Avant-projet de norme soumis à enquête probatoire jusqu'au :
15 octobre 2009

Pr NF ISO/CEI 27005

Indice de classement : Z 74-225

T1 Technologies de l'information

T2 Techniques de sécurité

T3 Gestion du risque en sécurité de l'information

E : Information technology — Security techniques — Information security risk management

D :

Avant-projet de norme française homologuée

Remplace :

Correspondance

Analyse

Modifications

ISO/CEI /JTC1/SC 27

Date: **2008-06-15**

ISO/CEI 27005:2008(F)

ISO/CEI /JTC1/SC **27**/GT

Secrétariat: **DIN**

Technologies de l'information — Techniques de sécurité — Gestion du risque en sécurité de l'information

Information technology — Security techniques — Information security risk management

Type du document: Norme internationale
Sous-type du document:
Stade du document: (60) Publication
Langue du document: F

M:\dp\AA_Production\ISO\27005\07_TRAD_Publication\Doc traduit\ISO-CEI_27005_(F).doc STD Version 2.2

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/TC JTC1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des TI*.

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 de risque en sécurité de l'information dans une organisation qui viennent, notamment, en appui des exigences d'un SMSI tel qu'il est défini dans l'ISO/CEI 27001. Cependant, la présente Norme internationale ne fournit aucune méthodologie spécifique à la gestion de risque en sécurité de l'information. Il est du ressort de chaque organisation de définir son approche de la gestion de risque, en fonction, par exemple, du périmètre du SMSI, de l'existant dans le domaine de la gestion de risques, ou encore du 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 de risque 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 du risque en sécurité de l'information

1 Domaine d'application

La présente Norme internationale contient des lignes directrices relatives à la gestion de risque 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 de risque.

Il est important de connaître les concepts, les modèles, les processus et les terminologies décrites dans l'ISO/CEI 27001 afin de bien comprendre cette 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 de leurs informations.

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 gestion de sécurité de l'information — Exigences*.

ISO/CEI 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)*.

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
évitement 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 du risque
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 du risque
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 du risque.

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 du risque.

3.6
identification du risque
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 du risque.

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 de risque.

4 Structure de la présente Norme internationale

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

Les informations générales sont fournies dans l'Article 5.

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

Toutes les activités liées à la gestion du risque 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 du risque dans l'Article 8 ;
- traitement du risque dans l'Article 9 ;
- acceptation du risque dans l'Article 10 ;
- communication du risque dans l'Article 11 ;
- surveillance et réexamen du risque dans l'Article 12.

Des informations supplémentaires relatives aux activités de gestion du risque 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 du risque 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 des risques sont traitées dans l'Annexe F.

Toutes les activités liées à la gestion de risque, telles que présentées dans les Articles 7 à 12, sont structurées de la manière suivante :

Elément(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.

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

5 Contexte

Une approche systématique de la gestion du risque 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 du risque de l'entreprise. Les efforts effectués en matière de sécurité devraient adresser les risques de manière efficace et opportune quand et lorsque cela est nécessaire. Il convient que la gestion du risque 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 du risque 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 du risque permettant de mettre en œuvre les recommandations et décisions. La gestion du risque analyse les évènements susceptibles de se produire et leurs possibles conséquences avant de décider 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 :

- 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 du risque,
- la priorisation des actions afin de réduire les occurrences des risques,
- l'implication des parties prenantes lors de la prise de décisions relatives à la gestion du risque et l'information sur l'état de la gestion du risque,
- l'efficacité de la supervision du traitement du risque,
- la surveillance et le réexamen réguliers des risques et du processus de gestion de risque,
- la capture de l'information afin d'améliorer l'approche de gestion du risque,
- la formation des dirigeants et du personnel sur les risques et les actions à entreprendre pour atténuer.

Le processus de gestion du risque 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 continuation d'activité).

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

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

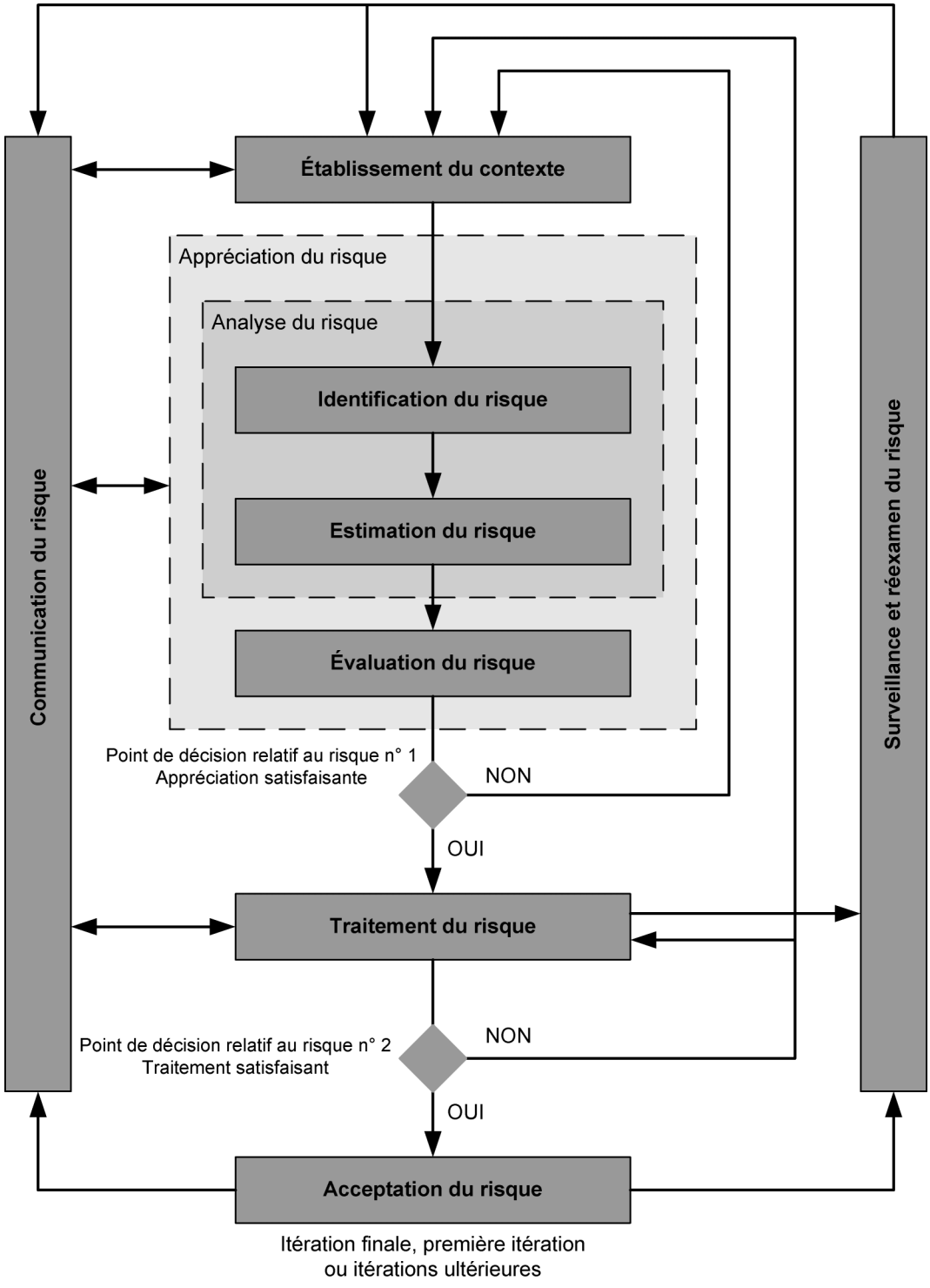

Figure 1 — Processus de gestion du risque en sécurité de l'information

Comme l'illustre la Figure 1, le processus de gestion du risque en sécurité de l'information peut être itératif pour les activités d'appréciation et/ou de traitement du risque. Une approche itérative de conduite de l'appréciation du risque permet de l'approfondir et de la préciser 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 du risque 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 du risque. Si les informations ne sont pas suffisantes, une autre itération de l'appréciation du risque sera réalisée avec un contexte révisé (par exemple les critères d'évaluation du risque, les critères d'acceptation du risque 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 du risque dépend des résultats de l'appréciation du risque. Il est possible que le traitement du risque ne donne pas immédiatement un niveau acceptable de risque résiduel. Dans ce cas, une nouvelle itération de l'appréciation du risque utilisant, si nécessaire, de nouveaux paramètres de contexte (à titre d'exemples : l'appréciation du risque, l'acceptation du risque ou les critères d'impact) peut être requise et suivie d'un autre traitement du risque (voir la Figure 1, Point de décision du risque n° 2).

L'activité d'acceptation du risque 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 du processus de gestion du risque 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 du risque 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 du risque 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'un organisme. Il convient que ce dernier 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 du risque, l'élaboration d'un plan de traitement du risque et l'acceptation du risque 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 du risque. Lors de la phase « Contrôler » du SMSI, les dirigeants déterminent les besoins en matière de révision de l'appréciation et du traitement du risque 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 du risque en sécurité de l'information, sont réalisées.

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

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

Processus SMSI	Processus de gestion du risque en sécurité de l'information
Planifier	Etablissement du contexte Appréciation du risque Elaboration du plan de traitement du risque Acceptation du risque
Déployer	Mise en œuvre du plan de traitement du risque
Contrôler	Surveillance et réexamen continus des risques
Agir	Maintien et amélioration du processus de gestion du risque en sécurité de l'information

7 Etablissement du contexte

7.1 Considérations générales

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

Action : Il convient d'établir le contexte de la gestion du risque en sécurité de l'information, ce qui implique de déterminer les critères de base nécessaires à la gestion du risque 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 du risque en sécurité de l'information (7.4).

Préconisations de mise en œuvre :

Il est essentiel de déterminer l'objectif de la gestion du risque 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 de l'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 ci-dessous aux Articles 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 du risque » [4.2.1 c)], spécifiées dans l'ISO/CEI 27001.

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

7.2 Critères de base

Selon le domaine d'application et les objectifs de la gestion du risque, 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 du risque adaptée qui comprenne des critères de base tels que les critères d'évaluation du risque, les critères d'impact et les critères d'acceptation du risque.

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

- effectuer une appréciation du risque et établir un plan de traitement du risque,
- 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 du risque en sécurité de l'information.

NOTE Voir également l'ISO/CEI 27001 (article 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 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,
- 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'organisme.

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

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),
- la perte d'activité métier 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 du risque

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

Il convient que l'organisme 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 du risque 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 certains cas,

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

- différents critères d'acceptation du risque 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 du risque 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 du risque 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 du risque 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 du risque correspondent aux « critères d'acceptation des risques et identifier le niveau de risque 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'organisme définisse le domaine d'application et les limites de la gestion du risque en sécurité de l'information.

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

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 de risque en sécurité de l'information.

Lors de la définition du domaine d'application et des limites, l'organisme devrait considérer 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,
- les exigences légales, réglementaires et contractuelles applicables à l'organisme,
- la politique de sécurité de l'information de l'organisme,
- l'approche globale de l'organisme vis-à-vis de la gestion du risque,
- 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 du risque peuvent être une application ou une infrastructure en technologie de l'information, un processus métier ou une partie définie d'un organisme.

NOTE Le domaine d'application et les limites de la gestion du risque en sécurité de l'information sont liés au domaine d'application et aux limites du SMSI exigés dans l'ISO/CEI 27001 4.2.1 a).

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

7.4 Organisation de la gestion du risque en sécurité de l'information

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

- élaboration du processus de gestion du risque 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 de risque de haut niveau de l'organisme (par exemple, gestion du risque opérationnel) 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.

NOTE L'ISO/CEI 27001 exige la détermination et la mise à disposition des ressources nécessaires pour établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI [5.2.1 a)]. L'organisation du fonctionnement du processus de gestion du risque peut être considérée comme l'une des ressources requises par l'ISO/CEI 27001.

8 Appréciation du risque en sécurité de l'information

8.1 Description générale de l'appréciation du risque en sécurité de l'information

NOTE L'activité d'appréciation du risque est appelée « processus »dans l'ISO/CEI 27001.

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

Action : Les risques sont 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 du risque 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 du risque comprend les activités suivantes :

- l'analyse du risque (paragraphe 8.2), qui comprend :
  - l'identification du risque (paragraphe 8.2.1),
  - l'estimation du risque (paragraphe 8.2.2) ;
- l'évaluation du risque (paragraphe 8.3).

L'appréciation du risque 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 du risque 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 le risque, 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.

Il incombe à l'organisme de choisir sa propre approche d'appréciation du risque en se basant sur les objectifs et le but de l'appréciation du risque.

Une discussion des approches d'appréciation du risque en sécurité de l'information se trouve en Annexe E.

Élément de sortie : Liste des risques appréciés classés par ordre de priorité en cohérence avec les critères d'évaluation du risque.

8.2 Analyse du risque

8.2.1 Identification du risque

8.2.1.1 Introduction à l'identification du risque

L'objectif de l'identification du risque est de déterminer les événements susceptibles de se produire causant une perte potentielle, et de donner un aperçu de comment, où, et quand cette perte pourrait survenir. Il convient que les étapes décrites dans les sous-paragraphes de l'Article 8.2.1 qui suivent permettent de produire les données d'entrée de l'activité d'estimation du risque.

NOTE Les activités décrites dans les autres paragraphes peuvent être effectuées dans un ordre différent selon la méthodologie appliquée.

8.2.1.2 Identification des actifs

Éléments d'entrée : Domaine d'application et limites de l'appréciation du risque à effectuer, liste des composants avec les propriétaires, emplacement, fonction etc.

Action : Il convient d'identifier les actifs relevant du domaine d'application établi (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 d)1)).

Préconisations de mise en œuvre :

Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection. Concernant l'identification des actifs, il convient de garder à l'esprit qu'un système d'information ne comprend pas uniquement du matériel et des logiciels.

