NORME INTERNATIONALE

ISO/CEI 27005

Première édition
2008-06-15

Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information

Information technology — Security techniques — Information security risk management

Numéro de référence
ISO/CEI 27005:2008(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2010

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27005 a été élaborée par le comité technique ISO/TC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette première édition de l'ISO/CEI 27005 annule et remplace l'ISO/CEI TR 13335-3:1998 et l'ISO/CEI TR 13335-4:2000, dont elle constitue une révision technique.

Introduction

La présente Norme internationale contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans une organisation, qui viennent notamment en appui des exigences d'un SMSI (système de management de la sécurité de l'information) tel que défini dans l'ISO/CEI 27001. Cependant, la présente Norme internationale ne fournit aucune méthodologie spécifique à la gestion des risques en sécurité de l'information. Il est du ressort de chaque organisation de définir son approche de la gestion des risques, en fonction, par exemple, du périmètre du SMSI, de ce qui existe dans l'organisme dans le domaine de la gestion des risques, ou encore de son secteur industriel. Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit dans la présente Norme internationale pour appliquer les exigences du SMSI.

La présente Norme internationale s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'une organisation et, le cas échéant, aux tiers prenant part à ces activités.

Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information

1 Domaine d'application

La présente Norme internationale contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

La présente Norme internationale vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001; elle est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.

Il est important de connaître les concepts, les modèles, les processus et les terminologies décrites dans l'ISO/CEI 27001 et l'ISO/CEI 27002 afin de bien comprendre la présente Norme internationale.

La présente Norme internationale est applicable à tous types d'organisations (par exemple les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif) qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisation.

2 Références normatives

Les documents de référence suivants sont indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence (y compris les éventuels amendements) s'applique.

ISO/CEI 27001:2005, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

ISO/CEI 27002:2005, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 27001, l'ISO/CEI 27002 et les suivants s'appliquent.

3.1
impact
changement radical au niveau des objectifs métiers atteints

3.2
risque de sécurité de l'information
possibilité qu'une menace donnée exploite les vulnérabilités d'un actif ou d'un groupe d'actifs et nuise donc à l'organisation

NOTE Le risque est mesuré en termes de combinaison entre la vraisemblance d'un événement et ses conséquences.

3.3
refus du risque
décision de se retirer d'une situation à risque, ou de ne pas s'y engager

[ISO/CEI Guide 73:2002]

3.4
communication relative aux risques
échange ou partage de l'information concernant un risque entre le décideur et les autres parties prenantes

[ISO/CEI Guide 73:2002]

3.5
estimation des risques
processus utilisé pour affecter des valeurs à la probabilité et aux conséquences d'un risque

[ISO/CEI Guide 73:2002]

NOTE 1 Dans le cadre de la présente Norme internationale, le terme «activité» est utilisé en lieu et place du terme «processus» pour l'estimation des risques.

NOTE 2 Dans le cadre de la présente Norme internationale, le terme «vraisemblance» est utilisé en lieu et place du terme «probabilité» pour l'estimation des risques.

3.6
identification des risques
processus utilisé pour trouver, lister et caractériser les éléments à risque

[ISO/CEI Guide 73:2002]

NOTE Dans le cadre de la présente Norme internationale, le terme «activité» est utilisé en lieu et place du terme «processus» pour l'identification des risques.

3.7
réduction du risque
mesures prises pour diminuer la probabilité, les conséquences négatives, ou les deux à la fois, associées à un risque

[ISO/CEI Guide 73:2002]

NOTE Dans le cadre de la présente Norme internationale, le terme «vraisemblance» est utilisé en lieu et place du terme «probabilité» pour la réduction du risque.

3.8
maintien du risque
acceptation du poids de la perte ou du bénéfice de gain découlant d'un risque particulier

[ISO/CEI Guide 73:2002]

NOTE Dans le cadre des risques en sécurité de l'information, seules les conséquences négatives (pertes) sont prises en compte pour le maintien du risque.

3.9
transfert du risque
partage avec un tiers du poids de la perte ou du bénéfice de gain découlant d'un risque

[ISO/CEI Guide 73:2002]

NOTE Dans le cadre des risques en sécurité de l'information, uniquement les conséquences négatives (pertes) sont prises en compte pour le transfert du risque.

