C	Serveur C	Exploitation	
Logiciel	LS901	Unix	Exploitation	
	LS801	Oracle	Administrateur BD	
	LS802	SAP	Exploitation	
	LS701	Compta	Développement A	
	LS702	Mkg	Développement B	
	LS703	Paye	Développement C	
	LS704	Fabrication	Développement D	
Réseau	REAA	Concentrateur	Exploitation	
	REBB	Carte crypto	RSI	

◆ Fiche technique n° 7 : types de menaces

Voici des exemples de menaces (liste non exhaustive) extraits de l'annexe C de la norme NF ISO/CEI 27005, *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information* (parue en novembre 2010).

Tableau FT 7 Liste de menaces par types (exemples)

Type	Menaces
Dommages physiques	Incendie
	Dégâts des eaux
	Poussière, corrosion
	pollution
Catastrophes naturelles	Phénomène climatique
	Phénomène sismique
	Phénomène volcanique
	Phénomène météorologique
	Inondation
Perte de services essentiels	Panne de climatisation
	Perte d'alimentation électrique
	Panne de télécommunication
Perturbation due à des rayonnements	Rayonnements électromagnétiques
	Rayonnements thermiques
	Impulsions électromagnétiques
Compromission d'information	Interception de signaux
	Espionnage à distance
	Écoute
	Vol de supports ou de documents
	Vol de matériel
	Récupération de supports recyclés ou au rebut
	Divulgation
	Données provenant de sources douteuses
	Piégeage de matériel
	Piégeage de logiciel
	Géolocalisation

Type	Menaces
Défaillances techniques	Panne de matériel
	Dysfonctionnement de matériel
	Saturation du système d'information
	Dysfonctionnement du logiciel
	Violation de la maintenabilité du SI
Actions non autorisées	Utilisation non autorisée du matériel
	Reproduction frauduleuse de logiciel
	Utilisation de logiciel copié (contrefaçon)
	Corruption de données
	Traitement illégal de données
Compromission des fonctions	Erreur d'utilisation
	Abus des droits
	Usurpation de droits
	Reniement d'actions
	Violation de la disponibilité du personnel

◆ Fiche technique n° 8 : sources de menaces humaines

Voici des exemples de menaces (liste non exhaustive) extraits de l'annexe C de la norme NF ISO/CEI 27005, *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information* (parue en novembre 2010)

Tableau FT 8 Liste de menaces par catégories de sources (exemples)

Origine	Conséquences possibles
Pirate informatique	Piratage
	Intrusion
	Accès non autorisé

Origine	Conséquences possibles
Escroc informatique	Délit
	Usurpation d'identité, interception
	Corruption d'informations
	Intrusion
Terrorisme	Bombe
	Guerre de l'information
	Attaque du système
	Pénétration dans un système
	Piégeage du système
Espionnage industriel	Avantage (politique, défense)
	Exploitation économique
	Vol d'informations
	Intrusion dans la vie privée
	Pénétration dans un système
	Accès non autorisé
Employés (ex-employés)	Agression
	Chantage
	Malveillance
	Fraude et vol
	Corruption d'informations
	Saisie de données falsifiées, corrompues
	Interception
	Code malveillant (virus, cheval de Troie)
	Vente d'informations personnelles
	Bugs du système
	Sabotage du système
	Accès non autorisé

◆ Fiche technique n° 9 : vulnérabilités et menaces

Voici des exemples de vulnérabilités et de menaces (liste non exhaustive) extraits de l'annexe D de la norme NF ISO/CEI 27005, *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information* (parue en novembre 2010).

Tableau FT 9.1 Exemples pour des actifs de type matériel

Vulnérabilités	Menaces
Maintenance insuffisante	Violation de la maintenabilité
Absence de remplacement périodique	Destruction de matériel ou de support
Sensibilité à l'humidité, poussière	Corrosion
Sensibilité aux rayonnements	Rayonnements électromagnétiques
Absence de contrôle efficace de modification de configuration	Erreur d'utilisation
Sensibilité aux variations de tension	Perte d'alimentation électrique
Sensibilité aux variations de température	Phénomène météorologique
Stockage non protégé	Vol de support ou de document
Manque de prudence lors de la mise au rebut	Vol de support ou de document
Reproduction non contrôlée	Vol de support ou de document

Tableau FT 9.2 Exemples pour des actifs de type logiciel

Vulnérabilités	Menaces
Tests absents ou insuffisants	Abus de droits
Failles dans le logiciel	Abus de droits
Pas de fermeture de session en quittant le poste	Abus de droits
Mise au rebut ou réutilisation sans véritable effacement	Abus de droits
Absence de traces d'audit	Abus de droits

Attribution erronée des droits d'accès	Abus de droits
Logiciel distribué à grande échelle	Corruption de données
Application de mauvaises données	Corruption de données
Interface utilisateur compliquée	Erreur d'utilisation
Absence de documentation	Erreur d'utilisation
Réglage incorrect de paramètres	Erreur d'utilisation
Dates incorrectes	Erreur d'utilisation
Absence de mécanismes d'identification	Usurpation de droits
Mots de passe non protégés	Usurpation de droits
Activation de services non nécessaire	Traitement illégal de données
Spécifications confuses ou incomplètes	Dysfonctionnement du logiciel
Absence de contrôle des modifications	Dysfonctionnement du logiciel
Chargement et utilisation du logiciel non contrôlé	Piégeage de logiciel
Absence de copie de sauvegarde	Piégeage de logiciel
Absence de protection physique du bâtiment	Vol de supports ou de documents

Tableau FT 9.3 Exemples pour des actifs de type réseau

Vulnérabilités	Menaces
Absence de preuves d'envoi ou de réception d'un message	Reniement d'actions
Voies de communication non protégées	Écoute
Trafic sensible non protégé	Écoute
Mauvais câblage	Panne du matériel de télécommunication
Point de défaillance unique	Panne du matériel de télécommunication

Vulnérabilités	Menaces
Absence d'identification et d'authentification de l'expéditeur ou du destinataire	Usurpation de droits
Architecture réseau non sécurisée	Espionnage à distance
Transfert de mots de passe en clair	Espionnage à distance
Gestion du réseau inadaptée	Saturation du système d'information
Connexions au réseau public non protégées	Utilisation non autorisée du matériel