Il convient de réaliser l'identification des actifs à un niveau de détail adapté qui fournisse suffisamment d'informations pour l'appréciation du risque. Le niveau de détail utilisé pour l'identification des actifs influence la quantité totale d'informations réunies pendant l'appréciation du risque. Le niveau peut être affiné lors d'itérations ultérieures de l'appréciation du risque.

Il convient d'identifier le propriétaire de chaque actif afin d'assurer la responsabilité. Le propriétaire de l'actif peut ne pas jouir de droits de propriété sur l'actif mais est responsable de sa production, de son développement, de sa maintenance, de son utilisation et de sa protection selon le cas. Le propriétaire de l'actif est souvent la personne la plus à même de déterminer la valeur qu'il représente pour l'organisme (voir en 8.2.2.2 concernant la valorisation des actifs).

Les limites du réexamen sont le périmètre des actifs de l'organisme défini comme devant être géré par le processus de gestion du risque en sécurité de l'information.

De plus amples informations quant à l'identification et à la valorisation des actifs liés à la sécurité de l'information sont disponibles dans l'Annexe B.

Éléments de sortie : Liste des actifs dont les risques sont à gérer et liste des processus métier relatifs aux actifs et leur pertinence.

8.2.1.3 Identification des menaces

Éléments d'entrée : Informations relatives aux menaces obtenues grâce au réexamen des incidents, aux propriétaires des actifs, aux utilisateurs et à d'autres sources, y compris des catalogues de menaces externes.

Action : Il convient d'identifier les menaces et leurs sources (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 d)2)).

Préconisations de mise en œuvre :

Une menace est susceptible d'endommager les actifs tels que des informations, des processus et des systèmes et, par conséquent, des organismes. Les menaces peuvent être d'origine naturelle ou humaine et peuvent être accidentelles ou délibérées. Il convient d'identifier les sources de menace à la fois accidentelles et délibérées. Une menace peut survenir de l'intérieur ou de l'extérieur de l'organisme. Il convient d'identifier les menaces de manière générique et par type (à titre d'exemples : des actions non autorisées, des dommages physiques, des défaillances techniques) puis, lorsque cela est pertinent, des menaces individuelles particulières peuvent être identifiées au sein d'une classe générique. Cela signifie qu'aucune menace n'est négligée, même une menace imprévue, mais que le volume de travail requis reste limité.

Certaines menaces peuvent affecter plus d'un actif. Dans ce cas, elles peuvent avoir différentes conséquences selon l'actif affecté.

Les éléments d'entrée de l'identification des menaces et de l'estimation de la vraisemblance (voir en 8.2.2.3) peuvent être obtenus auprès des propriétaires ou des utilisateurs d'actifs, auprès de l'équipe des ressources humaines, des spécialistes en infogérance et en sécurité de l'information, des experts en sécurité physique, du service juridique et d'autres organismes (y compris des organismes juridiques), des services météorologiques, des compagnies d'assurance et des autorités nationales gouvernementales. Lors du traitement des menaces, les aspects relatifs à l'environnement et à la culture doivent être pris en compte.

Lors de la réalisation d'une appréciation, il convient de tenir compte de l'expérience obtenue en interne à partir d'incidents et d'appréciations de menaces antérieures. Il peut s'avérer utile de consulter d'autres catalogues de menaces (pouvant être spécifiques à un organisme ou à un secteur d'activité) afin de compléter le cas échéant la liste de menaces génériques. Les statistiques et catalogues relatifs aux menaces sont disponibles auprès d'organismes industriels, d'administrations gouvernementales, d'organismes juridiques, de compagnies d'assurance, etc.

Lors de l'utilisation de catalogues relatifs aux menaces ou de résultats d'appréciations de menaces antérieures, il convient de garder à l'esprit que les menaces sont sans cesse en évolution, notamment lorsque l'environnement de l'activité métier ou les systèmes d'information changent.

De plus amples informations relatives aux types de menace sont disponibles dans l'Annexe C.

Élément de sortie : Liste de menaces avec identification du type et de la source de la menace.

8.2.1.4 Identification des mesures de sécurité existantes

Éléments d'entrée : Documentation relative aux mesures de sécurité, plans de mise en œuvre du traitement du risque.

Action : Il convient d'identifier les mesures de sécurité existantes et prévues.

Préconisations de mise en œuvre :

Il convient de procéder à une identification des mesures de sécurité existantes pour éviter des travaux ou des coûts inutiles dus, par exemple, à une redondance des mesures de sécurité. En outre, tout en identifiant les mesures de sécurité existantes, il convient d'effectuer un contrôle afin de garantir que les mesures de sécurité fonctionnent correctement - une référence aux rapports d'audit du SMSI déjà existants peut limiter le temps dédié à cette tâche. Si une mesure de sécurité ne fonctionne pas comme prévu, des vulnérabilités peuvent être engendrées. Il convient de tenir compte du cas où le fonctionnement d'une mesure de sécurité (ou une stratégie) choisie échoue et, par conséquent, où des mesures de sécurité complémentaires sont requises pour répondre au risque identifié de manière efficace. Dans un SMSI, conformément à l'ISO/CEI 27001, ce point est pris en charge par l'évaluation de l'efficacité des mesures. Un bon moyen d'estimer l'effet d'une mesure de sécurité consiste à examiner la manière dont elle réduit la vraisemblance d'une menace et la facilité à exploiter la vulnérabilité, ou l'impact de l'incident. Les revues de direction et les rapports d'audit fournissent également des informations relatives à l'efficacité des mesures de sécurité existantes.

Il convient de considérer les mesures de sécurité prévues pour déploiement, conformément aux plans de mise en œuvre du traitement du risque, de la même manière que les mesures de sécurité déjà mises en œuvre.

Une mesure de sécurité existante ou prévue peut être identifiée comme étant inefficace, insuffisante ou injustifiée. Si elle s'avère injustifiée ou insuffisante, il convient de contrôler la mesure de sécurité afin de déterminer s'il convient de la retirer, de la remplacer par une autre mesure de sécurité plus adaptée, ou s'il convient de la laisser en place, par exemple pour des raisons de coûts.

Les activités suivantes peuvent s'avérer utiles pour l'identification des mesures de sécurité existantes ou prévues :

- le réexamen des documents contenant des informations relatives aux mesures de sécurité (par exemple, les plans de mise en œuvre du traitement du risque). Si les processus de gestion de sécurité de l'information sont bien documentés, il convient que toutes les mesures de sécurité existantes ou prévues, ainsi que le statut de leur mise en œuvre, soient mis à disposition,

- la vérification avec les personnes responsables de la sécurité de l'information (par exemple un responsable de la sécurité de l'information et un responsable de la sécurité du système d'information, un responsable de la sécurité physique ou un responsable des opérations) et avec les utilisateurs afin de vérifier quelles mesures de sécurité sont réellement mises en œuvre pour le processus d'information ou le système d'information considérés,

- la revue sur site des mesures de sécurité physiques, en comparant les mesures mises en œuvre à la liste des mesures à déployer et en vérifiant les mesures mises en œuvre pour savoir si elles fonctionnent correctement et efficacement,

- l'examen des résultats des audits internes.

Éléments de sortie : Liste de toutes les mesures de sécurité existantes et prévues, l'état relatif à leur mise en œuvre et à leur utilisation.

8.2.1.5 Identification des vulnérabilités

Éléments d'entrée : Liste des menaces connues, listes des actifs et des mesures de contrôle existantes.

Action : Il convient d'identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 d)3)).

Préconisations de mise en œuvre :

Les vulnérabilités peuvent être identifiées dans :

- l'organisme,
- les processus et procédures,
- les activités récurrentes de gestion,
- le personnel,
- l'environnement physique,
- la configuration du système d'information,
- les matériels, logiciels ou infrastructures de communication,
- la dépendance aux parties externes.

La présence d'une vulnérabilité n'entraîne pas de dommage en elle-même, puisque la présence d'une menace est nécessaire pour l'exploiter. Une vulnérabilité à laquelle ne correspond aucune menace peut ne pas exiger la mise en œuvre d'une mesure de sécurité, mais il convient qu'elle soit identifiée et surveillée en cas de changements. Il convient de noter qu'une mesure de sécurité mal mise en œuvre, ou présentant un dysfonctionnement, ou encore utilisée de manière incorrecte peut constituer une vulnérabilité. Une mesure de sécurité peut s'avérer efficace, ou non, selon l'environnement dans lequel elle est mise en œuvre. Inversement, une menace à laquelle ne correspond aucune vulnérabilité peut ne pas entraîner de risque.

Les vulnérabilités peuvent être liées à des propriétés de l'actif susceptibles d'être utilisées d'une manière, ou à des fins différentes de celles prévues lorsque l'actif a été acheté ou élaboré. Les vulnérabilités dues à différentes sources nécessitent d'être prises en compte, par exemples celles qui sont intrinsèques ou extrinsèques à l'actif.

Des exemples de vulnérabilités et de méthodes d'appréciation des vulnérabilités sont disponibles dans l'Annexe D.

Éléments de sortie : Liste des vulnérabilités liées aux actifs, aux menaces et aux mesures de sécurité ; liste des vulnérabilités qui ne sont pas liées à une menace identifiée pour réexamen.

8.2.1.6 Identification des conséquences

Éléments d'entrée : Liste des actifs, liste des processus métier et liste des menaces et vulnérabilités, le cas échéant, liées aux actifs et leur pertinence.

Action : Il convient d'identifier les conséquences que des pertes de confidentialité, d'intégrité et de disponibilité peuvent avoir sur les actifs (voir l'ISO/CEI 27001 4.2.1 d) 4)).

Préconisations de mise en œuvre :

Une conséquence peut être une perte d'efficacité, des conditions de fonctionnement défavorables, une perte d'activité métier, de réputation, un dommage, etc.

Cette activité identifie les dommages, ou les conséquences pour l'organisme, susceptibles d'être dus à un scénario d'incident. Un scénario d'incident est la description d'une menace exploitant une certaine vulnérabilité, ou un ensemble de vulnérabilités, lors d'un incident de sécurité de l'information (voir l'ISO/CEI 27002, article 13). Les conséquences des scénarii d'incident doivent être déterminées en tenant compte des critères d'impact définis lors de l'activité d'établissement du contexte. Un ou plusieurs actifs, ou une partie d'un actif peuvent être affectés. Les actifs peuvent donc se voir attribuer des valeurs, à la fois, selon leur coût financier et selon les conséquences sur l'activité métier s'ils sont endommagés ou compromis. Les conséquences peuvent être temporaires ou permanentes, comme dans le cas de la destruction d'un actif.

NOTE L'ISO/CEI 27001 décrit l'occurrence de scénarii d'incident comme des « défaillances de la sécurité ».

Il convient que les organismes identifient les conséquences opérationnelles des scénarii d'incident en termes de (sans s'y limiter) :

- temps d'investigation et de réparation,
- temps (de travail) perdu,
- perte d'opportunités,
- santé et sûreté,
- coût financier des compétences spécifiques nécessaires pour réparer les dommages,
- image et valorisation financière de l'entreprise.

Des détails relatifs à l'appréciation des vulnérabilités techniques se trouvent en B.3 Appréciation des impacts.

Élément de sortie : Liste des scénarii d'incident et de leurs conséquences liées aux actifs et aux processus métier.

8.2.2 Estimation du risque

8.2.2.1 Méthodologies d'estimation du risque

L'analyse de risque peut être effectuée à différents niveaux de détail selon la criticité des actifs, la portée des vulnérabilités connues et des incidents antérieurs expérimentés au sein de l'organisme. Selon les circonstances, une méthodologie d'estimation peut être qualitative, quantitative ou une combinaison des deux.,En pratique, l'estimation qualitative est souvent utilisée en premier lieu pour obtenir une indication générale du niveau de risque et pour mettre en exergue les principaux risques. Il peut ensuite être nécessaire d'entreprendre une analyse plus spécifique ou quantitative des risques majeurs, étant donné qu'il est souvent moins complexe et moins onéreux d'effectuer une analyse qualitative qu'une analyse quantitative.

Il convient que le type d'analyse menée soit cohérent avec les critères d'évaluation du risque définis lors de l'établissement du contexte.

De plus amples informations relatives aux méthodologies d'estimation sont décrites ci-dessous :

(a) Estimation qualitative :

L'estimation qualitative utilise une échelle d'attributs qualificatifs pour décrire l'ampleur des conséquences potentielles (par exemple : faible, moyenne et élevée) ainsi que la probabilité de leur occurrence. Un des avantages de l'estimation qualitative est sa facilité de compréhension par l'ensemble du personnel concerné ; en revanche un inconvénient est qu'elle dépend du choix subjectif de l'échelle.

Ces échelles peuvent être adaptées, ou ajustées, afin de convenir aux circonstances, et différentes descriptions peuvent être utilisées pour différents risques. L'estimation qualitative peut être utilisée :

- comme une activité d'examen initial destiné à identifier les risques qui exigent une analyse plus détaillée,
- lorsque ce type d'analyse est adapté à la prise de décisions,
- lorsque les données numériques ou les ressources ne sont pas adaptées à une estimation quantitative.

Il convient que l'analyse qualitative utilise des informations et des données factuelles, si elles sont disponibles.

(b) Estimation quantitative :

L'estimation quantitative utilise une échelle comportant des valeurs numériques (plutôt que les échelles descriptives utilisées lors de l'estimation qualitative), à la fois pour les conséquences et pour la vraisemblance, à l'aide de données obtenues à partir de sources diverses. La qualité de l'analyse dépend de la précision et de l'exhaustivité des valeurs numériques et de la validité des modèles utilisés. Dans la plupart des cas, l'estimation quantitative utilise des données relatives à des incidents expérimentés, l'avantage étant qu'elles peuvent être directement liées aux objectifs et aux préoccupations de l'organisme en matière de sécurité de l'information. L'inconvénient est le manque de ces données sur les nouveaux risques ou les faiblesses de la sécurité de l'information. Un inconvénient de l'approche quantitative est que, lorsque les données factuelles et auditables ne sont pas disponibles, une illusion d'utilité et de précision de l'appréciation du risque est créée.