4 Structure de la présente Norme internationale

La présente norme contient la description du processus de gestion des risques en sécurité de l'information, et la description de ses activités.

Les informations générales sont fournies dans l'Article 5.

Un aperçu général du processus de gestion des risques en sécurité de l'information est donné dans l'Article 6.

Toutes les activités liées à la gestion des risques en sécurité de l'information, telles que présentées dans l'Article 6, sont ensuite décrites dans les articles suivants:

- établissement du contexte dans l'Article 7;
- appréciation des risques dans l'Article 8;
- traitement des risques dans l'Article 9;
- acceptation des risques dans l'Article 10;
- communication relative aux risques dans l'Article 11;
- surveillance et revue du risque dans l'Article 12.

Des informations supplémentaires relatives aux activités de gestion des risques en sécurité de l'information sont présentées dans les annexes. L'établissement du contexte est abordé dans l'Annexe A (Définition du domaine d'application et des limites du processus de gestion des risques en sécurité de l'information). L'identification, la valorisation des actifs et l'appréciation des impacts sont traitées dans l'Annexe B (exemples d'actifs), dans l'Annexe C (exemples de menaces type) et dans l'Annexe D (exemples de vulnérabilités type).

Des exemples d'approches relatives à l'appréciation des risques en sécurité de l'information sont présentés dans l'Annexe E.

Les contraintes liées à la réduction du risque sont traitées dans l'Annexe F.

Toutes les activités liées à la gestion des risques, présentées dans les Articles 7 à 12, sont structurées de la manière suivante:

Élément(s) d'entrée: Identifie toute information requise pour réaliser l'activité.

Action: Décrit l'activité.

Préconisations de mise en œuvre: Propose des préconisations pour réaliser l'action. Il se peut que certaines préconisations ne soient pas adaptées à tous les cas, et que d'autres solutions pour réaliser l'action s'avèrent préférables.

Élément(s) de sortie: Identifie toute information obtenue après la réalisation de l'activité.

5 Contexte

Une approche systématique de la gestion des risques en sécurité de l'information est nécessaire pour identifier les besoins organisationnels concernant les exigences en matière de sécurité de l'information, et pour créer un système de management de la sécurité de l'information (SMSI) efficace. Il convient que cette approche soit adaptée à l'environnement de l'organisation, et soit notamment alignée sur la démarche générale de gestion des risques de l'entreprise. Il convient que les efforts effectués en matière de sécurité adressent les risques de manière efficace et opportune quand et lorsque cela est nécessaire. Il convient que la gestion des risques en sécurité de l'information fasse partie intégrante de l'ensemble des activités de management de la sécurité de l'information et qu'elle s'applique à la fois à la mise en œuvre et au fonctionnement d'un SMSI.

Il convient que la gestion des risques en sécurité de l'information soit un processus continu. Il convient que ce processus établisse le contexte, apprécie les risques et les traite à l'aide d'un plan de traitement des risques permettant de mettre en œuvre les recommandations et décisions. La gestion des risques analyse les évènements susceptibles de se produire ainsi que leurs possibles conséquences avant de décider de ce qui pourrait être fait, dans quels délais et à quel moment, pour réduire les risques à un niveau acceptable.

Il convient que la gestion des risques en sécurité de l'information contribue é ce qui suit:

- l'identification des risques
- l'appréciation des risques en termes de conséquences sur les activités métier et de vraisemblance
- la communication et la compréhension de la vraisemblance et des conséquences de ces risques
- l'établissement d'un ordre de priorité pour le traitement des risques
- la définition des priorités d'actions afin de réduire les occurrences des risques
- l'implication des parties prenantes lors de la prise de décisions relatives à la gestion des risques et l'information sur l'état de la gestion des risques
- l'efficacité de la supervision du traitement des risques
- la surveillance et la revue régulières des risques et du processus de gestion des risques
- la capture de l'information afin d'améliorer l'approche de gestion des risques
- la formation des dirigeants et du personnel sur les risques et les actions à entreprendre pour les atténuer

Le processus de gestion des risques en sécurité de l'information peut s'appliquer à l'organisation dans son ensemble, à toute partie distincte de l'organisation (à titre d'exemples un département, un lieu physique, un service), à tout système d'information existant ou prévu, ou à des types particuliers de mesures de sécurité (par exemple la planification de la continuité d'activité).