Tableau FT 9.4 Exemples pour des actifs de type personnel

Vulnérabilités	Menaces
Absence de personnel	Violation de la disponibilité du personnel
Procédures de recrutement inadaptées	Destruction de matériel ou de support
Formation insuffisante à la sécurité	Erreur d'utilisation
Utilisation incorrecte du logiciel et du matériel	Erreur d'utilisation
Absence de sensibilisation à la sécurité	Erreur d'utilisation
Absence de mécanisme de surveillance	Traitement illégal de données
Travail non sécurisé d'une équipe extérieure	Vol de supports ou de documents
Absence de politiques relatives à la bonne utilisation des supports de télécommunication et de messagerie	Utilisation non autorisée de matériel

◆ Fiche technique n° 10 : la disponibilité

Pour mesurer la disponibilité on utilise la formule de calcul suivante :

% temps disponible = (temps effectivement disponible/temps convenu) x 100

Avec :

Temps effectivement disponible = temps convenu – temps indisponible

Les indicateurs clés de la disponibilité sont :

- Le MTBSI (*mean time beetween system incidents*) est l'intervalle de temps entre deux incidents : MTBSI = MTTR + MTBF
- Le MTBF (*mean time beetween failures*) est l'intervalle de temps écoulé entre la reprise après un incident et l'apparition d'un autre incident. C'est le temps de disponibilité.
- Le MTTR (*mean time to repair*) est l'intervalle de temps écoulé entre l'apparition d'une panne et la reprise du service ; donc le délai nécessaire à la réparation. C'est le temps d'indisponibilité.

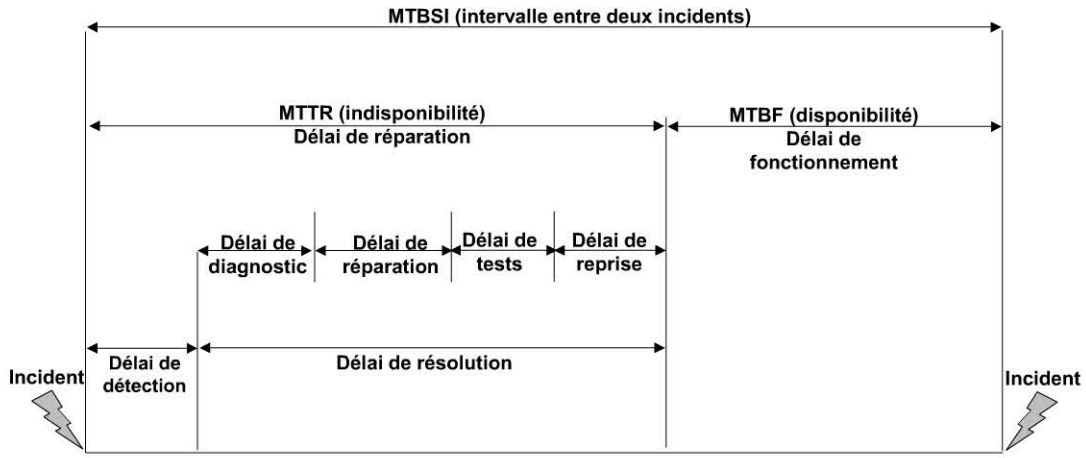


Figure FT 10 La cartographie des jalons de la disponibilité

◆ Fiche technique n° 11 : les niveaux de gravité

Voici des exemples de gravité extraits du fascicule de documentation FD X 50-117.

Tableau FT 11 Exemple de pondération des niveaux de gravité

Échelle probabilité	Ordres de grandeur indicatifs	Niveaux	
Coût du projet	Dépassement inférieur à 10 %	1	Sans impact
	Dépassement entre 10 et 20 %	2	Mineur
	Dépassement supérieur à 20 %	3	Majeur
	Dépassement supérieur à 50 %	4	Catastrophique
Délai du projet	Pas de retard significatif sur le planning	1	Sans impact
	Phasage impacté sans retard de livraison	2	Mineur
	Phasage impacté avec retard de livraison	3	Significatif
	Retard avec impact sur l'exploitation commerciale	4	Catastrophique
Performance de l'exploitation	Pas d'impact sur l'exploitation	1	Sans impact
	Nécessité de faire des maintenances rapprochées (augmentation coût d'exploitation)	2	Mineur
	Nécessité d'effectuer des modifications de conception	3	Majeur
	Exploitation impossible	4	Catastrophique

◆ Fiche technique n° 12 : probabilité des risques

Tableau FT 12 Exemple pour un projet (d'après le fascicule de documentation FD X 50-117)

Échelle de probabilité	Ordres de grandeur indicatifs	Niveaux
Probabilité	Très peu probable : inférieur à 1 chance sur 10 dans la durée du projet	1
	Peu probable : inférieur à 1 chance sur 2 dans la durée du projet	2
	Probable : supérieur à 1 chance sur 2 dans la durée du projet	3
	Quasi certain : supérieur à 9 chances sur 10 dans la durée du projet	4

◆ Fiche technique n° 13 : criticité et acceptabilité des risques

Voici un exemple de répartition de la criticité pour déterminer l'acceptabilité des risques. Cet exemple est extrait du fascicule de documentation FD X 50-117.

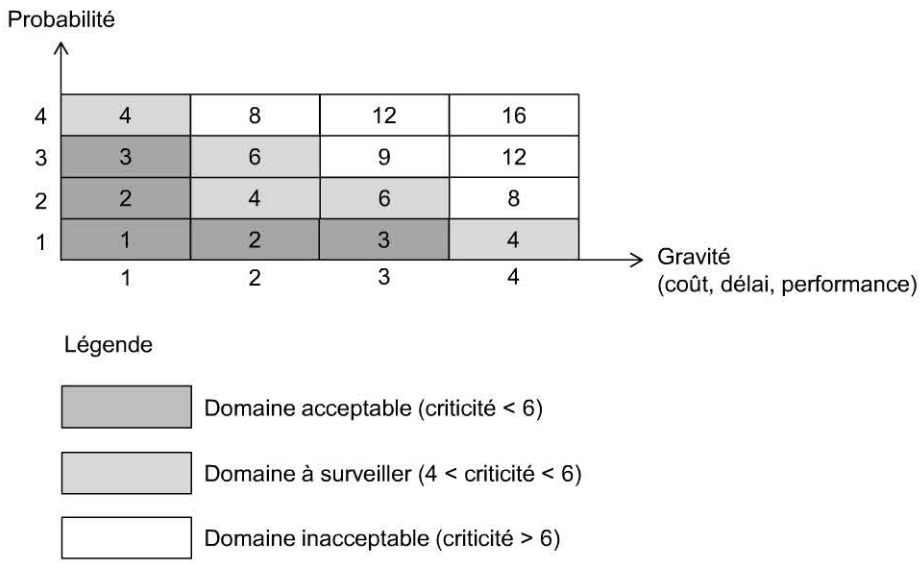


Figure FT 13 Grille de détermination de l'acceptabilité des risques

◆ Fiche technique n° 14 : la criticité des risques

Tableau FT 14 La criticité des risques sur les actifs/biens

Actif	Menace	Vulnérabilité	Disponibilité		Intégrité		Confidentialité	
			Impact	Fréquence	Impact	Fréquence	Impact	Fréquence