La manière d'exprimer les conséquences et la vraisemblance, et de les combiner pour fournir un niveau de risque varie en fonction du type de risque et de l'objectif pour lequel les résultats d'appréciation du risque vont être utilisés. Il convient que l'incertitude et la variabilité des conséquences et de la vraisemblance soient prises en compte dans l'analyse et communiquées de manière efficace.

8.2.2.2 Appréciation des conséquences

Élément d'entrée : Liste de scénarii d'incident pertinents identifiés, incluant l'identification des menaces, vulnérabilités, actifs altérés, conséquences pour les actifs et les processus métier.

Action : Il convient d'apprécier l'impact sur l'activité de l'organisme pouvant résulter d'incidents de sécurité de l'information potentiels ou avérés, en tenant compte des conséquences d'une atteinte à la sécurité de l'information telle qu'une perte de confidentialité, d'intégrité ou de disponibilité des actifs (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e) 1)).

Préconisations de mise en œuvre :

Une fois tous les actifs concernés identifiés, il convient de prendre en compte les valeurs attribuées à ces actifs lors de l'appréciation des conséquences.

La valeur d'un impact sur l'activité métier peut être exprimée de manière qualitative et quantitative, cependant une méthode d'attribution d'une valeur financière peut, en général, fournir davantage d'informations pour la prise de décision et permettre, ainsi, un processus de décision plus efficace.

La valorisation d'un actif commence par la classification des actifs en fonction de leur criticité en termes d'importance des actifs pour l'accomplissement des objectifs métiers de l'organisme. La valorisation est alors effectuée à l'aide de deux mesures :

- la valeur de remplacement de l'actif : le coût de retour à une situation normale et de remplacement des informations (dans la mesure du possible),

- les conséquences sur l'activité métier d'une perte ou d'une compromission de l'actif, tels que les potentielles conséquences négatives sur l'activité et/ou les conséquences légales ou réglementaires dues à la diffusion, la modification, la non disponibilité et/ou la destruction d'informations et d'autres actifs informationnels.

Cette évaluation peut être déterminée par une analyse d'impact sur l'activité métier. La valeur, déterminée par la conséquence sur l'activité, est souvent nettement supérieure au simple coût de remplacement, en fonction de l'importance que joue l'actif dans l'accomplissement des objectifs métiers de l'organisme.

La valorisation des actifs est un facteur clé de l'appréciation des impacts d'un scénario d'incident car l'incident peut affecter plus d'un actif (par exemple, des actifs dépendants) ou uniquement une partie d'un actif. Différentes menaces et vulnérabilités auront des impacts différents sur les actifs, comme une perte de confidentialité, d'intégrité ou de disponibilité. L'appréciation des conséquences est donc liée à la valorisation des actifs, basée sur l'analyse des impacts sur l'activité métier.

Les conséquences, ou l'impact sur l'activité métier, peuvent être déterminés en modélisant les résultats d'un événement ou d'un ensemble d'événements, ou par extrapolation d'études expérimentales ou de données passées.

Les conséquences peuvent être exprimées en termes de critères d'impact financier, technique ou humain, ou d'autres critères pertinents dans le contexte de l'organisme. Dans certains cas, plus d'une valeur numérique est nécessaire pour spécifier les conséquences à différents moments, sites, groupes ou situations.

Il convient de mesurer les conséquences en termes de délais et de coûts à l'aide de la même approche que celle utilisée pour la vraisemblance des menaces et la vulnérabilité. Il convient de conserver la cohérence de l'approche quantitative ou qualitative.

De plus amples informations concernant la valorisation des actifs et l'appréciation des impacts sont disponibles dans l'Annexe B.

Élément de sortie : Liste des conséquences d'un scénario d'incident appréciées et exprimées en cohérence avec les actifs et les critères d'impact.

8.2.2.3 Appréciation de la vraisemblance d'un incident

Éléments d'entrée : Liste des scénarii d'incident pertinents identifiés, incluant l'identification des menaces, actifs affectés, vulnérabilités exploitées et conséquences pour les actifs et les processus métier. De plus, la liste de toutes les mesures de sécurité existantes et prévues, leur efficacité et l'état relatif à leur mise en œuvre et à leur utilisation.

Action : Il convient d'apprécier la vraisemblance des scénarii d'incident (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e)2)).

Préconisations de mise en œuvre :

Une fois les scénarii d'incident identifiés, il est nécessaire d'apprécier la vraisemblance de chaque scénario et survenance d'impact, à l'aide de techniques d'estimation qualitatives et quantitatives. Il convient de tenir compte de la fréquence de survenance des menaces et de la facilité d'exploitation des vulnérabilités, en prenant en considération :

- l'expérience et les statistiques applicables à la vraisemblance des menaces,
- pour les menaces de source délibérée : la motivation et les capacités, qui évolueront au cours du temps, les ressources disponibles pour les attaquants potentiels, ainsi que la perception de l'attrait et de vulnérabilité des actifs pour un attaquant potentiel,
- pour les menaces de source accidentelle : les facteurs géographiques, par exemple la proximité d'usines chimiques ou d'exploitations pétrolières, la possibilité de conditions météorologiques extrêmes et les facteurs susceptibles d'influencer les erreurs humaines et les dysfonctionnements des équipements,
- les vulnérabilités, à la fois individuellement et agrégées,
- les mesures de sécurité existantes et leur efficacité pour réduire les vulnérabilités.

Par exemple, un système d'information peut présenter une vulnérabilité par rapport aux menaces d'usurpation d'identité et d'utilisation illicite des ressources. La vulnérabilité par rapport à l'usurpation d'identité peut être élevée en raison de l'absence d'authentification de l'utilisateur. Par ailleurs, la vraisemblance de l'utilisation illicite des ressources peut être faible, malgré l'absence d'authentification de l'utilisateur, car les usages détournés sont limités.

Selon le degré de précision requis, il est possible de regrouper les actifs ou il peut s'avérer nécessaire de les diviser en plusieurs éléments et d'associer les scénarii à ces éléments. Par exemple, en fonction des emplacements géographiques, la nature des menaces ou l'efficacité des mesures de sécurité existantes peuvent varier pour un même type d'actifs.

Élément de sortie : Vraisemblance des scénarii d'incident (quantitative ou qualitative).

8.2.2.4 Estimation du niveau de risque

Élément d'entrée : Liste des scénarii d'incident accompagnés de leurs conséquences liées aux actifs et aux processus métier, ainsi que leur vraisemblance (quantitative ou qualitative).

Action : Il convient d'estimer le niveau de risque de tous les scénarii d'incident pertinents (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e)4)).

Préconisations de mise en œuvre :

L'estimation du risque attribue des valeurs à la vraisemblance et aux conséquences d'un risque. Ces valeurs peuvent être quantitatives ou qualitatives. L'estimation du risque est basée sur l'appréciation des conséquences et de la vraisemblance. De plus, elle peut prendre en compte les bénéfices en termes de coût, les préoccupations des parties prenantes et d'autres variables en vue de l'évaluation du risque. Le risque estimé est une combinaison de la vraisemblance d'un scénario d'incident et de ses conséquences.

Des exemples de méthodes ou d'approche d'estimation du risque en sécurité de l'information sont disponibles dans l'Annexe E.

Élément de sortie : Liste des risques avec un niveau de risque valorisé.

8.3 Evaluation du risque

Éléments d'entrée : Liste des risques avec un niveau de risque valorisé et critères d'évaluation du risque.

Action : Il convient de comparer le niveau des risques aux critères d'évaluation du risque et aux critères d'acceptation du risque (conformément à l'ISO/CEI 27001, paragraphe 4.2.1 e) 4)).

Préconisations de mise en œuvre :

La nature des décisions relatives à l'évaluation du risque et les critères d'évaluation du risque qui seront utilisés pour prendre ces décisions ont été définis lors de l'établissement du contexte. A cette étape, ces décisions et le contexte doivent être revus en détail au regard des risques identifiés. Afin d'évaluer les risques, il convient que les organismes comparent les risques estimés (à l'aide de méthodes ou d'approches choisies comme abordé dans l'Annexe E) aux critères d'évaluation du risque définis lors de l'établissement du contexte.

Il convient que les critères d'évaluation du risque utilisés pour prendre des décisions soient cohérents avec le contexte interne et externe de gestion du risque en sécurité de l'information, et qu'ils tiennent compte des objectifs de l'organisme, du point de vue des parties prenantes etc. Les décisions prises lors de l'activité d'évaluation du risque sont essentiellement basées sur le niveau acceptable de risque. Toutefois, il convient de considérer également les conséquences, la vraisemblance et le degré de confiance dans l'identification et l'analyse du risque. L'agrégation de plusieurs risques faibles ou moyens peut engendrer des risques globaux nettement supérieurs qu'il convient de traiter en conséquence.

Il convient que ces considérations comprennent :

- *les propriétés relatives à la sécurité de l'information :* si un critère n'est pas pertinent dans le contexte de l'organisme (par exemple, une perte de confidentialité), tous les risques ayant un impact sur ce critère peuvent alors ne pas être pertinents,

- *l'importance du processus métier ou de l'activité reposant sur un actif ou un ensemble d'actifs particuliers :* si le processus est déterminé comme étant de faible importance, il convient d'accorder moins d'attention aux risques associés à ce processus qu'aux risques ayant un impact sur des activités ou des processus plus importants.

L'évaluation du risque utilise la compréhension du risque obtenue par l'analyse du risque pour prendre des décisions relatives aux actions futures. Il convient que ces décisions indiquent :

- s'il convient d'entreprendre une activité,

- les priorités de traitement de risque en tenant compte des niveaux de risque estimés.

Lors de l'étape d'évaluation du risque, les exigences légales et réglementaires sont des facteurs qu'il convient de prendre en compte en plus des risques estimés.

Élément de sortie : Liste des risques classés par ordre de priorité selon les critères d'évaluation du risque en relation avec les scénarii d'incident qui conduisent à ces risques.

9 Traitement du risque en sécurité de l'information

9.1 Description générale du traitement du risque

Élément d'entrée : Liste des risques classés par ordre de priorité en cohérence avec les critères d'évaluation du risque et en relation avec les scénarii d'incident qui conduisent à ces risques.

Action : Il convient de choisir des mesures de sécurité pour réduire, maintenir, éviter ou transférer les risques, et de définir un plan de traitement du risque.

Préconisations de mise en œuvre :

Quatre options de traitement du risque sont possibles : la réduction du risque (voir en 9.2), le maintien du risque (voir en 9.3), l'évitement du risque (voir en 9.4) et le transfert de risque (voir en 9.5).

NOTE L'ISO/CEI 27001 4.2.1. f) 2) utilise le terme "acceptation de risque" au lieu de "maintien du risque".

La Figure 2 illustre l'activité de traitement du risque au sein du processus de gestion du risque en sécurité de l'information tel que présenté à la Figure 1.

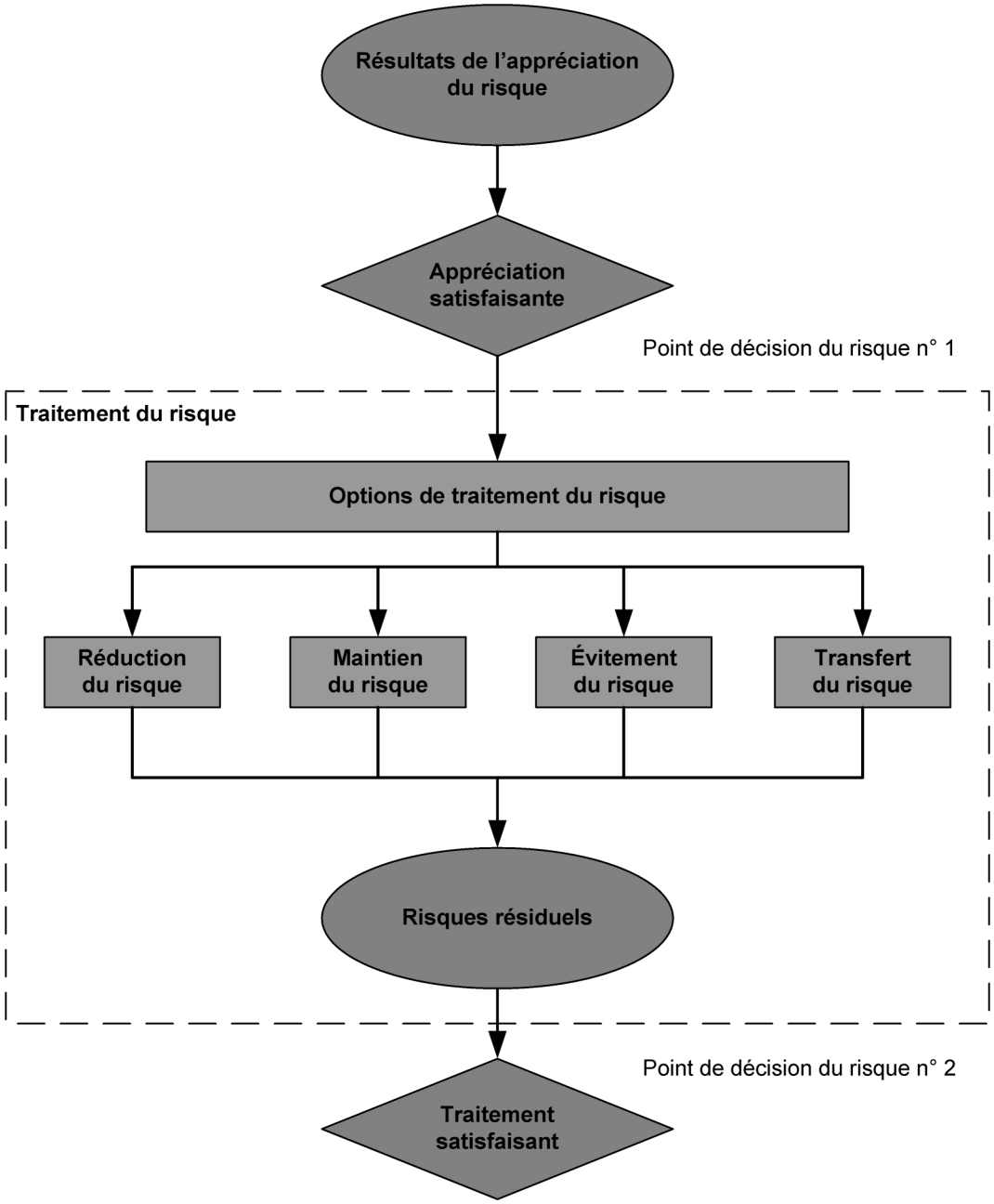

Figure 2 — Activité de traitement du risque

Il convient de choisir les options de traitement du risque sur la base des résultats de l'appréciation du risque, du coût prévu de mise en en œuvre ainsi que des bénéfices attendus de ces options.

