NORME INTERNATIONALE

ISO/CEI 27005

Deuxième édition
2011-06-01

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/CEI 27005:2011(F)

Version française parue en 2013

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 ne saurait être tenue pour responsable 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/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 27005:2008), qui a fait l'objet d'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'organisation 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 pour 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 s'applique (y compris les éventuels amendements).

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

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

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 27000 et les suivants s'appliquent.

NOTE Les différences de définitions entre l'ISO/CEI 27005:2008 et la présente Norme internationale sont indiquées dans l'Annexe G.

3.1
conséquence
effet d'un **événement** (3.3) affectant les objectifs

[Guide ISO 73:2009]

NOTE 1 Un événement unique peut engendrer des conséquences multiples.

NOTE 2 Une conséquence peut être certaine ou incertaine et dans le cadre de la sécurité de l'information elle est généralement négative.

NOTE 3 Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

NOTE 4 Des conséquences initiales peuvent déclencher des réactions en chaîne.

3.2
mesure de sécurité
mesure qui modifie un **risque** (3.9)

[Guide ISO 73:2009]

NOTE 1 Une mesure de sécurité du risque en sécurité de l'information inclut n'importe quel processus, politique, procédure, recommandation, dispositif pratique ou organisation, qui peut être d'ordre administratif, technique, managérial ou juridique et qui modifie le risque en sécurité de l'information.

NOTE 2 Une mesure de sécurité du risque n'aboutit pas toujours à la modification voulue ou supposée.

NOTE 3 Une mesure de sécurité du risque est également utilisée comme synonyme de protection ou contre-mesure.

3.3
événement
occurrence ou changement d'un ensemble particulier de circonstances

[Guide ISO 73:2009]

NOTE 1 Un événement peut être unique ou se reproduire, et peut avoir plusieurs causes.

NOTE 2 Un événement peut consister en quelque chose qui ne se produit pas.

NOTE 3 Il peut parfois être fait référence à un événement en tant qu'«incident» ou «accident».

3.4
contexte externe
environnement externe dans lequel l'organisation cherche à atteindre ses objectifs

[Guide ISO 73:2009]

NOTE Le contexte externe peut inclure:

— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local;

— les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisation; et

— les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

3.5
contexte interne
environnement interne dans lequel l'organisation cherche à atteindre ses objectifs

[Guide ISO 73:2009]

NOTE Le contexte interne peut inclure:

— la gouvernance, l'organisation, les rôles et responsabilités;

— les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers;

— les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies);

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels);

— les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs;

— la culture de l'organisation;

— les normes, lignes directrices et modèles adoptés par l'organisation; et

— la forme et l'étendue des relations contractuelles.

3.6
niveau de risque
importance d'un **risque** (3.9), exprimée en termes de combinaison des **conséquences** (3.1) et de leur **vraisemblance** (3.7)

[Guide ISO 73:2009]

3.7
vraisemblance
possibilité que quelque chose se produise

[Guide ISO 73:2009]

NOTE 1 Dans la terminologie de la gestion des risques, le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

NOTE 2 Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie de la gestion des risques, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

3.8
risque résiduel
risque (3.9) subsistant après le **traitement des risques** (3.17)

[Guide ISO 73:2009]

NOTE 1 Un risque résiduel peut inclure des risques non identifiés.

NOTE 2 Un risque résiduel peut également être appelé «risque maintenu».

3.9
risque
effet de l'incertitude sur l'atteinte des objectifs

[Guide ISO 73:2009]

NOTE 1 Un effet est un écart, positif et/ou négatif, par rapport à un attendu, positif et/ou négatif.

NOTE 2 Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'une organisation toute entière).

NOTE 3 Un risque est souvent caractérisé en référence à des événements (3.3) et des conséquences (3.1) potentiels ou à une combinaison des deux.

NOTE 4 Un risque en sécurité de l'information est souvent exprimé en termes de combinaison des conséquences d'un événement de sécurité de l'information et de sa vraisemblance (3.9).