◆ Fiche technique n° 15 : activités de traitement des risques

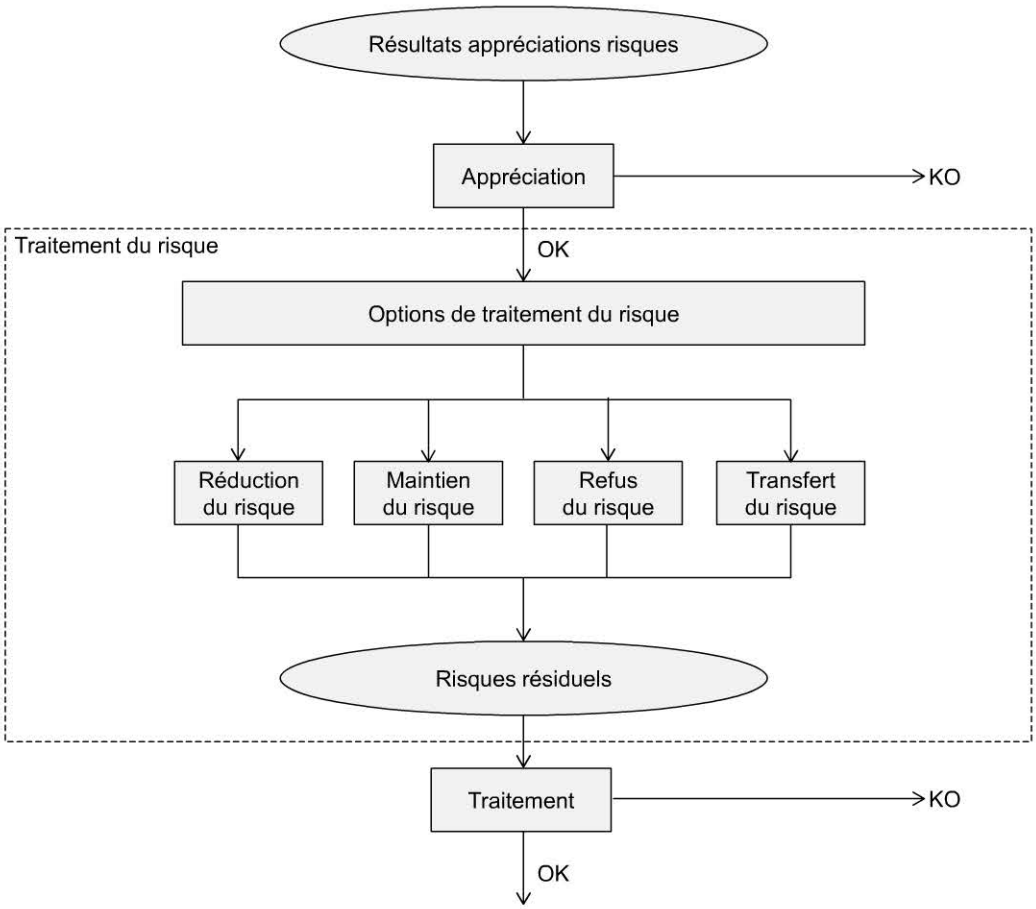


Figure FT15 Processus de traitement des risques d'après la norme NF ISO/CEI 27005

◆ Fiche technique n° 16 : exemple tableau/plan de traitement des risques

Tableau FT 16 Plan de traitement des risques

Identification					Évaluation (Avant traitement)			Traitement			Évaluation (après traitement)		
N° fiche	Description	Nature	Période active	État	Probabilité apparition	Gravité	Criticité	Actions	Pilote	Échéance	Probabilité apparition	Gravité	Criticité

◆ Fiche technique n° 17 : le processus de gestion du risque en sécurité de l'information