Lorsqu'il est possible d'obtenir d'importantes réductions en réalisant relativement peu de dépenses, il convient de mettre en œuvre ces options. D'autres options d'améliorations peuvent être peu rentables ; il est donc nécessaire de bien les analyser afin de savoir si elles se justifient.

En général, il convient de rendre les conséquences négatives des risques aussi faibles que possible et indépendantes de tout critère absolu. Il convient que les dirigeants tiennent compte des risques rares mais aux impacts importants. Dans ces cas, les mesures de sécurité qui sont difficilement justifiables sur le plan

économique peuvent nécessiter d'être mises en œuvre (par exemple, des mesures de sécurité liées à la continuité de l'activité identifiées pour couvrir des risques spécifiques élevés).

Les quatre options relatives au traitement du risque ne s'excluent pas mutuellement. L'organisme peut parfois retirer des bénéfices substantiels d'une combinaison d'options tels que la réduction de la vraisemblance des risques et de leurs conséquences et le transfert ou la conservation de tout risque résiduel.

Certains traitements du risque peuvent répondre à plus d'un risque de manière efficace (par exemple, la formation et la sensibilisation en matière de sécurité de l'information). Il convient de définir un plan de traitement du risque, qui identifie clairement les priorités et les délais, selon lequel il convient de mettre en œuvre chaque traitement de risque. Les priorités peuvent être établies à l'aide de diverses techniques, notamment le classement des risques et l'analyse du rapport coûts/bénéfices. Il est de la responsabilité des dirigeants de l'organisme d'équilibrer les coûts de mise en œuvre des mesures de sécurité et l'attribution de budgets.

L'identification des mesures de sécurité existantes peut déterminer que ces mesures sont supérieures aux besoins réels, en termes de comparaison des coûts incluant la maintenance. Si le retrait de mesures de sécurité redondantes ou inutiles est envisagé (surtout si ces mesures entraînent des coûts de maintenance élevés), il convient de tenir compte des facteurs relatifs à la sécurité de l'information et aux coûts. Etant donné que les mesures de sécurité peuvent s'influencer mutuellement, la suppression des mesures de sécurité redondantes peut réduire le niveau de sécurité global actuel. En outre, il est parfois moins onéreux de laisser en place les mesures de sécurité redondantes ou inutiles plutôt que de les retirer.

Il convient de considérer les options liées au traitement du risque en tenant compte :

- de la façon dont les parties concernées perçoivent le risque,
- des manières les plus adaptées de communiquer avec ces parties.

L'établissement du contexte (voir en 7.2 – Critères d'évaluation du risque) fournit des informations relatives aux exigences légales et réglementaires auxquelles l'organisme doit se conformer. Le risque encouru par les organismes est la non-conformité ; il convient donc de mettre en œuvre des options de traitement destinées à limiter cette éventualité. Lors du traitement du risque, il convient de prendre en compte l'ensemble des contraintes – organisationnelles, techniques, structurelles, etc. – identifiées au cours de l'activité d'établissement du contexte.

Une fois le plan de traitement du risque défini, il est nécessaire de déterminer les risques résiduels. Cela implique la mise à jour ou la réitération de l'appréciation du risque, en tenant compte des effets pressentis du traitement de risque proposé. Dans le cas où le risque résiduel ne remplirait toujours pas les critères d'acceptation du risque de l'organisme, une autre itération du traitement de risque peut s'avérer nécessaire avant de procéder à l'acceptation du risque. De plus amples informations sont disponibles dans l'ISO/CEI 27002, paragraphe 0.3.

Éléments de sortie : Plan de traitement du risque et risques résiduels soumis à la décision d'acceptation des dirigeants de l'organisme.

9.2 Réduction du risque

Action : Il convient de réduire le niveau de risque par la sélection des mesures de sécurité afin que le risque résiduel puisse être réapprécié et jugé acceptable.

Préconisations de mise en œuvre :

Il convient de choisir des mesures de sécurité adaptées et justifiées afin de répondre aux exigences identifiées par l'appréciation et le traitement du risque. Il convient que ce choix tienne compte des critères d'acceptation du risque ainsi que des exigences légales, réglementaires et contractuelles. Il convient qu'il tienne également compte du coût et du délai de mise en œuvre des mesures de sécurité ou des aspects techniques, environnementaux et culturels. Il est souvent possible de diminuer le coût total de maintenance d'un système grâce à des mesures de sécurité de l'information correctement choisies.

En général, les mesures de sécurité peuvent fournir un ou plusieurs types de protection : la correction, l'élimination, la prévention, l'atténuation des impacts, la dissuasion, la détection, la récupération, la surveillance et la sensibilisation. Lors de la sélection des mesures de sécurité, il est important d'évaluer le coût d'acquisition, de mise en œuvre, d'administration, d'exploitation, de surveillance et de maintenance des mesures de sécurité par rapport à la valeur des actifs protégés. En outre, il convient de considérer le retour sur investissement en termes de réduction du risque et de nouvelles opportunités offertes par certaines mesures de sécurité. De plus, il convient de prendre en compte les compétences spécifiques susceptibles d'être nécessaires pour définir et mettre en œuvre de nouvelles mesures de sécurité, ou pour modifier les mesures existantes.

L'ISO/CEI 27002 fournit des informations détaillées sur les mesures de sécurité.

Il existe de nombreuses contraintes susceptibles d'affecter le choix des mesures de sécurité. Les contraintes techniques telles que les exigences de performance, les questions relatives aux possibilités de gestion (exigences de soutien opérationnel) et les problèmes de compatibilité peuvent empêcher l'utilisation de certaines mesures de sécurité, ou pourraient provoquer des erreurs humaines annulant la mesure de sécurité, en créant une fausse impression de sécurité, ou même en augmentant le risque au-delà de la non mise en œuvre de la mesure (par exemple, en exigeant des mots de passe complexes sans réelle formation, poussant ainsi les utilisateurs à écrire leur mot de passe sur papier). De plus, une mesure de sécurité pourrait altérer les performances. Il convient que les dirigeants essaient d'identifier une solution permettant de répondre aux exigences de performances tout en garantissant un niveau de sécurité de l'information suffisant. Le résultat de cette étape consiste en une liste des mesures de sécurité possibles présentant leur coût, leur(s) avantage(s) et la priorité de leur mise en œuvre.

Il convient de tenir compte de diverses contraintes lors du choix des mesures de sécurité et de leur mise en œuvre. En général, on considère les contraintes suivantes :

- contraintes de temps,
- contraintes financières,
- contraintes techniques,
- contraintes opérationnelles,
- contraintes culturelles,
- contraintes éthiques,
- contraintes environnementales,
- contraintes légales,
- facilité d'utilisation,
- contraintes liées au personnel,
- contraintes liées à l'intégration de mesures de sécurité nouvelles et existantes.

De plus amples informations concernant les contraintes liées à la réduction des risques sont disponibles dans l'Annexe F.

9.3 Maintien du risque

Action : Il convient de prendre la décision de maintenir le risque sans autre action en fonction de l'évaluation du risque.

NOTE L'ISO/CEI 27001 4.2.1 f 2) "l'acceptation des risques en connaissance de cause et avec objectivité, dans la mesure où ils sont acceptables au regard des politiques de l'organisme et des critères d'acceptation des risques" décrit la même activité.

Préconisations de mise en œuvre :

Si le niveau de risque répond aux critères d'acceptation du risque, il n'est pas nécessaire de mettre en œuvre d'autres mesures de sécurité, le risque peut alors être conservé.

9.4 Évitement du risque

Action : Il convient d'éviter l'activité ou la situation qui donne lieu à un risque particulier.

Préconisations de mise en œuvre :

Lorsque les risques identifiés sont jugés trop élevés ou lorsque les coûts de mise en œuvre d'autres options de traitement du risque dépassent les bénéfices attendus, il est possible de prendre la décision d'éviter complètement le risque, en abandonnant une ou plusieurs activités prévues ou existantes, ou en modifiant les conditions dans lesquelles l'activité est effectuée. Par exemple, pour les risques découlant d'incidents naturels, il peut être plus rentable de déplacer physiquement les moyens de traitement de l'information à un endroit où le risque n'existe pas ou est maîtrisé.

9.5 Transfert du risque

Action : Il convient de transférer le risque à une autre partie capable de gérer de manière plus efficace le risque spécifique en fonction de l'évaluation du risque.

Préconisations de mise en œuvre :

Le transfert du risque implique la décision de partager certains risques avec des parties externes. Il peut créer de nouveaux risques ou modifier les risques identifiés existants. Par conséquent, un autre traitement de risque peut s'avérer nécessaire.

Le transfert peut être effectué à l'aide d'une assurance qui prendra en charge les conséquences ou en sous-traitant à un partenaire dont le rôle consistera à surveiller le système d'information et à entreprendre des actions immédiates destinées à arrêter une attaque avant qu'un niveau de dommages défini ne soit atteint.

Il convient de noter qu'il peut être possible de transférer la responsabilité de gestion du risque mais il est en général impossible de transférer la responsabilité légale d'un impact. Les clients attribuent en général la responsabilité d'un effet indésirable à l'organisme.

10 Acceptation du risque en sécurité de l'information

Éléments d'entrée : Plan de traitement du risque et appréciation du risque résiduel soumis à la décision d'acceptation des dirigeants de l'organisme.

Action : Il convient de prendre la décision d'accepter les risques et les responsabilités de cette décision et de l'enregistrer formellement (conformément à l'ISO/CEI 27001 paragraphe 4.2.1 h)).

Préconisations de mise en œuvre :

Il convient que les plans de traitement du risque décrivent la manière dont les risques vont être traités afin de remplir les critères d'acceptation du risque (voir paragraphe 7.2 relatif aux critères d'acceptation du risque). Il est important que les dirigeants en charge réexaminent et approuvent les plans de traitement du risque proposés et les risques résiduels associés, puis enregistrent les conditions associées à l'approbation.

Les critères d'acceptation du risque peuvent être plus complexes et ne pas consister simplement à savoir si un risque résiduel se situe au-dessus ou en-dessous d'un seuil unique.

Dans certains cas, il est possible que le niveau de risque résiduel ne remplisse pas les critères d'acceptation du risque car les critères appliqués ne tiennent pas compte des circonstances prédominantes. Par exemple, il peut être avancé qu'il est nécessaire d'accepter les risques car les bénéfices liés à ces risques sont très avantageux, ou parce que le coût de la réduction du risque est trop élevé. De telles circonstances indiquent que les critères d'acceptation du risque sont inadaptés et qu'il convient, si possible, de les réviser. Toutefois, il n'est pas toujours possible de les réviser rapidement. Dans ce cas, il est possible que les décideurs aient à accepter des risques qui ne remplissent pas les critères normaux d'acceptation. Si cela s'avère nécessaire, il convient que le décideur commente explicitement les risques et inclut une justification de la décision d'outrepasser les critères normaux d'acceptation.

Élément de sortie : Liste des risques acceptés et justification pour les risques ne remplissant pas les critères normaux d'acceptation du risque de l'organisme.

11 Communication du risque en sécurité de l'information

Éléments d'entrée : L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque (voir la Figure 1).

Action : Il convient d'échanger et/ou de partager les informations relatives au risque entre le décideur et les autres parties prenantes.

Préconisations de mise en œuvre :

La communication du risque consiste en une activité visant à atteindre un accord sur la manière de gérer les risques par un échange et/ou un partage des informations relatives au risque entre les décideurs et les autres parties prenantes. Ces informations comprennent, sans toutefois s'y limiter, l'existence, la nature, le type, la vraisemblance, la gravité, le traitement et l'acceptabilité des risques.

Une communication efficace entre les parties prenantes est essentielle puisqu'elle peut avoir une forte influence sur les décisions à prendre. Cette communication garantit que les personnes responsables de la mise en œuvre de la gestion du risque et que les personnes ayant un intérêt direct comprennent les fondements sur lesquels les décisions sont prises et les raisons pour lesquelles des actions spécifiques sont nécessaires. La communication est bidirectionnelle.

Les perceptions du risque peuvent varier en raison de différences d'hypothèses, de concepts et de besoins, de questions et préoccupations des parties prenantes puisqu'elles sont liées au risque ou aux questions abordées. Les parties prenantes sont susceptibles d'émettre des jugements concernant l'acceptabilité du risque basés sur leur perception du risque. Il est particulièrement important de veiller que les perceptions du risque par les parties prenantes, ainsi que leurs perceptions des bénéfices, puissent être identifiées et documentées, et que les raisons sous-jacentes soient clairement comprises et traitées.

Il convient de procéder à la communication du risque pour parvenir à :

- garantir les résultats de la gestion de risque de l'organisme,
- réunir les informations relatives au risque,
- partager les résultats obtenus grâce à l'appréciation du risque et présenter le plan de traitement du risque,
- éviter ou réduire à la fois l'occurrence et les conséquences des violations de sécurité de l'information dues à un manque de compréhension mutuelle entre les décideurs et les parties prenantes,
- aider au processus de prise de décision,
- obtenir de nouvelles connaissances en sécurité de l'information,
- assurer une coordination avec d'autres parties et prévoir des réponses destinées à réduire les conséquences des incidents pouvant survenir,
- responsabiliser les décideurs et les parties prenantes quant aux risques,
- améliorer la sensibilisation à la sécurité de l'information.

