NORME INTERNATIONALE

ISO/IEC 27005

Troisième édition
2018-07

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

Information technology — Security techniques — Information security risk management

Numéro de référence
ISO/IEC 27005:2018(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée 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 l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27005:2011) qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

— toutes les références directes à l'ISO/IEC 27001:2005 ont été supprimées;

— une information claire a été ajoutée, stipulant que le présent document ne contient pas de préconisations directes concernant la mise en œuvre des exigences du SMSI spécifiées dans l'ISO/IEC 27001 (voir Introduction);

— l'ISO/IEC 27001:2005 a été supprimée de l'Article 2;

— l'ISO/IEC 27001 a été ajoutée à la Bibliographie;

— l'Annexe G et toutes les références à cette Annexe ont été supprimées;

— des modifications éditoriales ont été effectuées en conséquence.

Introduction

Le présent document contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans un organisme. Cependant, le présent document ne fournit aucune méthodologie spécifique à la gestion des risques en sécurité de l'information. Il est du ressort de chaque organisme de définir son approche de la gestion des risques, en fonction, par exemple, du périmètre d'un système de management de la sécurité de l'information (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 le présent document pour appliquer les exigences du SMSI. Le présent document est fondé sur la méthode d'identification des risques liés à des actifs, des menaces et des vulnérabilités, qui n'est plus exigée par l'ISO/IEC 27001; il existe d'autres approches qui peuvent être utilisées.

Le présent document ne contient pas de préconisations directes concernant la mise en œuvre des exigences du SMSI spécifiées dans l'ISO/IEC 27001.

Le présent document s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'un organisme et, le cas échéant, aux tiers prenant part à ces activités.

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

1 Domaine d'application

Le présent document contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

Le présent document appuie les concepts généraux énoncés dans l'ISO/IEC 27001; il est conçu 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/IEC 27001 et l'ISO/IEC 27002 afin de bien comprendre le présent document.

Le présent document est applicable à tous types d'organismes (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'organisme.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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 s'applique (y compris les éventuels amendements).

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 27000 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

4 Structure du présent document

Le présent document 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 et concertation relatives aux risques dans l'Article 11;

— surveillance et réexamen des risques 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. L'Annexe C donne des exemples de menaces type et l'Annexe D traite des vulnérabilités et des méthodes d'appréciation des vulnérabilités. 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'organisme 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 externe et interne, 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 à 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 le réexamen réguliers 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'organisme dans son ensemble, à toute partie distincte de l'organisme (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

Un aperçu de haut niveau du processus de gestion des risques est spécifié dans l'ISO 31000 et illustré à la Figure 1.