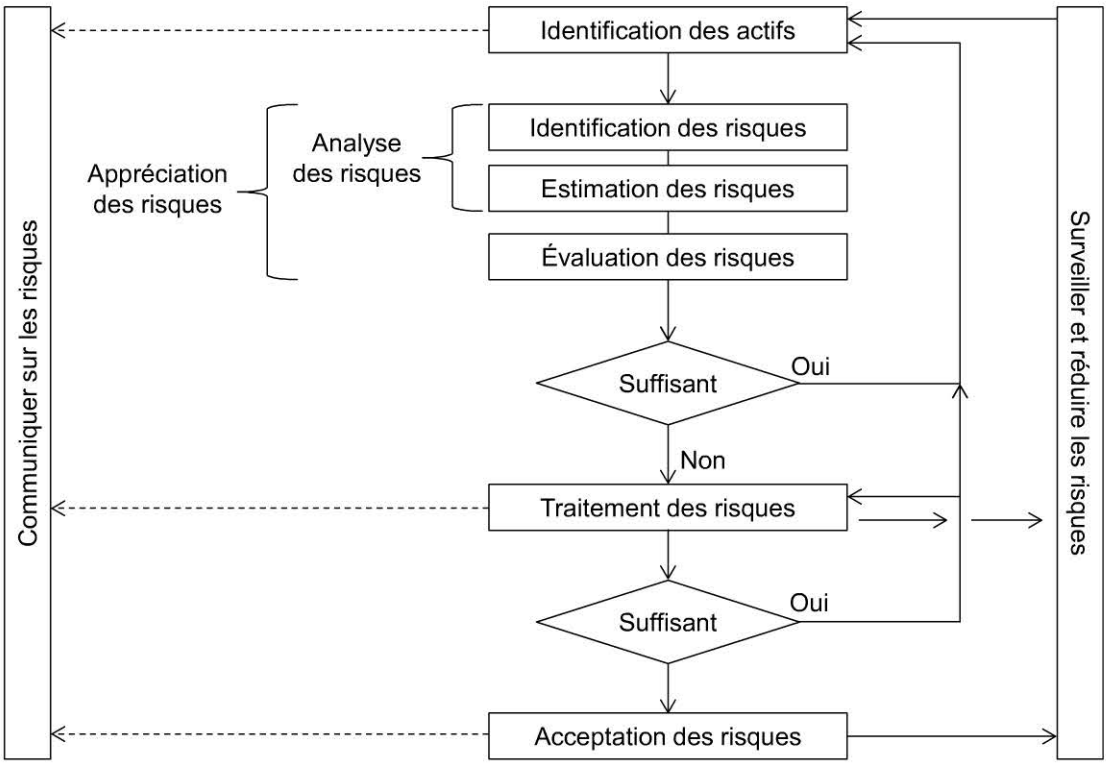


Figure FT 16 Processus de gestion des risques d'après la norme NF ISO/CEI 27005

◆ Fiche technique n° 18 : management du risque

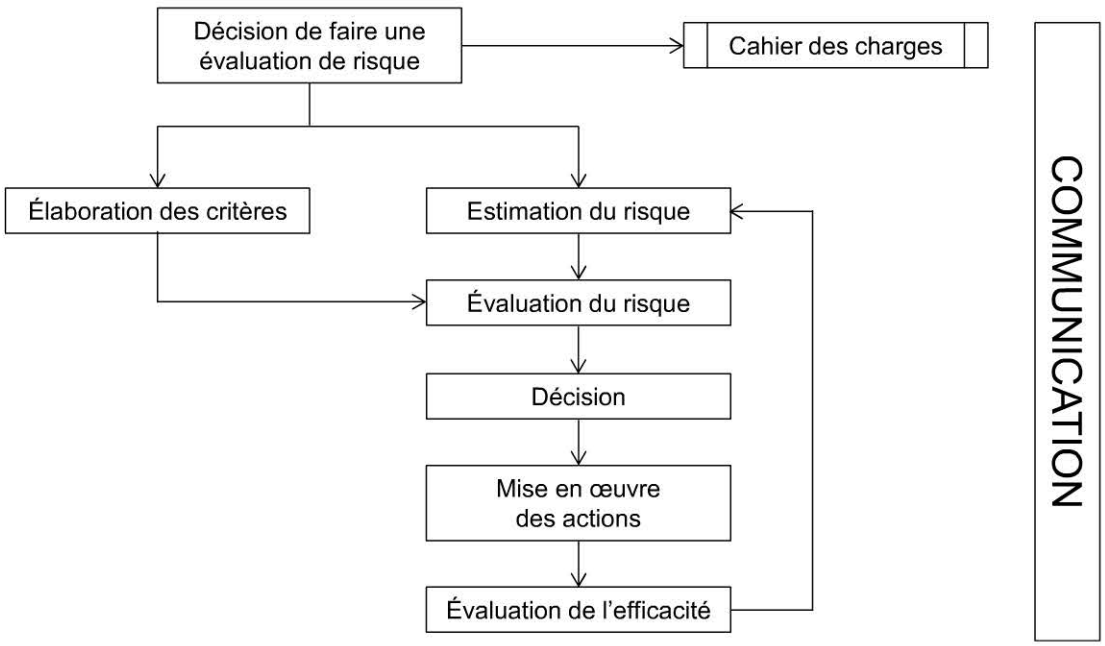


Figure FT 18 A Processus de management du risque d'après le fascicule de documentation FD X 50-252

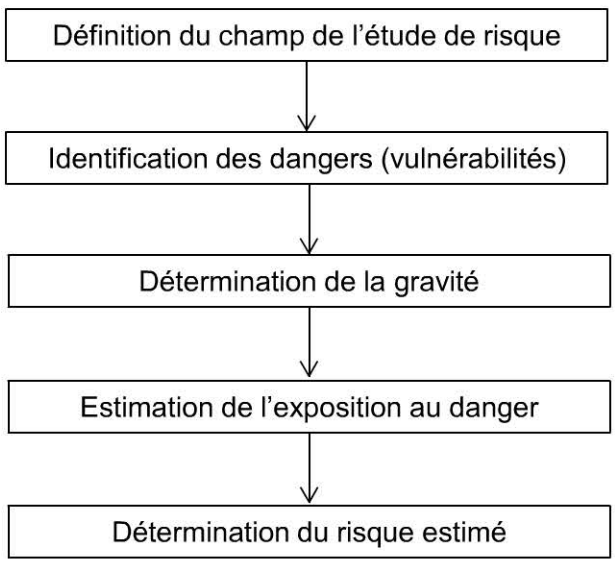


Figure FT 18 B Détail de l'estimation du risque d'après le fascicule de documentation FD X 50-252