Il convient qu'un organisme élabore des plans de communication du risque en fonctionnement normal ainsi que dans les situations d'urgence. Par conséquent, il convient de procéder de manière continue à l'activité de communication du risque.

La coordination entre les principaux décideurs et les principales parties prenantes peut être mise en œuvre en constituant un comité, de manière à ce qu'un débat sur les risques, sur leur niveau de priorité et le caractère adapté de leur traitement puisse avoir lieu.

Il est important de coopérer avec les bons services de communication ou de relations publiques au sein de l'organisme afin de coordonner toutes les tâches associées à la communication du risque. Cette communication est essentielle, notamment en cas d'actions de communication de crise, pour répondre à des incidents spécifiques.

Élément de sortie : Compréhension permanente du processus et des résultats de la gestion du risque en sécurité de l'information de l'organisme.

12 Surveillance et réexamen du risque en sécurité de l'information

12.1 Surveillance et réexamen des facteurs de risque

Élément d'entrée : L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque (voir la Figure 1).

Action : Il convient de surveiller et de réexaminer les risques et leurs facteurs (à savoir valeur des actifs, impacts, menaces, vulnérabilités et vraisemblance) pour identifier au plus tôt toutes les modifications dans le contexte de l'organisme et pour maintenir une cartographie complète des risques.

Préconisations de mise en œuvre :

Les risques ne sont pas statiques. Les menaces, les vulnérabilités, la vraisemblance ou les conséquences peuvent changer brutalement sans aucune indication préalable. Par conséquent, une surveillance constante est nécessaire pour détecter ces changements. Cette surveillance peut être assurée par des services externes qui fournissent des informations relatives à de nouvelles menaces ou vulnérabilités.

Il convient que les organismes s'assurent que les éléments suivants sont constamment surveillés :

- les nouveaux actifs ayant été inclus dans le domaine d'application de la gestion du risque,
- les modifications nécessaires des valeurs des actifs, en raison par exemple des modifications des exigences métier,
- les nouvelles menaces susceptibles d'être actives à la fois à l'intérieur et à l'extérieur de l'organisme et qui n'ont pas été appréciées,
- la possibilité que des vulnérabilités nouvelles ou accrues puissent permettre aux menaces de les exploiter,
- les vulnérabilités identifiées pour déterminer celles qui deviennent exposées à des menaces nouvelles ou qui réapparaissent,
- l'augmentation de l'impact ou des conséquences des menaces, des vulnérabilités et des risques appréciés en agrégation entraînant un niveau de risque inacceptable,
- les incidents liés à la sécurité de l'information.

De nouvelles menaces, vulnérabilités ou modifications de la vraisemblance ou des conséquences peuvent accroître les risques appréciés auparavant comme des risques peu élevés. Il convient que le réexamen des risques peu élevés et acceptés prenne en compte chaque risque individuellement, puis de manière globale, afin d'apprécier le cumul potentiel des impacts. Si les risques ne relèvent pas de la catégorie de risques peu élevés ou acceptables, il convient de les traiter à l'aide d'une ou de plusieurs options présentées à l'Article 9.

Les facteurs affectant la vraisemblance et les conséquences des menaces peuvent changer, de même que les facteurs affectant la pertinence et le coût des diverses options de traitement. Il convient que les modifications majeures de l'organisme entraînent un réexamen plus spécifique. Par conséquent, il convient de répéter régulièrement les activités de surveillance du risque et de réexaminer périodiquement les options choisies de traitement du risque.

Le résultat des activités de surveillance du risque peut servir de donnée d'entrée à d'autres activités de réexamen du risque. Il convient que l'organisme réexamine régulièrement l'ensemble des risques, notamment lors de modifications importantes (conformément à l'ISO/CEI 27001, paragraphe 4.2.3)).

Éléments de sortie : Alignement continu de la gestion du risque avec les objectifs métiers de l'organisme ainsi qu'avec les critères d'acceptation du risque.

12.2 Surveillance, réexamen et amélioration de la gestion du risque

Éléments d'entrée : L'ensemble des informations, relatives au risque, obtenues grâce aux activités de gestion du risque (voir la Figure 1).

Action : Il convient de constamment surveiller, réexaminer et améliorer le processus de gestion du risque en sécurité de l'information si nécessaire et de manière appropriée.

Préconisations de mise en œuvre :

Une surveillance et un réexamen permanents sont nécessaires pour garantir que le contexte, les résultats de l'appréciation et du traitement du risque, ainsi que les plans de gestion, restent adaptés aux circonstances.

Il convient que l'organisme s'assure que le processus de gestion du risque en sécurité de l'information et les activités associées restent adaptés aux circonstances actuelles et qu'ils soient respectés. Il convient de notifier aux dirigeants concernés toute amélioration acceptée apportée au processus ou aux actions nécessaires pour améliorer la conformité au processus afin qu'ils aient la garantie qu'aucun risque n'est négligé ou sous-estimé, que les actions nécessaires soient mises en œuvre et les décisions nécessaires sont prises pour garantir la compréhension réaliste du risque et la capacité à y répondre.

En outre, il convient que l'organisme vérifie régulièrement que les critères utilisés pour mesurer le risque et ses éléments constitutifs sont encore valables et cohérents avec les objectifs métiers, les stratégies et les politiques, et que les modifications apportées au contexte métier sont correctement prises en compte au cours du processus de gestion du risque en sécurité de l'information. Il convient que cette activité de surveillance et de réexamen réponde aux points suivants (sans toutefois s'y limiter) :

- le contexte légal et environnemental,
- le contexte concurrentiel,
- l'approche liée à l'appréciation du risque,
- la valeur et les catégories d'actifs,
- les critères d'impact,
- les critères d'évaluation du risque,
- les critères d'acceptation du risque,
- le coût total de maintenance,
- les ressources nécessaires.

Il convient que l'organisme s'assure que les ressources relatives à l'appréciation et au traitement du risque soient constamment disponibles pour réexaminer le risque, traiter des menaces ou des vulnérabilités nouvelles, ou modifiées et conseiller les dirigeants en conséquence.

La surveillance de la gestion du risque peut entraîner la modification ou l'enrichissement de l'approche, de la méthodologie ou des outils utilisés en fonction :

- des changements identifiés,
- de l'itération de l'appréciation du risque,
- de l'objectif du processus de gestion du risque en sécurité de l'information (par exemple, la continuité de l'activité, la résilience aux incidents, la conformité),
- du domaine d'application du processus de gestion du risque en sécurité de l'information (par exemple, l'organisme, l'entité opérationnelle, le processus d'informations, sa mise en œuvre technique, son application, sa connexion à Internet).

Élément de sortie : Pertinence permanente du processus de gestion du risque en sécurité de l'information avec les objectifs métiers de l'organisme ou mise à jour du processus.

Annex A
(informative)

Définition du domaine d'application et des limites du processus de gestion du risque en sécurité de l'information

A.1 Étude de l'organisme

Évaluer l'organisme L'étude de l'organisme rappelle les éléments caractéristiques qui définissent l'identité d'un organisme. Cette étude concerne l'objectif, l'activité, les missions, les valeurs et les stratégies de cet organisme. Il convient d'identifier ces éléments ainsi que les éléments contribuant à leur développement (par exemple, la sous-traitance).

La difficulté de cette activité consiste à comprendre parfaitement la manière dont l'organisme est structuré. L'identification de sa structure réelle permettra de comprendre le rôle et l'importance de chaque division dans le processus de réalisation des objectifs de l'organisme.

Par exemple, le fait que le responsable de la sécurité de l'information s'adresse aux hauts dirigeants, plutôt qu'aux gestionnaires des technologies de l'information, peut indiquer l'implication des hauts dirigeants dans le domaine de la sécurité de l'information.

Principal objectif de l'organisme L'objectif principal d'un organisme peut être défini comme la raison pour laquelle il existe (son domaine d'activité, son segment de marché, etc.).

Son activité L'activité de l'organisme, définie par les techniques et le savoir-faire de ses employés, lui permet de remplir ses missions. Elle est spécifique au domaine d'activité de l'organisme et définit souvent sa culture.

Sa mission L'organisme atteint son objectif en accomplissant sa mission. Afin d'identifier ses missions, il convient d'identifier les services fournis et/ou les produits fabriqués par rapport aux utilisateurs finaux.

Ses valeurs Les valeurs sont les principes majeurs ou le code de conduite bien défini appliqué à la pratique d'une activité. Elles peuvent concerner le personnel, les relations avec des agents extérieurs (clients, etc.), la qualité des produits ou des services fournis.

Prenons l'exemple d'un organisme dont l'objectif est le service public, dont l'activité est le transport et dont les missions comprennent le transport d'enfants de leur domicile à l'école, et inversement. Ses valeurs peuvent être la ponctualité du service et la sécurité pendant le transport.

Structure de l'organisme Il existe différents types de structure :

- structure divisionnaire : chaque division est placée sous l'autorité d'un chef de division responsable des décisions stratégiques, administratives et opérationnelles concernant son service,
- structure fonctionnelle : l'autorité fonctionnelle est exercée sur les procédures, la nature du travail et, parfois, les décisions ou la planification (par exemple, la production, les technologies de l'information, les ressources humaines, le marketing, etc.).

Remarques :

- Une division située au sein d'un organisme possédant une structure divisionnaire peut être organisée comme une structure fonctionnelle, et inversement ;
- Un organisme peut être considéré comme ayant une structure matricielle s'il possède des éléments empruntés aux deux types de structure ;
- Dans toute structure organisationnelle, il est possible de distinguer les niveaux suivants :
  - le niveau de processus décisionnel (définition des orientations stratégiques),
  - le niveau de leadership (coordination et management),
  - le niveau opérationnel (activités de production et de soutien).

Organigramme La structure de l'organisme est représentée sous forme de schéma dans un organigramme. Il convient que cette représentation souligne les axes hiérarchiques et de délégation de l'autorité, mais il convient qu'elle comprenne également d'autres relations qui, même si elles ne sont pas fondées sur une autorité formelle, sont cependant des flux d'informations.

Stratégie de l'organisme Cette stratégie requiert une expression formelle des principes directeurs de l'organisme. La stratégie de l'organisme détermine l'orientation et le développement nécessaires afin de tirer profit des problématiques en jeu et des changements majeurs qu'elle prévoit.

A.2 Liste des contraintes affectant l'organisme

Il convient de tenir compte de toutes les contraintes affectant l'organisme et déterminant l'orientation de sa sécurité de l'information. Leur source peut se trouver au sein de l'organisme, auquel cas, l'organisme les contrôle, ou en dehors de l'organisme et, par conséquent, ces contraintes ne sont en général pas négociables. Les contraintes liées aux ressources (budget, personnel) et aux urgences font partie des contraintes les plus importantes.

L'organisme définit ses objectifs (relatifs à son activité, son comportement, etc.) en s'engageant sur une certaine voie, probablement pour une longue période. Il définit ce qu'il souhaite devenir et les moyens à mettre en œuvre. En spécifiant cette voie, l'organisme tient compte des développements techniques et du savoir-faire, des souhaits exprimés par les utilisateurs, les clients, etc. Cet objectif peut être exprimé sous la forme de stratégies de fonctionnement ou de développement avec pour objectif, par exemple, de réduire les coûts d'exploitation, d'améliorer la qualité du service, etc.

Ces stratégies comprennent probablement des informations ainsi que le système d'informations (SI) prenant part à leur application. Par conséquent, les caractéristiques relatives à l'identité, à la mission et aux stratégies de l'organisme constituent des éléments fondamentaux de l'analyse du problème, puisque la violation d'un aspect lié à la sécurité de l'information peut contraindre à la reformulation de ces objectifs stratégiques. En outre, il est essentiel que les propositions liées aux exigences de sécurité de l'information restent cohérentes avec les règles, les usages et les moyens en vigueur au sein de l'organisme.

La liste des contraintes inclut les éléments suivants, sans toutefois s'y limiter :

Contraintes de nature politique

Ces contraintes peuvent concerner des administrations, des institutions publiques ou, de manière plus générale, toute organisation devant appliquer des décisions gouvernementales. Il s'agit habituellement de décisions relatives à l'orientation stratégique ou opérationnelle prises par une division d'administrations publiques ou un organisme décideur et qu'il convient d'appliquer.

Par exemple, l'informatisation des factures ou de documents administratifs engendre des problèmes liés à la sécurité de l'information.

Contraintes de nature stratégique

Les contraintes peuvent provenir de changements prévus ou potentiels apportés aux structures ou à l'orientation de l'organisme. Elles sont exprimées dans les programmes stratégiques ou opérationnels de l'organisme.

Par exemple, une coopération internationale destinée à partager des informations sensibles peut exiger des accords relatifs à la sécurisation de l'échange.

Contraintes territoriales

La structure et/ou l'objectif de l'organisme peuvent créer des contraintes spécifiques comme la distribution des sites sur l'ensemble du territoire national ou à l'étranger.

Par exemple, des services postaux, des ambassades, des banques, des filiales d'un grand groupe industriel, etc.

Contraintes liées au climat économique et politique

Le fonctionnement d'un organisme peut être profondément modifié par des événements spécifiques comme des grèves ou des crises nationales ou internationales.

Il convient, par exemple, que certains services soient en mesure de continuer à fonctionner même pendant une crise grave.

Contraintes structurelles

La nature de la structure d'un organisme (divisionnaire, fonctionnelle ou autre) peut conduire à une politique de sécurité de l'information spécifique et à une organisation de la sécurité adaptée à cette structure.

Par exemple, il convient qu'une structure internationale soit en mesure d'établir un lien entre les exigences de sécurité spécifiques à chaque pays.