6 Présentation générale du processus de gestion des risques en sécurité de l'information

Le processus de gestion des risques en sécurité de l'information comprend l'établissement du contexte (Article 7), l'appréciation des risques (Article 8), le traitement des risques (Article 9), l'acceptation des risques (Article 10), la communication relatives aux risques (Article 11), ainsi que la surveillance et la revue du risque (Article 12).

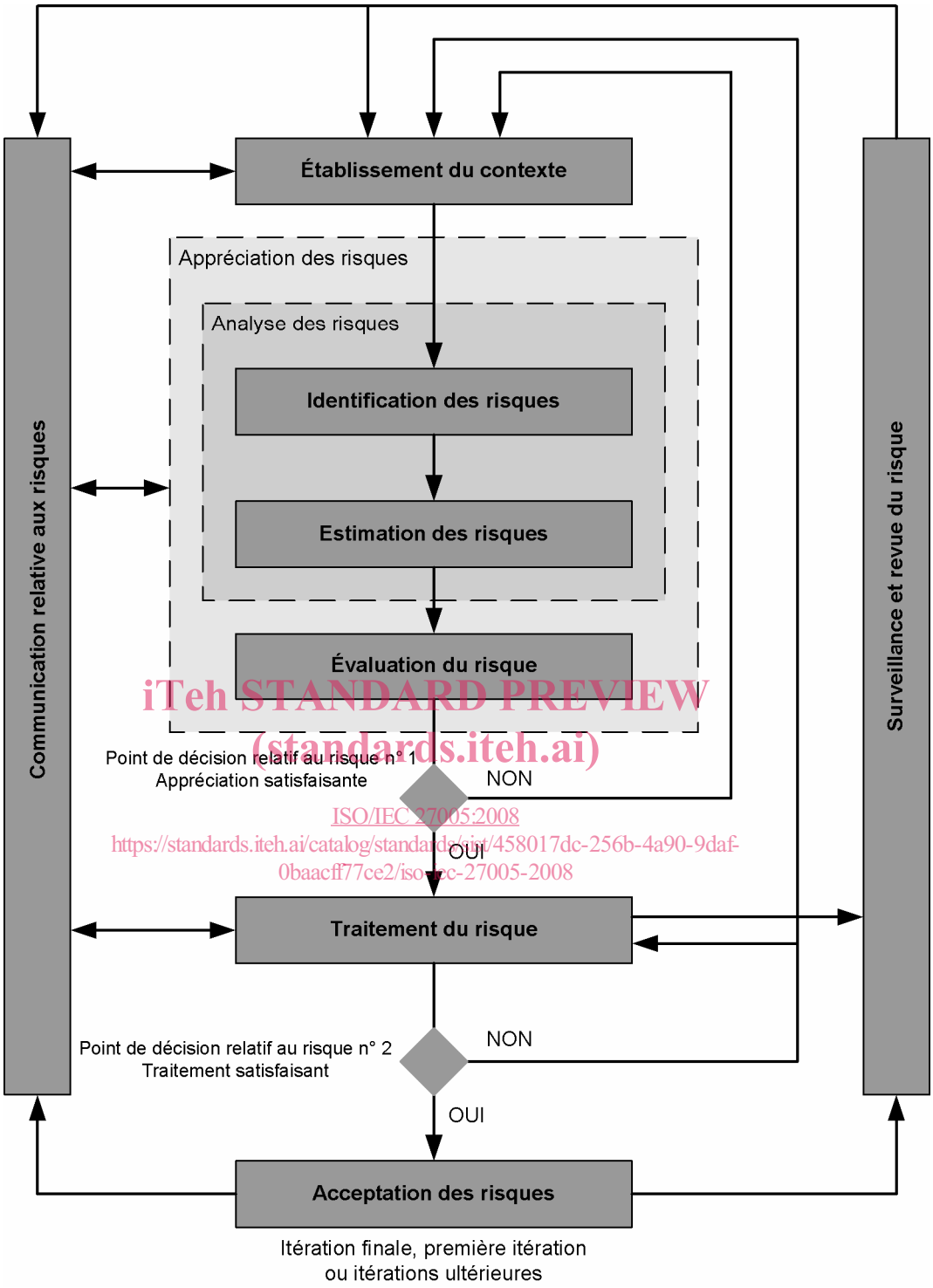

Figure 1 — Processus de gestion des risques en sécurité de l'information

Comme l'illustre la Figure 1, le processus de gestion des risques en sécurité de l'information peut être itératif pour les activités d'appréciation et/ou de traitement des risques. Une approche itérative de conduite de l'appréciation des risques permet d'approfondir et de préciser l'appréciation à chaque itération. Cette approche itérative assure un bon équilibre entre la minimisation du temps et des efforts investis dans l'identification des mesures de sécurité et l'assurance que les risques élevés sont correctement appréciés.

Le contexte est établi en premier lieu. Une appréciation des risques est ensuite réalisée. Si cette appréciation donne suffisamment d'informations pour déterminer correctement les actions nécessaires pour ramener les risques à un niveau acceptable, la tâche est alors terminée et suivie par le traitement des risques. Si les informations ne sont pas suffisantes, une autre itération de l'appréciation des risques sera réalisée avec un contexte révisé (par exemple les critères d'évaluation des risques, les critères d'acceptation des risques ou les critères d'impact) et, éventuellement, sur des parties limitées de l'ensemble du domaine d'application (voir Figure 1, point de décision du risque n° 1).

L'efficacité du traitement des risques dépend des résultats de l'appréciation des risques. Il est possible que le traitement des risques ne donne pas immédiatement un niveau acceptable de risque résiduel. Dans ce cas, une nouvelle itération de l'appréciation des risques utilisant, si nécessaire, de nouveaux paramètres de contexte (à titre d'exemples l'appréciation des risques, l'acceptation des risques ou les critères d'impact) peut être requise et suivie d'un autre traitement des risques (voir la Figure 1, Point de décision du risque n° 2).