◆ Fiche technique n° 19 : exemple de pondération de probabilité d'un danger

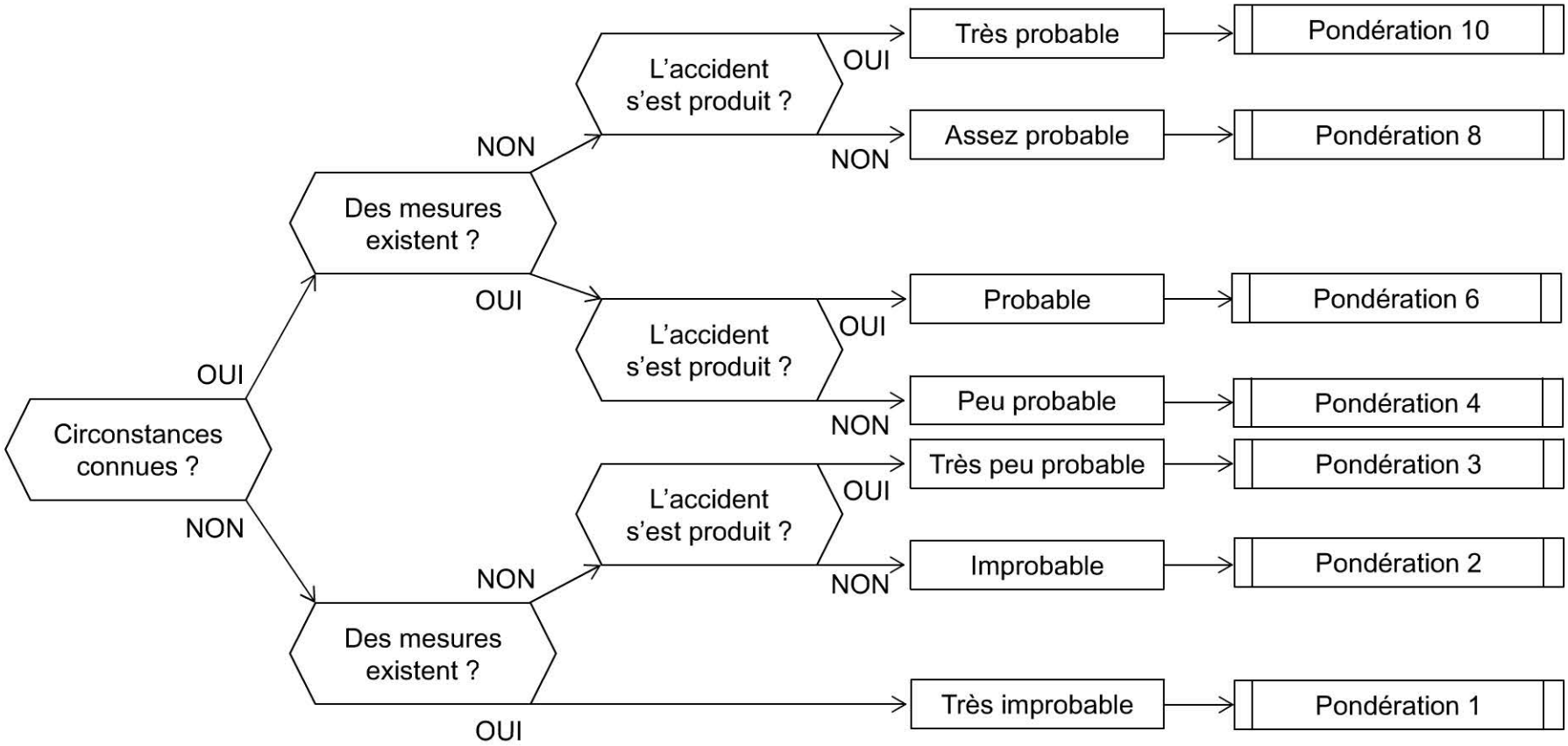


Figure FT 19 Exemple d'après le fascicule de documentation FD X 50-252

◆ Fiche technique n° 20 : exemple de pondération de la fréquence d'exposition à un danger

Voici un exemple de pondération de la fréquence d'exposition à un danger. Cet exemple est extrait du fascicule de documentation FD X 50-252.

Tableau FT 20 Grille de pondération en fonction de la fréquence d'exposition à un danger

	Occasionnelle	Intermittente	Fréquente	Permanente
Jour	< 30 mn	30 < t < 120 mn	2 h < t < 6 h	> 6 h
Semaine	< 2 h	2 h < t < 8 h	1 j < t < 3 j	> 3 j
Mois	< 1 jour	1 J < t < 6 j	6 j < t < 15 j	> 15 j
Année	< 15 jours	15 j < t < 2 mois	2 mois < t < 5 mois	> 5 mois
Pondération	1	2	3	4

◆ Fiche technique n° 21 : la gestion des incidents

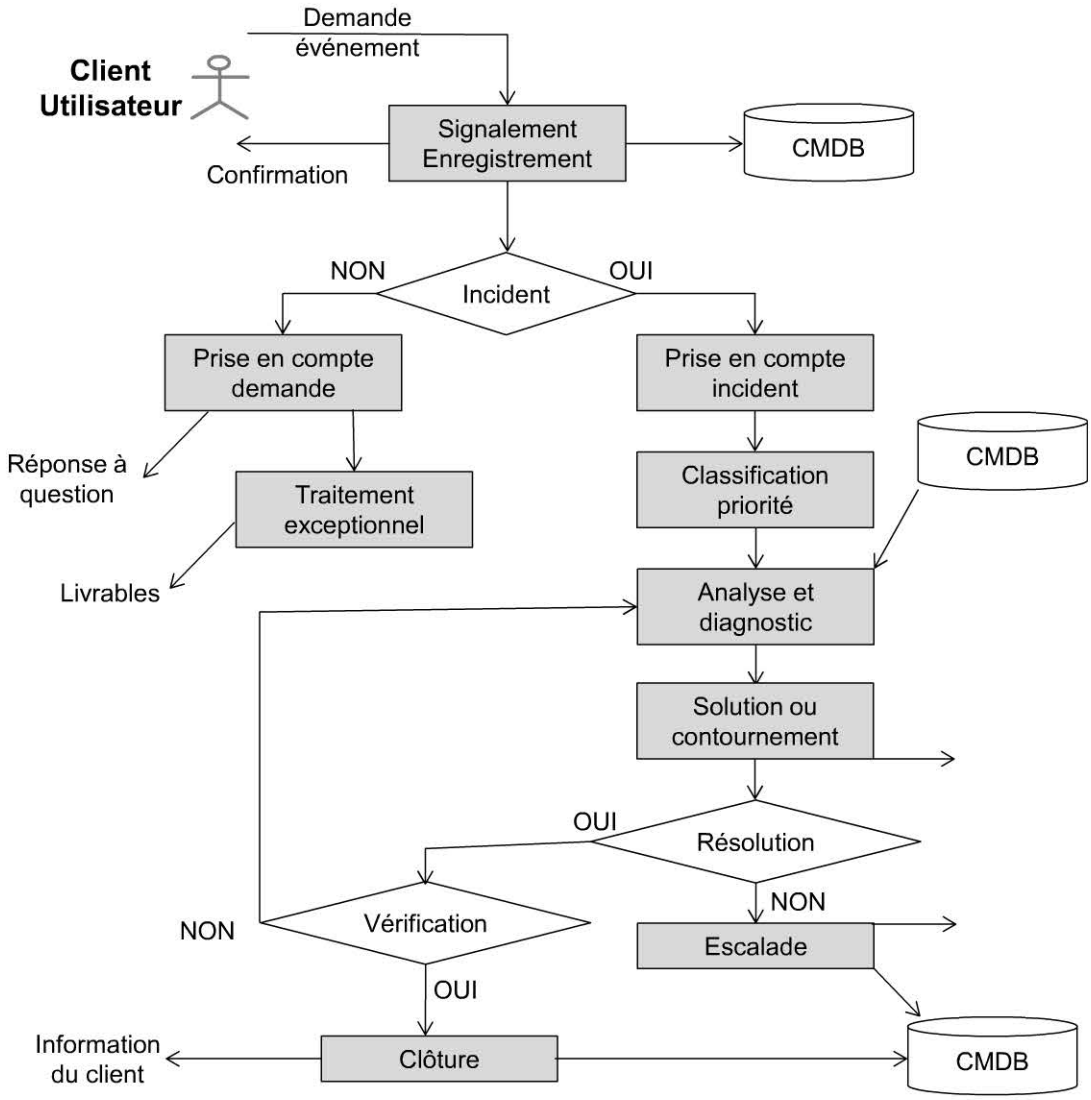


Figure FT 21 Le logigramme de traitement des incidents

◆ Fiche technique n° 22 : le plan de reprise (continuité)

Sommaire de plan de reprise générique

Introduction :

Mise à jour : Procédure de mise à jour du plan.