Contraintes fonctionnelles

Les contraintes fonctionnelles résultent directement des missions générales ou spécifiques de l'organisme.

Par exemple, il convient qu'un organisme qui travaille 24 heures sur 24 s'assure que ses ressources sont toujours disponibles.

Contraintes liées au personnel

La nature de ces contraintes varie de manière considérable. Ces contraintes sont liées : au niveau de responsabilité, au recrutement, à la qualification, à la formation, à la sensibilisation à la sécurité, à la motivation, à la disponibilité, etc.

Par exemple, il convient que l'ensemble du personnel d'un organisme de défense soit autorisé à traiter des informations hautement confidentielles.

Contraintes liées au calendrier de l'organisme

Ces contraintes peuvent résulter de la restructuration ou de la mise en place de nouvelles politiques nationales ou internationales imposant certains délais.

Par exemple, la création d'un service de sécurité.

Contraintes liées aux méthodes

Il sera nécessaire d'imposer des méthodes adaptées au savoir-faire de l'organisme pour des aspects comme la planification d'un projet, ses spécifications, son développement, etc.

Une contrainte type de ce genre concerne, par exemple, le besoin d'introduire dans la politique de sécurité les obligations légales de l'organisme.

Contraintes de nature culturelle

Dans certains organismes, les habitudes de travail ou l'activité principale ont créé une « culture » spécifique au sein de l'organisme, qui peut s'avérer incompatible avec les contrôles de sécurité. Cette culture constitue le cadre de référence général du personnel lequel peut être déterminé par de nombreux aspects, y compris l'éducation, l'instruction, l'expérience professionnelle, l'expérience en-dehors du travail, les opinions, la philosophie, les croyances, le statut social, etc.

Contraintes budgétaires

Les mesures de sécurité recommandées peuvent parfois avoir un coût très élevé. Même s'il n'est pas toujours approprié de faire reposer des investissements liés à la sécurité sur la rentabilité, une justification économique est généralement exigée par le service financier de l'organisme.

Par exemple, dans le secteur privé et dans certains organismes publics, il convient que le coût total des mesures de sécurité ne soit pas supérieur au coût des conséquences éventuelles des risques. Il convient, par conséquent, que la direction évalue et prenne des risques calculés si elle souhaite éviter des coûts excessifs liés à la sécurité.

A.3 Liste des références législatives et réglementaires applicables à l'organisme

Il convient d'identifier les exigences réglementaires applicables à l'organisme. Ces exigences peuvent être des lois, des décrets, des règlements spécifiques au domaine de l'organisme ou des règlements internes ou externes. Elles concernent également les contrats et accords et d'une manière plus générale, toute obligation de nature légale ou réglementaire.

A.4 Liste des contraintes affectant le domaine d'application

En identifiant les contraintes, il est possible de dresser la liste de celles ayant un impact sur le domaine d'application et de déterminer lesquelles sont toutefois propices à l'action. Elles s'ajoutent aux contraintes de l'organisme définies ci-dessus, voire même les amendent. Les paragraphes suivants présentent une liste non exhaustive des types de contraintes possibles.

Contraintes liées aux processus préexistants

Les projets d'application ne sont pas nécessairement élaborés simultanément. Certains projets dépendent de processus préexistants. Même si un processus peut être divisé en sous-processus, il ne subit pas nécessairement l'influence de l'ensemble des sous-processus d'un autre processus.

Contraintes techniques

Les contraintes techniques relatives à l'infrastructure proviennent en général de matériels, de logiciels installés et de locaux, ou de sites hébergeant les processus :

- les dossiers (exigences concernant l'organisme, la gestion des supports, la gestion des règles d'accès, etc.),
- l'architecture générale (exigences relatives à la topologie (centralisée, répartie, client-serveur), à l'architecture physique, etc.),
- les logiciels d'application (exigences relatives à la conception de logiciels spécifiques, aux standards du marché, etc.),
- les progiciels (exigences relatives aux standards, au niveau d'évaluation, à la qualité, la conformité aux normes, à la sécurité, etc.),
- le matériel (exigences relatives aux standards, à la qualité, à la conformité aux normes, etc.),
- les réseaux de communication (exigences relatives à la couverture, aux standards, à la capacité, à la fiabilité, etc.),
- l'infrastructure des bâtiments (exigences relatives au génie civil, à la construction, aux hautes et basses tensions, etc.).

Contraintes financières

La mise en œuvre de mesures de sécurité est souvent limitée par le budget que l'organisme peut y consacrer. Toutefois, il convient que la contrainte financière soit toujours considérée en dernier lieu, puisque l'attribution du budget à la sécurité peut être négociée sur la base de l'étude de la sécurité.

Contraintes environnementales

Les contraintes environnementales proviennent de l'environnement géographique ou économique dans lequel les processus sont mis en œuvre : pays, climat, risques naturels, situation géographique, climat économique, etc.

Contraintes de temps

Il convient de tenir compte du temps nécessaire à la mise en œuvre des mesures de sécurité en cohérence avec la capacité de mettre à jour le système d'information ; si le temps de mise en œuvre est très long, les risques pour lesquels la mesure de sécurité a été conçue peuvent avoir changé. Le temps est un facteur déterminant dans le choix des solutions et des priorités.

Contraintes liées aux méthodes

Il convient d'utiliser des méthodes adaptées au savoir-faire de l'organisme pour la planification du projet, ses spécifications, son développement, etc.

Contraintes organisationnelles

Diverses contraintes peuvent apparaître à la suite des exigences organisationnelles :

- le fonctionnement (exigences relatives aux délais d'exécution, à la fourniture de services, à la surveillance, aux plans d'urgence, à la dégradation du fonctionnement, etc.),
- la maintenance (exigences relatives au diagnostic des incidents, aux actions préventives, à la correction rapide, etc.),
- la gestion des ressources humaines (exigences relatives à la formation des opérateurs et des utilisateurs, aux qualifications pour des postes d'administrateur système ou d'administrateur de données, etc.),
- la gestion administrative (exigences relatives aux responsabilités, etc.),
- la gestion du développement (exigences relatives aux outils de développement, au génie logiciel assisté par ordinateur, aux plans d'acceptation, à l'organisation à mettre en place, etc.),
- la gestion des relations extérieures (exigences relatives à l'organisation de relations avec des tiers, aux contrats, etc.).

Annex B
(informative)

Identification et évaluation des actifs et appréciation des impacts

B.1 Exemples d'identification des actifs

Afin de procéder à l'évaluation des actifs, il est nécessaire pour un organisme d'identifier ses actifs (à un niveau de détail approprié). Il est possible de distinguer deux types d'actifs :

- les actifs primordiaux :
  - processus et activités métier
  - informations
- les actifs en support (sur lesquels reposent les actifs primordiaux du domaine d'application) de tous les types :
  - matériel
  - logiciels
  - réseau
  - personnel
  - site
  - structure de l'organisme

B.1.1 Identification des actifs primordiaux

Pour décrire le domaine d'application de manière plus précise, cette activité consiste à identifier les actifs primordiaux (processus et activités métier, informations). Cette identification est effectuée par un groupe de travail mixte représentatif du processus (dirigeants, spécialistes et utilisateurs de systèmes d'information).

Les actifs primordiaux sont, en général, les processus centraux et informations de l'activité dans le domaine d'application. Il est également possible de considérer d'autres actifs primordiaux comme les processus de l'organisme, qui seront plus adaptés pour élaborer une politique de sécurité de l'information ou un plan de continuité de l'activité. Selon l'objectif, certaines études n'exigeront pas d'analyse exhaustive de l'ensemble des éléments constitutifs du domaine d'application. Dans ce cas, les limites de l'étude peuvent être réduites aux éléments clés du domaine d'application.

Il existe deux types d'actifs primordiaux :

1 – Les processus (ou sous processus) et activités métier, par exemple :

- les processus dont la perte ou la dégradation rend impossible la réalisation de la mission de l'organisme,
- les processus contenant des processus secrets ou les processus impliquant une technique brevetée,
- les processus qui, s'ils sont modifiés, peuvent considérablement affecter l'accomplissement de la mission de l'organisme,
- les processus qui sont nécessaires à l'organisme pour être conforme aux exigences contractuelles, légales ou réglementaires.

2 – Les informations :

D'une façon plus générale, les informations primordiales comprennent essentiellement :

- les informations vitales pour l'exercice de la mission ou de l'activité de l'organisme,
- les informations personnelles, telles que définies de manière spécifique par la législation nationale relative à la vie privée,
- les informations stratégiques requises pour atteindre les objectifs définis par les orientations stratégiques,
- les informations à forte valeur financière dont la collecte, le stockage, le traitement et la transmission nécessitent un long délai et/ou impliquent un coût d'acquisition élevé.

Les processus et informations, qui ne sont pas jugés sensibles, après cette activité n'auront aucune classification dans le reste de l'étude. Cela signifie que même si ces processus et informations sont compromis, l'organisme parviendra malgré tout à accomplir la mission.

Toutefois, ils exigeront souvent la mise en œuvre de mesures de sécurité afin de protéger les processus et informations jugés sensibles.

B.1.2 Liste et description des actifs en support

Le domaine d'application se compose d'actifs qu'il convient d'identifier et de décrire. Ces actifs présentent des vulnérabilités exploitables par des menaces visant à affaiblir les actifs primordiaux du domaine d'application (processus et informations). Ils sont de divers types :

Matériel

Le type relatif au matériel se compose de tous les éléments physiques prenant en charge des processus.

Equipement de traitement des données (actif)

Equipement automatique de traitement de l'information comprenant les éléments nécessaires pour fonctionner de manière indépendante.

Equipement transportable

Equipement informatique portable.

Exemples : ordinateur portable, PDA (Personal Digital Assistant).

Equipement fixe

Equipement informatique utilisé dans les locaux de l'organisme.

Exemples : serveur, microordinateur utilisé comme poste de travail.

Périphériques de traitement

Equipement relié à un ordinateur via un port de communication (lien en série, lien parallèle, etc.) pour saisir, transporter ou transmettre des données.

Exemples : imprimante, lecteur de disque amovible.

Support de données (passif)

Il s'agit de supports destinés à stocker des données ou des fonctions.

Support électronique

Support d'information pouvant être relié à un ordinateur ou à un réseau informatique afin de stocker des données. Malgré leur taille compacte, ces supports peuvent contenir de nombreuses données. Ils peuvent être utilisés avec un équipement informatique standard.

Exemples : disquette, CD ROM, cartouche de secours, disque dur amovible, clé USB, cassette.

Autres supports

Supports statiques et non électriques contenant des données.

Exemples : papier, diapositive, transparent, documentation, fax.

Logiciels

Les logiciels comprennent tous les programmes contribuant au fonctionnement d'un ensemble de traitement de données.

Système d'exploitation

Ce système inclut tous les programmes d'un ordinateur qui constituent la base opérationnelle à partir de laquelle tous les autres programmes (services ou applications) sont gérés. Il comporte un noyau et des fonctions, ou des services de base. Selon l'architecture, un système d'exploitation peut être monolithique ou constitué d'un micronoyau et d'un ensemble de services fonctionnels. Les principaux éléments du système d'exploitation sont tous des services de gestion du matériel (unité centrale, mémoire, disque et interfaces réseau), les services de gestion des tâches ou des processus ainsi que les services de gestion des droits utilisateurs.

Logiciels de service, de maintenance ou d'administration

Logiciel caractérisé par le fait qu'il complète les services du système d'exploitation et qu'il ne situe pas directement au service des utilisateurs ou des applications (même s'il est souvent essentiel, voire indispensable au fonctionnement d'ensemble du système d'information).

Progiciel ou logiciel standard

Les logiciels standards ou progiciels sont des produits complets commercialisés comme tels (plutôt que comme exemplaire unique ou comme développements spécifiques) avec un support, une version et une maintenance. Ils fournissent des services destinés aux utilisateurs et aux applications, mais ne sont pas personnalisés ou spécifiques comme le sont les applications de gestion.

Exemples : logiciel de gestion de base de données, logiciel de messagerie électronique, groupware, logiciel d'annuaire, logiciel serveur, etc.

Applications métier

Application métier standard

Il s'agit d'un logiciel commercial conçu pour donner aux utilisateurs un accès direct aux services et aux fonctions qu'ils exigent de leur système d'information dans le cadre de leur profession. Il existe une très large gamme de domaines, illimitée en théorie.

Exemples : logiciel de comptabilité, logiciel de commande de machines outils, logiciel d'assistance clientèle, logiciel de gestion des compétences personnelles, logiciel administratif, etc.

Application métier spécifique

Il s'agit d'un logiciel dont divers aspects (principalement le soutien, la maintenance, la mise à jour, etc.) ont été spécialement conçus pour donner aux utilisateurs un accès direct aux services et fonctions qu'ils exigent de leur système d'information. Il existe une très large gamme de domaines, illimitée en théorie.

Exemples : Gestion des factures de clients d'opérateurs téléphoniques, application de surveillance en temps réel pour le lancement de fusée.

Réseau

Le type de réseau comprend tous les dispositifs de télécommunication utilisés pour interconnecter plusieurs ordinateurs ou éléments distants d'un système d'information.

Supports

Les supports ou matériels de communication et de télécommunication s'identifient principalement aux caractéristiques physiques et techniques de l'équipement (point à point, diffusion) et aux protocoles de communication (lien ou réseau – niveaux 2 et 3 de modèle de couche OSI 7).

Exemples : Réseau téléphonique commuté public (RTCP), Ethernet, GigabitEthernet, ADSL (Ligne d'abonné numérique asymétrique), spécifications de protocole sans fil (par exemple WiFi 802.11), Bluetooth, FireWire.

Relais actif ou passif

Ce sous-type comprend tous les dispositifs qui ne sont pas des terminaisons logiques de communication (vision SI), mais des dispositifs intermédiaires ou de relais. Les relais se caractérisent par les protocoles de communication par réseau pris en charge. Hormis le relais de base, ils comprennent souvent des fonctions et des services de routage et/ou de filtrage, en utilisant des sélecteurs de radiocommunication et des routeurs avec filtres. Ils peuvent souvent être gérés à distance et sont, en général, capables de générer des journaux.