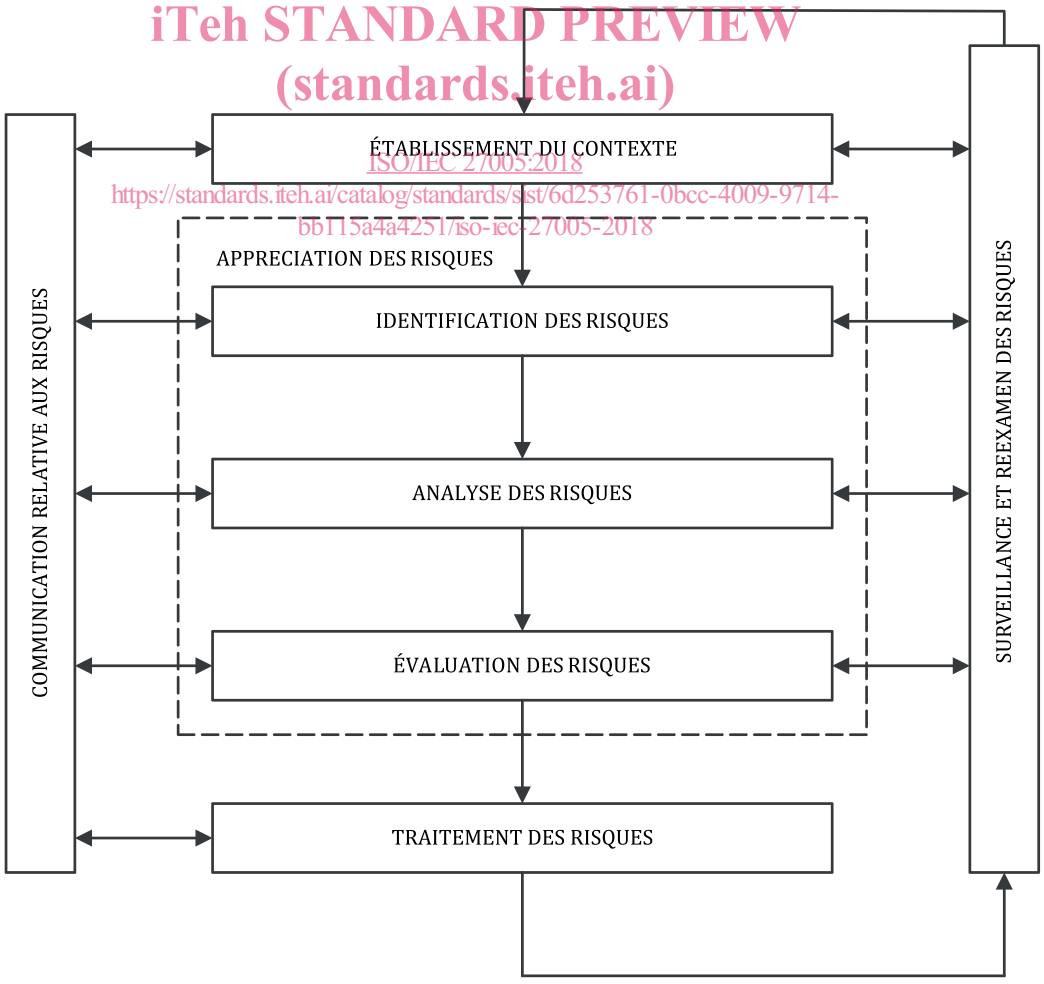

Figure 1 — Processus de gestion des risques

La Figure 2 illustre la manière dont le présent document applique ce processus de gestion des risques.

Le processus de gestion des risques en sécurité de l'information inclut 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 et la concertation relatives aux risques (Article 11), ainsi que la surveillance et le réexamen des risques (Article 12).