Classification des sinistres : Gravité, durée, dommages.

Déclenchement : Moment et conditions.

Destinataires : Liste du personnel concerné

Sections spécialisées :

Administration.

Infrastructure informatique.

Personnel.

Sécurité.

Sites de reprise.

Restauration/rétablissement.

Procédures :

– ….

– ….

– ….

– ….

◆ Fiche technique n° 23 : le Manuel de Management de la Sécurité de l'Information

Le Manuel de Management de la Sécurité de l'Information est le document décrivant les dispositions générales prises par l'entreprise pour obtenir la sécurité de l'information et satisfaire aux objectifs fixés. Pour faciliter la revue documentaire, nous recommandons le plan type suivant qui est calé sur le plan des exigences de la norme internationale ISO/IEC 27001.

Plan type d'un Manuel de Management de la Sécurité

En préambule, la déclaration de la direction générale.

Chapitre 1 : Le contexte, présentation de l'entreprise

- Les activités.
- Le(s) marché(s).
- Les ressources.
- Les chiffres clés.
- L'organigramme.
- Les produits ou services offerts aux clients.

Chapitre 2 : Les références normatives

Chapitre 3 : Le vocabulaire et les définitions

Chapitre 4 : Le système de gestion de la sécurité de l'information

LE SMSI

- L'établissement du SMSI
- La mise en œuvre et le fonctionnement du SMSI
- La surveillance et le réexamen du SMSI
- La mise à jour et l'amélioration du SMSI

La documentation

- La maîtrise des documents
- La maîtrise des enregistrements

Chapitre 5 : La responsabilité de la direction

- L'implication de la direction
- Le management des ressources
  - La mise à disposition des ressources
    - La formation,
    - La sensibilisation,
    - Les compétences.

Chapitre 6 : Les audits internes du SMSI

Chapitre 7 : La revue de direction du SMSI

- Les éléments d'entrée du réexamen
- Les éléments de sortie du réexamen

Chapitre 8 : L'amélioration du SMSI

L'amélioration continue

Les actions correctives

Les actions préventives

◆ Fiche technique n° 24 : description de la fonction de monsieur Sécurité – *risk manager*

▶ Pour réussir dans l'exercice de cette fonction, le titulaire du poste doit démontrer son aptitude au regard des compétences suivantes :

- ▼ de l'expérience ;
- ▼ une bonne connaissance de l'organisme ;
- ▼ un esprit analytique ;
- ▼ des aptitudes à communiquer ;
- ▼ une expertise sur le domaine de la sécurité.

▶ Les principales missions confiées à monsieur sécurité concernent les activités suivantes :

- ▼ identifier, analyser, évaluer les risques ;
- ▼ proposer des actions préventives et correctives ;
- ▼ vérifier le suivi et l'efficacité des actions ;
- ▼ s'assurer de la conservation des enregistrements ;
- ▼ communiquer sur les risques ;
- ▼ sensibiliser et former les acteurs à la problématique de gestion des risques.

▶ La déclinaison opérationnelle de ces missions confiées à monsieur sécurité va se traduire en différentes tâches. Parmi les plus courantes, nous pouvons citer les tâches suivantes :

- ▼ définir, entretenir et tenir à jour le SMSI ;
- ▼ participer avec la direction à la définition des objectifs de sécurité ;
- ▼ entretenir le niveau de sensibilisation et de formation des acteurs ;

- être responsable de la tenue et de la gestion des indicateurs (tableau de bord des risques) ;
- communiquer sur la gestion des risques ;
- assurer la veille réglementaire et technique sur le thème des risques.

◆ Fiche technique n° 25 : l'amélioration continue

➢ Le principe

Les améliorations se déroulent selon le principe du PDCA (*Plan, Do, Check, Act*). Ce principe est matérialisé par la figure FT 25 appelée « roue de Deming[18] ».

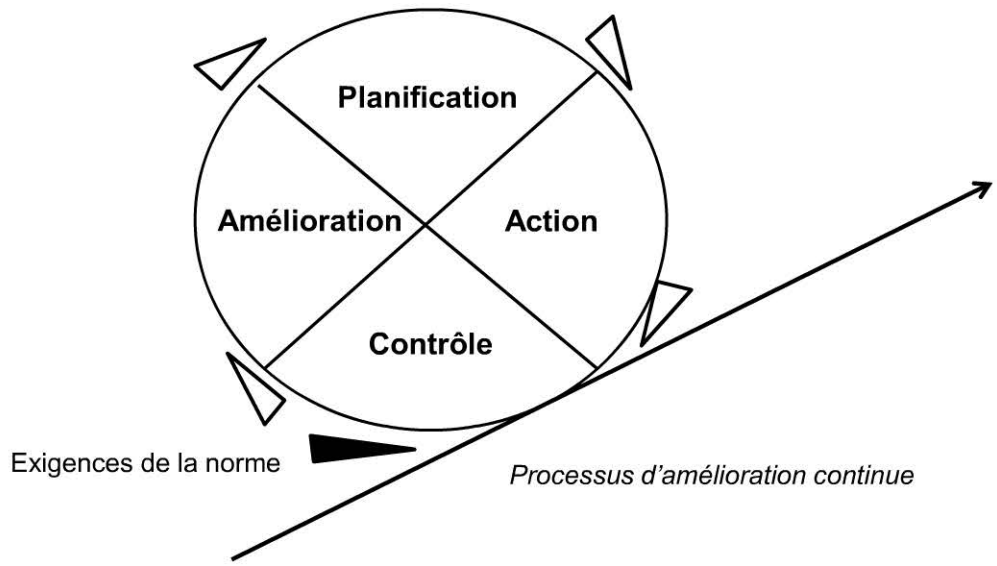


Figure FT 25 La roue de Deming

18 William Edwards Deming (1900-1993) a été un chercheur en mathématiques au ministère américain de l'Agriculture et un expert en échantillonnage au Bureau américain du recensement. Le prix japonais de la Qualité porte aussi son nom.