NOTE 5 L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

NOTE 6 Le risque en sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'une ressource d'information ou d'un groupe de ressources d'information et portent de ce fait préjudice à l'organisation.

3.10
analyse des risques
processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le **niveau de risque** (3.6)

[Guide ISO 73:2009]

NOTE 1 L'analyse des risques fournit la base de l'évaluation du risque et les décisions relatives au traitement des risques.

NOTE 2 L'analyse des risques inclut l'estimation des risques.

3.11
appréciation des risques
ensemble du processus d'**identification des risques** (3.15), d'**analyse des risques** (3.10) et d'**évaluation du risque** (3.14)

[Guide ISO 73:2009]

3.12
communication et concertation relatives aux risques
processus itératifs et continus mis en œuvre par une organisation afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les **parties prenantes** (3.18) concernant la gestion des risques (3.9)

[Guide ISO 73:2009]

NOTE 1 Ces informations peuvent concerner l'existence, la nature, la forme, la vraisemblance, l'importance, l'évaluation, l'acceptabilité et le traitement des risques.

NOTE 2 La concertation est un processus de communication argumentée à double sens entre une organisation et ses parties prenantes sur une question donnée avant de prendre une décision ou de déterminer une orientation concernant ladite question. La concertation est:

— un processus dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir; et

— une contribution à une prise de décision, et non une prise de décision conjointe.

3.13
critères de risque
termes de référence vis-à-vis desquels le caractère significatif d'un **risque** (3.9) est évalué

[Guide ISO 73:2009]

NOTE 1 Les critères de risque sont fondés sur les objectifs de l'organisation ainsi que sur le contexte externe et interne.

NOTE 2 Les critères de risque peuvent être issus de normes, de lois, de politiques et d'autres exigences.

3.14
évaluation du risque
processus de comparaison des résultats de l'**analyse des risques** (3.10) avec les **critères de risque** (3.13) afin de déterminer si les risques et/ou leur importance sont acceptables ou tolérables

[Guide ISO 73:2009]

NOTE L'évaluation du risque aide à la prise de décision relative au traitement des risques.

3.15
identification des risques
processus de recherche, de reconnaissance et de description des risques

[Guide ISO 73:2009]

NOTE 1 L'identification des risques comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles.

NOTE 2 L'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des parties prenantes.

3.16
gestion des risques
activités coordonnées dans le but de diriger et piloter une organisation en prenant en compte les risques

[Guide ISO 73:2009]

NOTE La présente Norme internationale utilise le terme «processus» pour décrire l'ensemble de la gestion des risques. Les éléments internes au processus de gestion des risques sont désignés les «activités».

3.17
traitement des risques
processus destiné à modifier un risque

[Guide ISO 73:2009]

NOTE 1 Le traitement des risques peut inclure:

— un refus du risque en décidant de ne pas démarrer ou poursuivre l'activité porteuse du risque;

— la prise ou l'augmentation d'un risque afin de saisir une opportunité;

— l'élimination de la source de risque;

— une modification de la vraisemblance;

— une modification des conséquences;

— un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque); et

— un maintien du risque fondé sur une décision argumentée.

NOTE 2 Les traitements des risques portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

NOTE 3 Le traitement des risques peut créer de nouveaux risques ou modifier des risques existants.

3.18
partie prenante
personne ou organisation susceptible d'affecter, d'être affectée ou de se sentir elle-même affectée par une décision ou une activité

[Guide ISO 73:2009]

NOTE Un décideur peut être une partie prenante.

4 Structure de la présente Norme internationale

La présente Norme internationale 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 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'identification des actifs). L'Annexe C donne des xemples 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.

Les différences de définitions entre l'ISO/CEI 27005:2008 et l'ISO/CEI 27005:2011 sont indiquées dans l'Annexe G.