L'activité d'acceptation des risques doit garantir que les risques résiduels sont explicitement acceptés par les dirigeants de l'organisation. Elle est particulièrement importante dans une situation où la mise en œuvre de mesures de sécurité est omise ou reportée, par exemple en raison des coûts.

Au cours du processus de gestion des risques en sécurité de l'information, il est important que les risques et leur traitement soient communiqués aux dirigeants et au personnel concerné. Avant même le traitement des risques, les informations relatives aux risques identifiés peuvent être très utiles pour gérer les incidents et contribuer à réduire les dommages potentiels. La sensibilisation des dirigeants et du personnel aux risques, la nature des mesures de sécurité mises en place pour atténuer les risques et les problèmes rencontrés par l'organisation sont utiles pour gérer les incidents et les événements imprévus de la manière la plus efficace. Il convient de documenter les résultats détaillés de toute activité du processus de gestion des risques en sécurité de l'information, ainsi que ceux obtenus à partir des deux points de décision de risque.

L'ISO/CEI 27001 spécifie que les mesures de sécurité mises en œuvre dans le domaine d'application, les limites et le contexte du SMSI doivent être fondées sur le risque. L'application d'un processus de gestion des risques en sécurité de l'information peut répondre à cette exigence. De nombreuses approches de ce processus peuvent être mises en œuvre avec succès au sein d'une organisation. Il convient que cette dernière utilise l'approche la plus adaptée à ses besoins pour chacun des usages spécifiques du processus.

Dans un SMSI, l'établissement du contexte, l'appréciation des risques, l'élaboration d'un plan de traitement des risques et l'acceptation des risques font partie intégrante de la phase «Planifier». Lors de la phase «Déployer» du SMSI, les actions et mesures de sécurité requises pour ramener le risque à un niveau acceptable sont mises en œuvre, conformément au plan de traitement des risques. Lors de la phase «Contrôler» du SMSI, les dirigeants déterminent les besoins en matière de révision de l'appréciation et du traitement des risques à la lumière des incidents et des changements de situations. Lors de la phase «Agir», toutes les actions nécessaires, y compris une itération supplémentaire du processus de gestion des risques en sécurité de l'information, sont réalisées.