◆ Fiche technique n° 26 : la gestion de l'amélioration

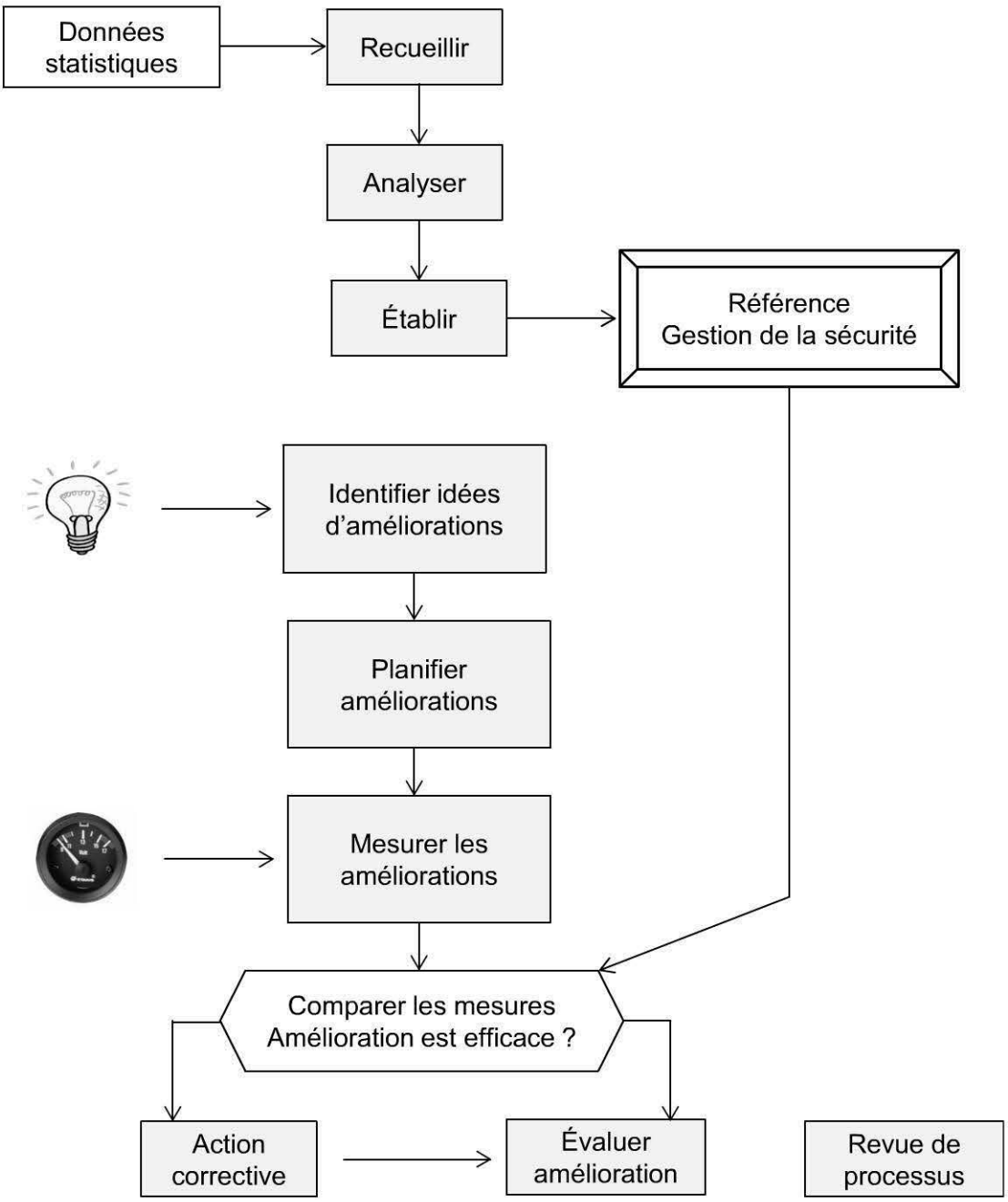


Figure FT 26 Le logigramme de traitement de l'amélioration continue

◆ Fiche technique n° 27 : quelques méthodes pour les risques

Voici une liste non limitative de quelques méthodes de référence en matière de gestion des risques :

- EBIOS (Expression des besoins et identification des objectifs de sécurité) maintenue par la Direction Centrale de la sécurité des Systèmes d'Information (DCSSI) ;
- MEHARI (Méthode d'analyse de risque) développée par le CLUSIF[19] ;
- NF ISO 31000, *Management du risque – Principes et lignes directrices*.
- NF ISO/CEI 27005, *Technologies de l'information – Techniques de sécurité – Gestion des risques en sécurité de l'information*.

◆ Fiche technique n° 28 : une règle d'or pour la sécurité

Sécurité informatique – Les 10 règles d'or

1. Mon mot de passe est confidentiel et personnel.
2. Mes données professionnelles sont stockées sur le serveur et sauvegardées dans les répertoires adéquats.
3. Mon poste est verrouillé lorsque je m'absente.
4. J'évite de connecter des clés USB de personnes tierces et je suis vigilant face aux pièces jointes.
5. Je respecte le niveau de confidentialité des informations et le secret des correspondances.
6. Je limite l'utilisation d'Internet à un usage strictement professionnel.
7. Je m'assure que mes données sensibles sont protégées.
8. Je ne modifie pas les réglages de sécurité de mon ordinateur.
9. Je ne fais pas suivre automatiquement mes messages sur une boîte externe.
10. Je n'hésite pas à m'adresser à mon correspondant SSI.

19 http://www.clusif.asso.fr/

Sigles et abréviations

AFNOR	Association française pour la normalisation
AFAQ	Association française pour l'assurance qualité
CEI/IEC	Comité électronique et informatique
COFRAC	Comité français d'accréditation
ISO	International standard organization
SMSI	Système de management de la sécurité de l'information

Normes et standards

La liste ci-dessous résume les principales normes internationales sur le thème de la gestion de la qualité.