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 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 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

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

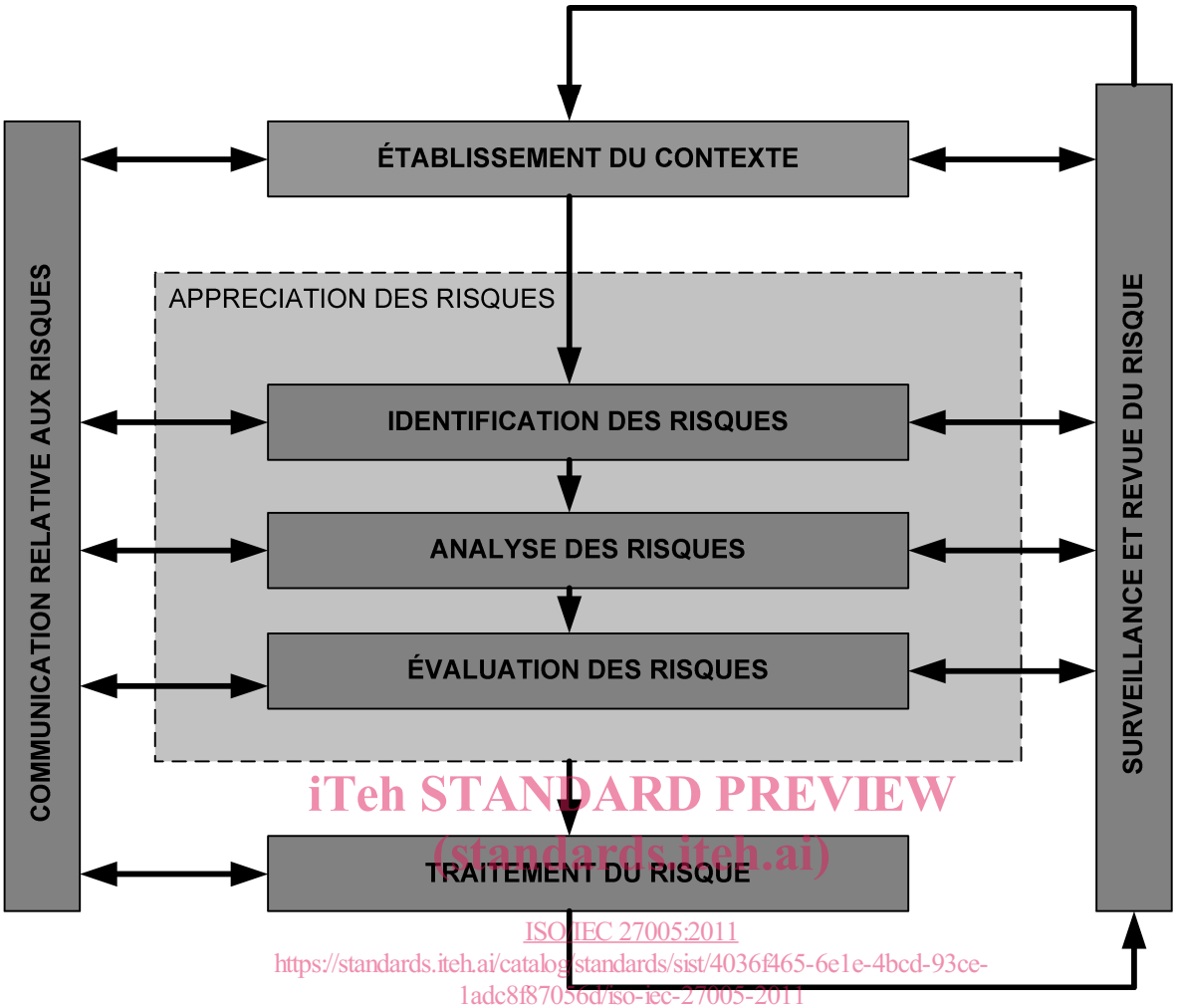

Figure 1 — Processus de gestion des risques

La Figure 2 illustre la manière dont la présente Norme internationale applique ce processus de gestion des risques.

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 relative aux risques (Article 11), ainsi que la surveillance et la revue du risque (Article 12).