Le tableau suivant résume les activités de gestion des risques en sécurité de l'information associées aux quatre phases du processus SMSI.

Tableau 1 — Alignement du SMSI et du processus de gestion des risques en sécurité de l'information

Processus SMSI	Processus de gestion des risques en sécurité de l'information
Planifier	Établissement du contexte Appréciation des risques Élaboration du plan de traitement des risques Acceptation des risques
Déployer	Mise en œuvre du plan de traitement des risques
Contrôler	Surveillance et revue continues des risques
Agir	Maintien et amélioration du processus de gestion des risques en sécurité de l'information

7 Établissement du contexte

7.1 Considérations générales

Éléments d'entrée: Toutes les informations relatives à l'organisation permettant l'établissement du contexte de la gestion des risques en sécurité de l'information.

Action: Il convient d'établir le contexte de la gestion des risques en sécurité de l'information, ce qui implique de déterminer les critères de base nécessaires à la gestion des risques en sécurité de l'information (7.2), de définir le domaine d'application et les limites (7.3), et d'établir une organisation adaptée au fonctionnement de la gestion des risques en sécurité de l'information (7.4).

Préconisations de mise en œuvre:

Il est essentiel de déterminer l'objectif de la gestion des risques en sécurité de l'information puisqu'il influence l'ensemble du processus et, en particulier, l'établissement du contexte. L'objectif peut être:

- une réponse aux exigences d'un SMSI;
- la conformité avec la loi et la preuve de la mise en œuvre du devoir de précaution;
- la préparation d'un plan de continuité d'activité;
- la préparation d'un plan de réponse aux incidents;
- la description des exigences en matière de sécurité de l'information pour un produit, un service ou un mécanisme.

Les préconisations de mise en œuvre des éléments d'établissement du contexte nécessaires pour répondre aux exigences d'un SMSI sont traitées en 7.2, 7.3 et 7.4.

NOTE L'ISO/CEI 270001 n'utilise pas le terme «contexte». Cependant, l'Article 7 aborde les exigences «définir le domaine d'application et les limites du SMSI» [4.2.1 a)], «définir une politique du SMSI» [4.2.1 b)] et «définir l'approche d'appréciation des risques» [4.2.1 c)], spécifiées dans l'ISO/CEI 27001.

Éléments de sortie: La spécification des critères de base, le domaine d'application et les limites, et l'organisation dédiée au fonctionnement processus de gestion des risques en sécurité de l'information.

7.2 Critères de base

Selon le domaine d'application et les objectifs de la gestion des risques, différentes approches peuvent s'appliquer. L'approche peut également être différente pour chaque itération.

Il convient de choisir ou d'élaborer une approche de gestion des risques adaptée qui comprenne des critères de base tels que les critères d'évaluation des risques, les critères d'impact et les critères d'acceptation des risques.

En outre, il convient que l'organisation évalue si les ressources nécessaires sont disponibles pour:

- effectuer une appréciation des risques et établir un plan de traitement des risques
- définir et mettre en œuvre des politiques et des procédures, y compris la mise en œuvre des mesures de sécurité choisies
- surveiller les mesures de sécurité
- surveiller le processus de gestion des risques en sécurité de l'information

NOTE Voir également l'ISO/CEI 27001 (5.2.1) relatif à la mise à disposition de ressources pour la mise en œuvre et le fonctionnement d'un SMSI.

Critères d'évaluation des risques

Il convient d'élaborer des critères d'évaluation des risques afin d'évaluer le risque de l'organisation en sécurité de l'information en prenant en compte les éléments suivants:

- la valeur stratégique des processus informationnels métier
- la criticité des actifs informationnels concernés
- les exigences légales et réglementaires ainsi que les obligations contractuelles
- l'importance opérationnelle et métier de la disponibilité, de la confidentialité et de l'intégrité
- les attentes et les perceptions des parties prenantes ainsi que les conséquences négatives sur la valorisation financière et la réputation de l'organisation

En outre, les critères d'évaluation des risques peuvent être utilisés pour spécifier les priorités du traitement des risques.