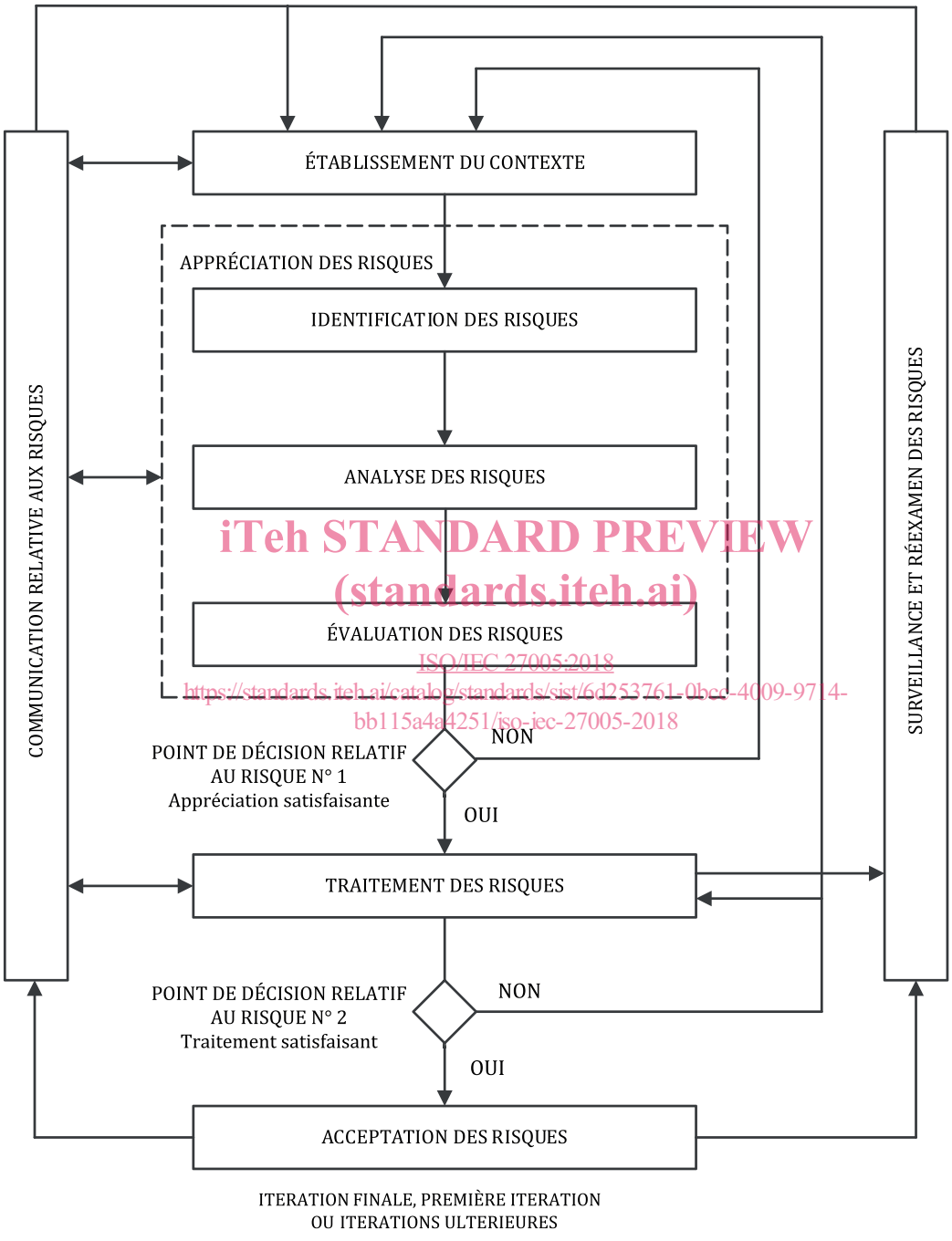

Figure 2 — Illustration du processus de gestion des risques en sécurité de l'information

Comme l'illustre la Figure 2, 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 est réalisée avec un contexte révisé (par exemple les critères d'évaluation du risque, 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 la Figure 2, point de décision relatif au risque n° 1).

L'efficacité du traitement des risques dépend des résultats de l'appréciation des risques.

Il est à noter que le traitement des risques implique un processus cyclique de:

— appréciation d'un traitement des risques;

— décision de reconnaître si les niveaux de risque résiduel sont acceptables;

— génération d'un nouveau traitement des risques si les niveaux de risque ne sont pas acceptables; et

— appréciation de l'efficacité du traitement considéré.

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 2, Point de décision relatif au risque n° 2).

L'activité d'acceptation des risques doit garantir que les risques résiduels sont explicitement acceptés par les dirigeants de l'organisme. 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 de l'ensemble 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'organisme 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/IEC 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 permettent de déterminer les mesures de sécurité pour mettre en œuvre les options choisies en matière de traitement des risques.

Il convient que l'organisme établisse, mette en œuvre et tienne à jour des procédures pour identifier les exigences légales applicables pour:

— la sélection des critères pour l'évaluation des risques (7.2.2), l'impact des risques (7.2.3) et l'acceptation des risques (7.2.4);

— la définition du domaine d'application et des limites de la gestion des risques en sécurité de l'information (7.3 et A.2);

— l'évaluation des risques (8.4);

— le traitement des risques (9.1) et la mise en œuvre de plans de réduction des risques (9.2 et Annexe F);

— la surveillance, la revue et l'amélioration de la gestion des risques (12.2);

— l'identification des actifs (B.1.3) et la valorisation des actifs (B.2.3); et

— l'estimation des risques (voir les exemples en E.2.1).

7 Établissement du contexte

7.1 Considérations générales

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

Action: Il convient d'établir le contexte externe et interne 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 ses 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; et

— 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.

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

7.2 Critères de base

7.2.1 Approche de gestion des risques

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 inclue des critères de base tels que les critères d'évaluation du risque, les critères d'impact et les critères d'acceptation des risques.

En outre, il convient que l'organisme 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; et

— surveiller le processus de gestion des risques en sécurité de l'information.

7.2.2 Critères d'évaluation du risque

Il convient d'élaborer des critères d'évaluation du risque afin d'évaluer le risque de l'organisme 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;

— 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'organisme.

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

7.2.3 Critères d'impact

NOTE L'ISO 31000 utilise le concept de «critères de conséquences» au lieu de «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'organisme 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.