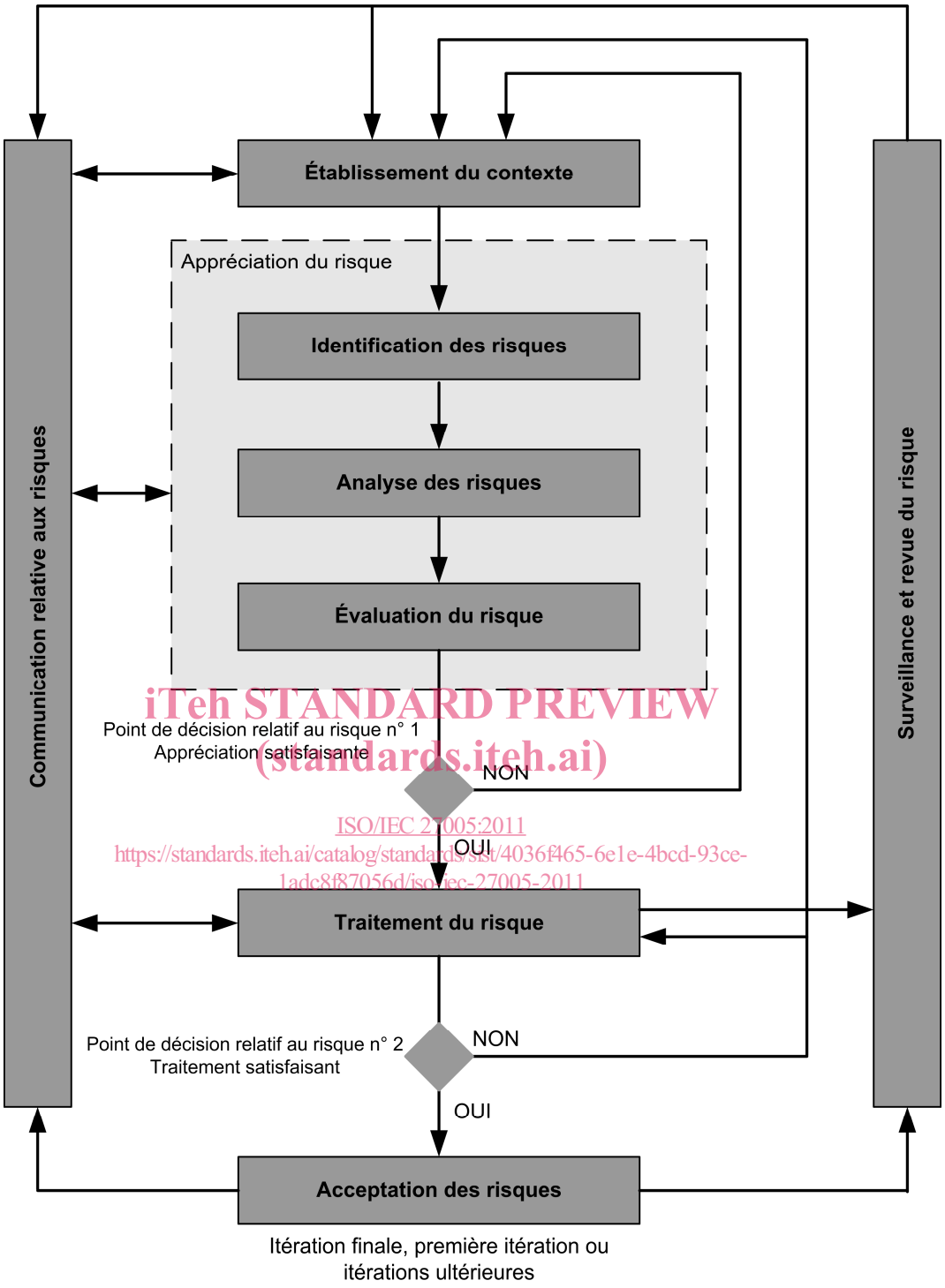

Figure 2 — Illustration du processus de gestion des risques en sécurité de l'information

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.