Exemples : pont, routeur, concentrateur, sélecteur, central automatique.

Interface de communication

Les interfaces de communication des unités centrales sont reliées à ces unités centrales mais se caractérisent par les supports et les protocoles pris en charge, par tout filtrage installé, des fonctions et capacités de génération de journal ou d'avertissement et par la possibilité et l'exigence d'administration à distance.

Exemples : GPRS (service général de paquets radio), adaptateur Ethernet.

Personnel

Le personnel comprend tous les groupes de personnes impliqués dans le système d'information.

Décideur

Les décideurs sont les propriétaires des actifs primordiaux (informations et fonctions) ainsi que les dirigeants de l'organisme ou du projet spécifique.

Exemples : direction générale, chef de projet.

Utilisateurs

Les utilisateurs représentent les membres du personnel qui manipulent des éléments sensibles dans le cadre de leur activité et ont une responsabilité spéciale à cet égard. Ils peuvent avoir des droits d'accès spéciaux au système d'information afin d'effectuer leurs tâches quotidiennes.

Exemples : gestion des ressources humaines, gestion financière, gestionnaire de risques.

Personnel d'exploitation / de maintenance

Il s'agit du personnel en charge de l'exploitation et de la maintenance du système d'information. Ils disposent de droits d'accès spéciaux au système d'information afin d'effectuer leurs tâches quotidiennes.

Exemples : administrateur système, administrateur de données, back-up, centre d'assistance, opérateur de télédistribution, responsables de la sécurité.

Développeurs

Les développeurs sont chargés de développer les applications d'un organisme. Ils ont accès à une partie du système d'information grâce à des droits de haut niveau mais n'effectuent aucune action sur les données de production.

Exemples : développeurs d'applications de gestion.

Site

Le site comprend tous les emplacements contenant le domaine d'application ou une partie du domaine d'application ainsi que les moyens physiques requis pour que ce domaine fonctionne.

Emplacement

Environnement extérieur

Il concerne tous les emplacements au sein desquels les moyens de sécurité de l'organisme ne peuvent s'appliquer.

Exemples : résidence du personnel, locaux d'un autre organisme, environnement situé à l'extérieur du site (zone urbaine, zone dangereuse).

Locaux

Cet endroit est délimité par le périmètre de l'organisme directement en contact avec l'extérieur. Il peut s'agir d'une limite physique de protection obtenue en créant des barrières physiques ou des dispositifs de surveillance autour des bâtiments.

Exemples : établissement, bâtiments.

Zone

Une zone est formée par une limite physique de protection créant des cloisons dans les locaux d'un organisme. Elle est obtenue en créant des barrières physiques autour des infrastructures de traitement de l'information de l'organisme.

Exemples : bureaux, zone d'accès réservé, zone sécurisée.

Services essentiels

Tous les services nécessaires au fonctionnement du matériel d'un organisme.

Communication

Services et matériel de télécommunications fournis par un opérateur.

Exemples : ligne téléphonique, PABX (installation automatique d'abonnés avec postes supplémentaires), réseaux téléphoniques internes.

Utilitaires

Services et moyens (sources et câblage) nécessaires pour alimenter le matériel et les périphériques de technologie de l'information.

Exemples : alimentation électrique basse tension, onduleur, centre distributeur d'un circuit électrique.

Alimentation en eau

Traitement des déchets

Services et moyens (matériel, contrôle) destinés à rafraîchir et à purifier l'air.

Exemples : conduites d'eau fraîche, appareil de climatisation.

Organisme

L'organisme décrit le cadre organisationnel, composé de l'ensemble des structures de personnel dédiées à une tâche ainsi que les procédures destinées à contrôler ces structures.

Autorités

Il s'agit d'organismes desquels l'organisme étudié tire son autorité. Ils peuvent être légalement affiliés ou externes. Les autorités imposent sur l'organisme étudié des contraintes en termes de réglementation, de décisions et d'actions.

Exemples : entité responsable, siège social d'un organisme.

Structure de l'organisme

Elle comprend les différentes branches de l'organisme, y compris ses activités transverses, sous le contrôle de sa gestion.

Exemples : gestion des ressources humaines, gestion des technologies de l'information, gestion des achats, gestion des entités opérationnelles, service de sécurité des bâtiments, service incendie, gestion des audits.

Organisation de projet ou de système

Elle concerne l'organisation définie pour un projet ou un service spécifique.

Exemples : nouveau projet de développement d'une application, projet de migration d'un système d'information.

Sous-traitants / Fournisseurs / Fabricants

Il s'agit d'organismes qui fournissent à l'organisme un service ou des ressources et qui y sont liés par un contrat.

Exemples : entreprise de gestion des locaux, entreprise de sous-traitance, cabinets de consultants.

B.2 Évaluation des actifs

L'étape suivant l'identification des actifs consiste à déterminer l'échelle à utiliser, ainsi que les critères destinés à attribuer à chaque actif un emplacement spécifique sur cette échelle, sur la base d'une évaluation. En raison de la diversité des actifs détectés dans la plupart des organismes, il est probable que certains actifs ayant une valeur monétaire connue soient évalués dans l'unité monétaire locale, tandis que d'autres ayant une valeur plus qualitative se voient attribuer une plage de valeurs, allant par exemple de « très faible » à « très élevée ». La décision d'utiliser une échelle quantitative, plutôt qu'une échelle qualitative, relève véritablement d'une question de préférence organisationnelle, mais il convient qu'elle soit cohérente avec les actifs évalués. Les deux types d'évaluation peuvent être utilisés pour le même actif.

Les termes type utilisés pour l'évaluation qualitative des actifs comprend des termes comme : négligeable, très faible, faible, moyenne, élevée, très élevée et critique. Le choix et la gamme de termes adaptés à un organisme dépendent fortement de ses besoins en termes de sécurité, de sa taille en termes d'organisation et d'autres facteurs spécifiques à l'organisme.

Critères

Il convient de définir à l'aide de termes sans équivoque les critères utilisés comme base pour attribuer une valeur à chaque actif. Il s'agit souvent d'un des aspects les plus difficiles de l'évaluation des actifs, car il peut s'avérer nécessaire de déterminer les valeurs de certains actifs de manière subjective et également parce que de nombreuses personnes différentes sont susceptibles d'effectuer cette détermination. Les critères pouvant être utilisés pour déterminer la valeur d'un actif comprennent son coût d'origine, son coût de remplacement ou de re-création ; sa valeur peut également être abstraite, par exemple la valeur de la réputation d'un organisme.

Une autre méthode d'évaluation des actifs repose sur les frais générés par une perte de confidentialité, d'intégrité et de disponibilité suite à un incident. Il convient également de tenir compte, le cas échéant, de la non-répudiation, de l'imputabilité, de l'authenticité et de la fiabilité. Cette évaluation fournit les principaux axes de valeur des actifs, en plus du coût de remplacement, en fonction des estimations des conséquences métier défavorables résultant d'incidents liés à la sécurité, conjugués avec un ensemble présumé de circonstances. Il faut souligner que cette approche tient compte des conséquences qui sont nécessaires à prendre en considération lors de l'appréciation du risque.

De nombreux actifs peuvent se voir attribuer plusieurs valeurs au cours de cette évaluation. Par exemple : un plan d'activités peut être évalué sur la base du travail effectué pour élaborer ce plan, sur la base du travail effectué pour saisir les données mais, aussi, sur la base de sa valeur par rapport à un concurrent. Chacune des valeurs attribuées varie très vraisemblablement de manière considérable. La valeur attribuée peut être la valeur maximale de toutes les valeurs possibles, la somme de certaines valeurs ou l'ensemble des valeurs possibles. Dans l'analyse finale, il convient de déterminer avec soin quelles valeurs sont attribuées à un actif, puisque la valeur finale attribuée intervient dans la détermination des ressources utilisées pour la protection de l'actif.

Réduction à une base commune

Finalement, toutes les évaluations d'actifs doivent être réduites à une base commune. Cette réduction s'effectue à l'aide des critères énoncés ci-dessous. Les critères susceptibles d'être utilisés pour évaluer les conséquences possibles résultant d'une perte de confidentialité, d'intégrité, de disponibilité, de non-répudiation, d'imputabilité, d'authenticité ou de fiabilité des actifs sont :

- la violation de la législation et/ou d'une réglementation,
- une déficience des performances de l'activité,
- une perte de réputation/un effet négatif sur la réputation,
- une violation associée aux informations personnelles,
- une atteinte à la sécurité personnelle,
- des effets défavorables pour l'application des lois,
- un manquement à l'obligation de confidentialité,
- une atteinte à l'ordre public,
- une perte financière,
- une interruption des activités,
- une atteinte à la sécurité environnementale.

Une autre approche destinée à évaluer les conséquences peut être :

- une interruption de service :
  - une incapacité à fournir le service,
- la perte de confiance d'un client :
  - la perte de crédibilité dans le système d'information interne,
  - une atteinte à la réputation,
- une interruption de fonctionnement interne :
  - une défaillance de l'organisme lui-même,
  - le coût interne supplémentaire,
- une interruption de fonctionnement d'un tiers :
  - une interruption d'une transaction entre un tiers et l'organisme,
  - divers types de préjudice,
- une violation de lois / réglementations :
  - une incapacité à remplir ses obligations légales,
- une rupture de contrat :
  - une incapacité à remplir ses obligations contractuelles,
- un danger compromettant la sécurité du personnel / des utilisateurs :
  - un danger pour le personnel et / ou les utilisateurs,
- une atteinte à la vie privée des utilisateurs,
- des pertes financières,
- des coûts financiers d'urgence ou de réparation :
  - en termes de personnel,
  - en termes d'équipement,
  - en termes d'études, de rapports d'experts,
- des pertes de biens / de fonds / d'actifs,
- des pertes de clients ou de fournisseurs,
- des procédures et peines judiciaires,
- une perte d'avantage concurrentiel ;
- une perte d'avance technologique / technique,

- une perte d'efficacité / de confiance,
- une perte de réputation technique,
- un affaiblissement de la capacité de négociation,
- une crise industrielle (grèves),
- une crise gouvernementale,
- une mise au chômage technique,
- des préjudices matériels.

Ces critères sont des exemples de problématiques à considérer lors de l'évaluation des actifs. Pour réaliser ces évaluations, un organisme doit choisir des critères adaptés à son type d'activité et à ses exigences en matière de sécurité. Cela peut signifier que certains des critères présentés ci-dessus ne sont pas applicables, et que d'autres peuvent être ajoutés à cette liste.

Échelle

Une fois établis les critères à considérer, il convient que l'organisme convienne d'une échelle à utiliser. La première étape consiste à déterminer le nombre de niveaux à utiliser. Il n'existe aucune règle relative au nombre de niveaux le plus adapté. Un plus grand nombre de niveaux fournit un niveau de granularité plus important mais, parfois, une différentiation plus précise rend plus difficiles les attributions dans l'organisme. Il est normalement possible d'utiliser tous les nombres de niveaux compris entre 3 (par exemple, faible, moyen et élevé) et 10 tant que ce nombre est cohérent avec l'approche utilisée par l'organisme pour l'ensemble du processus d'appréciation du risque.

Un organisme peut définir ses propres valeurs d'actifs, comme « faible », « moyenne » ou « élevée ». Il convient d'évaluer ces limites conformément aux critères choisis (par exemple, dans le cas d'une éventuelle perte financière, il convient de les présenter sous forme de valeurs monétaires mais, dans le cas de considérations telles qu'une atteinte à la sécurité personnelle, une évaluation monétaire peut s'avérer complexe et non adaptée à tous les organismes). Enfin, il incombe entièrement à l'organisme de décider ce qui est considéré comme une conséquence « faible » ou « élevée ». Une conséquence désastreuse pour un petit organisme peut paraître faible, voire même négligeable pour un très grand organisme.

Dépendances

Plus les processus métier pris en charge par un actif sont pertinents et nombreux, plus la valeur de cet actif est importante. Il convient d'identifier également les dépendances des actifs par rapport aux processus métier et aux autres actifs, puisque cela peut avoir une influence sur les valeurs des actifs. Par exemple, il convient de protéger la confidentialité des données pendant tout leur cycle de vie, et ce à toutes les étapes, y compris le stockage et le traitement, c'est-à-dire qu'il convient de relier directement les besoins relatifs à la sécurité des programmes de stockage et de traitement des données à la valeur représentant la confidentialité des données stockées et traitées. De plus, si un processus métier repose sur l'intégrité de certaines données produites par un programme, il convient que les données d'entrée de ce programme soient suffisamment fiables. En outre, l'intégrité des informations dépendra du matériel et des logiciels utilisés pour leur stockage et leur traitement. Ainsi, le matériel dépendra de l'alimentation électrique et éventuellement de la climatisation. Les informations relatives aux dépendances faciliteront donc l'identification des menaces mais, surtout, des vulnérabilités. Elles contribueront également à garantir que la valeur réelle des actifs (à travers les relations de dépendance) soit donnée aux actifs, indiquant ainsi le niveau de protection adapté.

Les valeurs des actifs, dont d'autres actifs dépendent, peuvent être modifiées de la manière suivante :

- si les valeurs des actifs dépendants (par exemple, des données) sont inférieures ou égales à la valeur de l'actif considéré (par exemple un logiciel), sa valeur reste la même,

- si les valeurs des actifs dépendants (par exemple des données) sont supérieures, alors il convient d'augmenter la valeur de l'actif considéré (par exemple, un logiciel) conformément :
  - au degré de dépendance,
  - aux valeurs des autres actifs.

Un organisme peut posséder des actifs qui sont disponibles plus d'une fois, comme des copies de programmes logiciels ou le même type d'ordinateur utilisé dans la plupart des bureaux. Il est important d'en tenir compte en procédant à l'évaluation des actifs. D'une part, ces actifs sont facilement ignorés, par conséquent, il convient de les identifier tous ; d'autre part, ils peuvent être utilisés pour réduire les problèmes de disponibilité.