7.2.4 Critères d'acceptation des risques

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

Il convient que l'organisme définisse ses propres échelles pour les niveaux 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 risque cible souhaité, tout en réservant aux cadres décisionnaires la possibilité d'accepter des risques situés au-dessus de ce niveau dans certaines circonstances définies;

— 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;

— les critères d'acceptation des risques peuvent inclure 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 réduire 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 opérationnels;

— aspects technologiques;

— aspects financiers;

— facteurs sociaux et humanitaires.

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

7.3 Domaine d'application et limites

Il convient que l'organisme 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 afin de traiter les risques susceptibles de survenir à travers elles.

Il convient de rassembler les informations relatives à l'organisme 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, il convient que l'organisme considère les informations suivantes:

— les objectifs stratégiques commerciaux, les stratégies et les politiques de l'organisme;

— les processus métier;

— les fonctions et la structure de l'organisme;

— la politique de sécurité de l'information de l'organisme;

— l'approche globale de l'organisme vis-à-vis de la gestion des risques;

— les actifs informationnels;

— les localisations de l'organisme et leurs caractéristiques géographiques;

— les contraintes affectant l'organisme;

— les attentes des parties prenantes;

— l'environnement socioculturel;

— les interfaces (c'est-à-dire les échanges d'information avec l'environnement).

De plus, il convient que l'organisme justifie toute exclusion du domaine d'application.

Des exemples de domaine d'application de gestion des risques peuvent être une application ou une infrastructure en technologie de l'information, un processus métier ou une partie définie d'un organisme.

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

7.4 Organisation de la gestion des risques en sécurité de l'information

Il convient de déterminer et de maintenir l'organisation et les responsabilités relatives au processus de gestion des risques en sécurité de l'information. Les principaux rôles et responsabilités de cette organisation sont les suivants:

— élaboration du processus de gestion des risques en sécurité de l'information adapté à l'organisme;

— identification et analyse des parties prenantes;

— définition des rôles et des responsabilités de toutes les parties, à la fois internes et externes à l'organisme;

— établissement des relations entre l'organisme et les parties prenantes, des interfaces avec les fonctions de gestion des risques de haut niveau de l'organisme (par exemple, gestion des risques opérationnels) ainsi que des interfaces avec d'autres projets ou activités, si cela est pertinent;

— détermination des processus d'escalade;

— spécification des enregistrements à conserver.

Il convient que cette organisation soit approuvée par les dirigeants concernés au sein de l'organisme.

8 Appréciation des risques en sécurité de l'information

8.1 Description générale de l'appréciation des risques en sécurité de l'information

Éléments d'entrée: Critères de base, domaine d'application et limites, et organisation pour l'établissement du processus de gestion des risques en sécurité de l'information.

Action: Il convient que les risques soient identifiés, quantifiés ou qualitativement décrits, et priorisés à partir des critères d'évaluation du risque et des objectifs significatifs pour l'organisme.

Préconisations de mise en œuvre:

Un risque est la combinaison des conséquences qui découleraient de l'occurrence d'un événement indésirable et de la probabilité d'occurrence de l'événement. L'appréciation des risques quantifie ou décrit qualitativement le risque et permet aux dirigeants de classer les risques par ordre de priorité selon leur gravité perçue ou en cohérence avec d'autres critères établis.

L'appréciation des risques inclut les activités suivantes:

— l'identification des risques (8.2);

— l'analyse des risques (8.3);

— l'évaluation des risques (8.4).

L'appréciation des risques détermine la valeur des actifs informationnels, identifie les menaces et les vulnérabilités applicables existantes (ou susceptibles d'exister), identifie les mesures de sécurité existantes et leurs effets sur le risque identifié, détermine les conséquences potentielles puis classe les risques ainsi obtenus par ordre de priorité en cohérence avec les critères d'évaluation du risque définis lors de l'établissement du contexte.

L'appréciation des risques est souvent réalisée en deux itérations (ou plus). Une appréciation de haut niveau est d'abord effectuée afin d'identifier les risques potentiels majeurs qui justifient une appréciation supplémentaire. L'itération suivante peut impliquer une étude détaillée des risques potentiels majeurs mis en lumière par l'itération initiale. Lorsque cette démarche ne fournit pas suffisamment d'informations pour apprécier les risques, d'autres analyses détaillées peuvent être réalisées, probablement sur des sous-ensembles du domaine d'application et, éventuellement, à l'aide d'une méthode différente.