Critères d'impact

Il convient que les critères d'impact soient élaborés et spécifiés en fonction du niveau de dommages ou de coûts pour l'organisation pouvant être causés par un événement lié à la sécurité de l'information, en tenant compte des points suivants:

- le niveau de classification de l'actif informationnel impacté
- l'atteinte à la sécurité de l'information (par exemple, une perte de confidentialité, d'intégrité et de disponibilité)

- les erreurs opérationnelles (équipes internes ou tierces parties)
- des pertes de marchés et de valeur financière
- la perturbation des plans d'actions et des délais
- les atteintes à la réputation
- le non respect des exigences légales, réglementaires ou contractuelles

NOTE Voir aussi l'ISO/CEI 27001 [Article 4.2.1 d) 4] concernant l'identification des critères d'impact relatifs aux pertes de confidentialité, d'intégrité et de disponibilité.

Critères d'acceptation des risques

Il convient que les critères d'acceptation des risques soient élaborés et spécifiés. Ces critères dépendent souvent des politiques de l'organisation, des intentions, des objectifs et des intérêts des parties prenantes.

Il convient que l'organisation définisse ses propres échelles pour les seuils d'acceptation des risques. Il y a lieu de prendre en compte les éléments suivants au moment de l'élaboration:

- les critères d'acceptation des risques peuvent inclure des seuils multiples correspondant à un niveau de risques cibles souhaité, tout en réservant aux cadres décisionnaires la possibilité d'accepter des risques situés au-dessus de ce niveau dans certains cas

- les critères d'acceptation des risques peuvent être exprimés comme un rapport entre le profit estimé (ou tout autre bénéfice métier) et le risque estimé

- différents critères d'acceptation des risques peuvent s'appliquer à différents types de risques, par exemple des risques susceptibles d'aboutir à une non-conformité, à des réglementations ou à des lois peuvent ne pas être acceptés, tandis que l'acceptation de risques élevés peut être autorisée si cela est spécifié comme une exigence contractuelle

- les critères d'acceptation des risques peuvent comprendre des exigences relatives à de futurs traitements additionnels. Ainsi, il est possible d'accepter un risque s'il y a un engagement et une validation que des mesures destinées à le ramener à un niveau acceptable, dans un délai défini, vont être mises en œuvre

Les critères d'acceptation des risques peuvent varier selon la durée d'existence prévue du risque; il est, par exemple, possible que le risque soit associé à une activité temporaire ou de courte durée. Il convient de déterminer les critères d'acceptation des risques en tenant compte des points suivants:

- critères commerciaux

- aspects légaux et réglementaires

- aspects opérationnels

- aspects technologiques

- aspects financiers

- facteurs sociaux et humanitaires

NOTE Les critères d'acceptation des risques correspondent aux «critères d'acceptation des risques et identifier le niveau des risques acceptable» spécifiés dans l'ISO/CEI 27001 Article 4.2.1 c) 2).

De plus amples informations sont données dans l'Annexe A.

7.3 Domaine d'application et limites

Il convient que l'organisation définisse le domaine d'application et les limites de la gestion des risques en sécurité de l'information.

Il est nécessaire de définir le domaine d'application du processus de gestion des risques en sécurité de l'information afin de garantir que tous les actifs concernés sont pris en compte dans l'appréciation des risques. En outre, il est nécessaire d'identifier les limites du périmètre [voir aussi l'ISO/CEI 27001, 4.2.1 a)] afin de traiter les risques susceptibles de survenir à travers elles.

Il convient de rassembler les informations relatives à l'organisation afin de déterminer l'environnement dans lequel il intervient ainsi que son adéquation avec le processus de gestion des risques en sécurité de l'information.

Lors de la définition du domaine d'application et des limites, l'organisation devrait considérer les informations suivantes:

- les objectifs stratégiques commerciaux, les stratégies et les politiques de l'organisation

- les processus métier

- les fonctions et la structure de l'organisation

- les exigences légales, réglementaires et contractuelles applicables à l'organisation

- la politique de sécurité de l'information de l'organisation