ISO 9000:2005, *Systèmes de management de la qualité – Principes essentiels et vocabulaire.*

ISO 9001:2008, *Systèmes de management de la qualité – Exigences.*

ISO 9004:2009, *Gestion des performances durables d'un organisme – Approche de management par la qualité.*

ISO 14001:2004, *Systèmes de management environnemental – Exigences et lignes directrices pour son utilisation.*

NF EN ISO 19011, *Lignes directrices pour l'audit des systèmes de management.*

La liste ci-dessous résume les principales normes sur le thème de la qualité des prestations de service informatique (information technology).

ISO/CEI 20000-1:2011, *Technologies de l'information – Gestion des services – Partie 1 : exigences du système de gestion des services.*

ISO/CEI 20000-2:2012, *Technologies de l'information – Gestion des services – Partie 2 : directives relatives à l'application des systèmes de management des services.*

ISO/CEI TR 20000-3:2009, *Technologies de l'information – Gestion des services – Partie 3 : directives pour la définition du domaine d'application et l'applicabilité de l'ISO/CEI 20000-1.*

ISO/CEI TR 20000-5:2010, *Technologies de l'information – Gestion des services – Partie 5 : exemple de plan de mise en application pour l'ISO/CEI 20000-1.*

La liste ci-dessous résume les principales normes et fascicules de documentation sur le thème du risque :

FD ISO GUIDE 73, *Management du risque – Vocabulaire.*

NF ISO 31000, *Management du risque – Principes et lignes directrices.*

FD X 50-117, *Management de projet – Gestion du risque – Management des risques d'un projet.*

FD X 50-252, *Management du risque – Lignes directrices pour l'estimation des risques.*

La liste ci-dessous résume les principales normes sur le thème de la sécurité de l'information :

NF ISO/CEI 27000, *Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Vue d'ensemble et vocabulaire.*

NF ISO/IEC 27001, *Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Exigences.*

ISO/IEC 27002:2005, *Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de sécurité d'information (ISO/CEI 17799:2005 et rectificatif 1 de 2007).*

ISO/IEC 27003:2010, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information.*

ISO/IEC 27004:2009, *Technologies de l'information – Techniques de sécurité – Management de la sécurité de l'information – Mesurage.*

NF ISO/IEC 27005, *Technologies de l'information – Techniques de sécurité – Système de management de la sécurité de l'information – Gestion des risques en sécurité de l'information.*

ISO/IEC 27006:2011, *Technologies de l'information – Techniques de sécurité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information.*

ISO/IEC 27011:2008, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour le management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002.*

Adresses sites internet

Association française de normalisation (AFNOR) : http://www.afnor.fr

Organisation internationale de normalisation (ISO) : http://www.iso.ch

Commission électronique internationale (CEI) : http://www.iec.ch

International Register of Certificated Auditors : http://www.irca.org

Agence nationale de la sécurité des systèmes d'information

Présentation EBIOS :
http://www.securite-informatique.gouv.fr/gp_article82.html

Documents accessibles gratuitement sur le site : http://www.ssi.gouv.fr/ebios

Club EBIOS (communauté des experts en gestion de la sécurité :

http://www.club-ebios.org/

Club de la sécurité de l'information français : http://www.clusif.asso.fr

http://www.clusif.asso.fr/fr/production/mehari/

CPI Conseil : http://cpi.conseil.free.fr/

Table des figures et des tableaux

Bibliographie

Du même auteur chez AFNOR Éditions

Basic easy, Découverte de la qualité, 2010.

10 clés pour réussir sa certification ISO 9001 – Version 2008, 2009.

10 clés pour réussir sa certification QSE, ISO 9001, OHSAS 18001, ISO 14001, 2009.

10 clés pour la gestion des services, de l'ITIL à l'ISO 20000, 2007.

10 clés pour réussir sa certification IS0 9001, 2006.

Sous la direction de C. Pinet (Groupe des experts qualité du CNAM), *La Qualité du logiciel – Retour d'expériences*, 1998.

Du même auteur chez d'autres éditeurs

Les référentiels normatifs – Gestion du cycle de vie du logiciel, Techniques de l'ingénieur, Collection « INFORMATIQUE H 4031 », 2012.

Les référentiels normatifs – Produit logiciel, Techniques de l'ingénieur, Collection « INFORMATIQUE H 4029 », 2011.

Les référentiels normatifs – Processus d'ingénierie informatique, Techniques de l'ingénieur, Collection « INFORMATIQUE H 4028 », 2011.

ITIL® et ISO 20000 Comment bien préparer sa certification de prestations de service I.T., Techniques de l'ingénieur, Collection « INFORMATIQUE H 3280 – ITIL et ISO 20000 / HB – Technologies logicielles – Architectures des systèmes », 2010.

Évaluation de processus logiciel, Techniques de l'ingénieur, Collection « INFORMATIQUE H 9 010 », 2005.

Processus d'ingénierie du logiciel. Méthodes et qualité, Pearson Éducation, 2002.

Qualité du logiciel : les Référentiels normatifs, Techniques de l'ingénieur, Collection « INFORMATIQUE H 4 028 », 2001.

Contributions (classeur à feuillets mobiles)

Certification ISO 9000, AFNOR Éditions, 2001-2005.

10 clés pour la sécurité de l'information

ISO/CEI 27001

Notre environnement quotidien est de plus en plus complexe et donc de plus en plus difficile à comprendre. Techniques et outils de plus en plus sophistiqués apparaissent et se développent.

Toute organisation, avant d'entreprendre une action quelle qu'elle soit, doit se poser la question de l'évaluation des conséquences que celle-ci est susceptible d'entraîner. Et c'est probablement dans le domaine de l'information que l'impact des décisions et des actions peut s'avérer le plus difficile à appréhender. Or, l'absence de maîtrise des risques liés à la sécurité de l'information peut avoir de lourdes répercussions.

Dans cet ouvrage, Claude Pinet fait œuvre utile et s'adresse d'une part à tous les intervenants liés au système d'information, et d'autre part à tout utilisateur afin d'améliorer la confiance dans les informations véhiculées. Il détaille et explique la structure et le contenu de la série des normes ISO/CEI 27000, qui traitent de la sécurité de l'information, sans oublier de les replacer dans leur contexte. Il montre comment ces normes, bien comprises et bien mises en œuvre, constituent le référentiel pour l'élaboration et la certification d'un système de management de la sécurité de l'information (SMSI).

ISBN : 978-2-12-465381-2
www.afnor.org/editions

9 782124 653812