Sortie

L'élément final de sortie de cette étape est une liste d'actifs et de leurs valeurs par rapport à la divulgation (préservation de la confidentialité), la modification (préservation de l'intégrité, de l'authenticité, de la non-répudiation et de l'imputabilité), la non-disponibilité, la destruction (préservation de la disponibilité et de la fiabilité) et du coût de remplacement.

B.3 Appréciation des impacts

Un incident lié à la sécurité de l'information peut affecter plus d'un actif ou seulement une partie d'un actif. Cet impact est lié au niveau de succès de l'incident. Par conséquent, il existe une différence importante entre la valeur de l'actif et l'impact résultant de l'incident. On considère qu'un impact a soit un effet immédiat (opérationnel), soit un effet futur (lié à l'activité) qui inclut des conséquences financières et commerciales.

Un impact immédiat (opérationnel) est direct ou indirect.

Direct :

a) la valeur financière de remplacement d'un actif (ou d'une partie d'un actif) perdu,

b) le coût d'acquisition, de configuration et d'installation du nouvel actif ou de sauvegarde,

c) le coût des opérations interrompues en raison de l'incident jusqu'à ce que le service fourni par le ou les actifs soit restauré,

d) les résultats d'impact d'une violation de la sécurité de l'information.

Indirect :

a) le coût de l'opportunité (les ressources financières nécessaires pour remplacer ou réparer un actif qui aurait été utilisé ailleurs),

b) le coût des opérations interrompues,

c) le mauvais usage potentiel des informations obtenues en raison d'une atteinte à la sécurité,

d) la violation des obligations statutaires ou réglementaires,

e) la violation des codes éthiques de conduite.

Ainsi, la première appréciation (sans aucune mesure de quelque sorte) estimera un impact très près de la(les) (combinaison de) valeur(s) de l'actif concerné. En cas d'itération supplémentaire concernant cet(ces) actif(s), l'impact sera différent (en général nettement moins important) en raison de la présence et de l'efficacité des mesures de sécurité mises en œuvre.

Annex C
(informative)
Exemples de menaces type

Le tableau suivant donne des exemples de menaces type. Cette liste peut être utilisée lors du processus d'appréciation des menaces. Les menaces peuvent être délibérées, accidentelles ou environnementales (naturelles), et peuvent résulter, à titre d'exemples, de dommages ou de la perte de services essentiels. La liste suivante indique pour chaque type de menace si D (délibérée), A (accidentelle) ou E (environnementale) s'applique. D est utilisé pour les actions délibérées destinées aux actifs informationnels, A est utilisé pour toutes les actions humaines qui peuvent endommager les actifs informationnels de manière accidentelle et E est utilisé pour tous les incidents qui ne reposent pas sur des actions humaines. Les groupes de menaces ne sont pas classés par ordre de priorité.

Type	Menaces	Origine
Dommage physique	Incendie	A, D, E
	Dégât des eaux	A, D, E
	Pollution	A, D, E
	Accident majeur	A, D, E
	Destruction de matériel ou de support	A, D, E
	Poussière, corrosion, congélation	A, D, E
Catastrophes naturelles	Phénomène climatique	E
	Phénomène sismique	E
	Phénomène volcanique	E
	Phénomène météorologique	E
	Inondation	E
Perte de services essentiels	Panne du système de climatisation ou d'alimentation en eau	A, D
	Perte de la source d'alimentation en électricité	A, D, E
	Panne du matériel de télécommunications	A, D
Perturbation due à des rayonnements	Rayonnements électromagnétiques	A, D, E
	Rayonnements thermiques	A, D, E
	Impulsions électromagnétiques	A, D, E
Compromission d'informations	Interception de signaux d'interférence compromettants	D
	Espionnage à distance	D
	Ecoute	D
	Vol de supports ou de documents	D
	Vol de matériel	D
	Récupération de supports recyclés ou mis au rebut	D
	Divulgation	A, D
	Données provenant de sources douteuses	A, D
	Piégeage de matériel	D
	Piégeage de logiciel	A, D
	Géolocalisation	D
Défaillances techniques	Panne de matériel	A
	Dysfonctionnement du matériel	A
	Saturation du système d'information	A, D
	Dysfonctionnement du logiciel	A
	Violation de la maintenabilité du système d'information	A, D
Actions non autorisées	Utilisation non autorisée du matériel	D
	Reproduction frauduleuse de logiciel	D
	Utilisation de logiciels copiés ou de contrefaçon	A, D
	Corruption de données	D
	Traitement illégal de données	D
Compromission des fonctions	Erreur d'utilisation	A
	Abus des droits	A, D
	Usurpation de droits	D
	Déni d'actions	D
	Violation de la disponibilité du personnel	A, D, E

Il convient de prêter une attention particulière aux sources de menace humaines. Ces sources sont présentées en détail de manière spécifique dans le tableau suivant :

Origine de la menace	Motivation	Conséquences possibles
Pirate informatique	Défi Amour-propre Rébellion Statut Argent	• Piratage informatique • Ingénierie sociale • Intrusion, introductions par effraction dans un système • Accès non autorisé dans un système
Escroc informatique	Destruction d'informations Divulgation illégale d'informations Gain financier Modification non autorisée de données	• Délit informatique (par exemple harcèlement par Internet) • Acte frauduleux (par exemple réémission, usurpation d'identité, interception) • Corruption d'informations • Usurpation • Intrusion dans un système
Terroriste	Chantage Destruction Exploitation Vengeance Avantage politique Couverture médiatique	• Bombe/Terrorisme • Guerre de l'information • Attaque du système (par exemple déni de service distribué) • Pénétration dans un système • Piégeage d'un système
Espionnage industriel (Renseignement, entreprises, gouvernements étrangers, intérêts d'autres gouvernements)	Avantage concurrentiel Espionnage économique	• Avantage en matière de défense • Avantage politique • Exploitation économique • Vol d'informations • Intrusion dans la vie privée • Ingénierie sociale • Pénétration dans un système • Accès non autorisé à un système (accès à des informations classées, propriétaires et/ou liées à la technologie)
Initiés (employés peu qualifiés, mécontents, malveillants, négligents, malhonnêtes ou ex-employés)	Curiosité Amour-propre Renseignement Gain financier Vengeance Erreurs et omissions involontaires (par exemple erreur de saisie des données, erreur de programmation)	• Agression d'un employé • Chantage • Exploration d'informations propriétaires • Malveillance informatique • Fraude et vol • Corruption d'informations • Saisie de données falsifiées, corrompues • Interception • Code malveillant (par exemple virus, bombe logique, cheval de Troie) • Vente d'informations personnelles • Bugs du système • Intrusion dans un système • Sabotage d'un système • Accès non autorisé dans un système

Annex D
(informative)
Vulnérabilités et méthodes d'appréciation des vulnérabilités

D.1 Exemples de vulnérabilités

Le tableau suivant fournit des exemples de vulnérabilités dans divers domaines de sécurité, y compris des exemples de menaces susceptibles d'exploiter ces vulnérabilités. Les listes peuvent contribuer, lors de l'appréciation des menaces et des vulnérabilités, à déterminer des scénarii d'incident pertinents. Il faut souligner que, dans certains cas, d'autres menaces peuvent également exploiter ces vulnérabilités.

Types	Exemples de vulnérabilités	Exemples de menaces
Matériel	Maintenance insuffisante/mauvaise installation des supports de stockage	Violation de la maintenabilité du système d'information
	Absence de programmes de remplacement périodique	Destruction de matériel ou de support
	Sensibilité à l'humidité, à la poussière, aux salissures	Poussière, corrosion, congélation
	Sensibilité aux rayonnements électromagnétiques	Rayonnements électromagnétiques
	Absence de contrôle efficace de modification de configuration	Erreur d'utilisation
	Sensibilité aux variations de tension	Perte de la source d'alimentation en électricité
	Sensibilité aux variations de température	Phénomène météorologique
	Stockage non protégé	Vol de supports ou de documents
	Manque de prudence lors de la mise au rebut	Vol de supports ou de documents
	Reproduction non contrôlée	Vol de supports ou de documents
Logiciel	Tests de logiciel absents ou insuffisants	Abus de droits
	Failles bien connues dans le logiciel	Abus de droits
	Pas de fermeture de session en quittant le poste de travail	Abus de droits
	Mise au rebut et réutilisation de supports de stockage 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 programmes de gestion à de mauvaises données en termes de temps	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

(*à suivre*)

(*suite*)

Types	Exemples de vulnérabilités	Exemples de menaces
Logiciel (fin)	Absence de mécanismes d'identification et d'authentification tels que l'authentification des utilisateurs	Usurpation de droits
	Tableaux de mots de passe non protégés	Usurpation de droits
	Mauvaise gestion des mots de passe	Usurpation de droits
	Activation de services non nécessaires	Traitement illégal de données
	Logiciel neuf ou en phase de rodage	Dysfonctionnement du logiciel
	Spécifications des développeurs confuses ou incomplètes	Dysfonctionnement du logiciel
	Absence de contrôle efficace des modifications	Dysfonctionnement du logiciel
	Chargement et utilisation non contrôlés du logiciel	Piégeage de logiciel
	Absence de copies de sauvegarde	Piégeage de logiciel
	Absence de protection physique du bâtiment, des portes et des fenêtres	Vol de supports ou de documents
	Impossibilité de produire les comptes-rendus de gestion	Utilisation non autorisée du matériel
Réseau	Absence de preuves d'envoi ou de réception d'un message	Déni d'actions
	Voies de communication non protégées	Ecoute
	Trafic sensible non protégé	Ecoute
	Mauvais câblage	Panne du matériel de télécommunications
	Point de défaillance unique	Panne du matériel de télécommunications
	Absence d'identification et d'authentification de l'expéditeur et du destinataire	Usurpation de droits
	Architecture réseau non sécurisée	Espionnage à distance
	Transfert de mots de passe en clair	Espionnage à distance
	Gestion réseau inadaptée (résilience du routage)	Saturation du système d'information
	Connexions au réseau public non protégées	Utilisation non autorisée du matériel
Personnel	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 mécanismes de surveillance	Traitement illégal de données
	Travail non surveillé d'une équipe extérieure ou de l'équipe d'entretien	Vol de supports ou de documents
	Absence de politiques relatives à la bonne utilisation de supports de télécommunications et de la messagerie	Utilisation non autorisée du matériel

(*à suivre*)

(*suite*)

Types	Exemples de vulnérabilités	Exemples de menaces
Site	Utilisation inadaptée ou négligente du contrôle d'accès physique aux bâtiments et aux salles	Destruction de matériel ou de support
	Emplacement situé dans une zone sujette aux inondations	Inondation
	Réseau électrique instable	Perte de la source d'alimentation en électricité
	Absence de protection physique du bâtiment, des portes et des fenêtres	Vol de matériel
Organisme	Absence de procédure formelle relative à l'enregistrement et au retrait des utilisateurs	Abus de droits
	Absence de processus formel relatif au réexamen des droits d'accès (supervision)	Abus de droits
	Absence de dispositions suffisantes (relatives à la sécurité) dans les contrats avec des clients et/ou des tiers	Abus de droits
	Absence de procédure de surveillance des moyens de traitement de l'information	Abus de droits
	Absence d'audits réguliers (supervision)	Abus de droits
	Absence de procédures d'identification et d'appréciation du risque	Abus de droits
	Absence de rapports d'erreur enregistrés dans les journaux administrateurs et les journaux opérations	Abus de droits
	Réponse inadaptée du service de maintenance	Violation de la maintenabilité du système d'information
	Accord de service absent ou insuffisant	Violation de la maintenabilité du système d'information
	Absence de procédure de contrôle des modifications	Violation de la maintenabilité du système d'information
	Absence de procédure formelle du contrôle de la documentation SMSI	Corruption de données
	Absence de procédure formelle de supervision des enregistrements SMSI	Corruption de données
	Absence de processus formel d'autorisation des informations à disposition du public	Données provenant de sources douteuses
	Absence de bonne attribution des responsabilités en sécurité de l'information	Déni d'actions
	Absence de plans de continuité	Panne de matériel
	Absence de politique relative à l'utilisation des emails	Erreur d'utilisation
	Absence de procédures d'introduction d'un logiciel dans des systèmes d'exploitation	Erreur d'utilisation

(*à suivre*)

(*fin*)

Types	Exemples de vulnérabilités	Exemples de menaces
Organisme (fin)	Absence d'enregistrements dans les journaux administrateurs et journaux opérations	Erreur d'utilisation
	Absence de procédures relatives au traitement de l'information classée	Erreur d'utilisation
	Absence de responsabilités en sécurité de l'information dans les descriptions de poste	Erreur d'utilisation
	Dispositions absentes ou insuffisantes (relatives à la sécurité de l'information) dans les contrats avec les employés	Traitement illégal de données
	Absence de processus disciplinaire défini en cas d'incident en sécurité de l'information	Vol de matériel
	Absence de politique formelle relative à l'utilisation des ordinateurs portables	Vol de matériel
	Absence de contrôle des actifs situés hors des locaux	Vol de matériel
	Politique absente ou insuffisante relative au « bureau propre et à l'écran vide »	Vol de supports ou de documents
	Absence d'autorisation relative aux moyens de traitement de l'information	Vol de supports ou de documents
	Absence de mécanismes de surveillance établis pour des violations de sécurité	Vol de supports ou de documents
	Absence de revues de direction régulières	Utilisation non autorisée du matériel
	Absence de procédures de signalement des failles de sécurité	Utilisation non autorisée du matériel
	Absence de procédures de la conformité des dispositions aux droits de propriété intellectuelle	Utilisation de logiciels copiés ou de contrefaçon

A.5 Méthodes d'appréciation des vulnérabilités techniques

Il est possible d'utiliser des méthodes proactives comme des tests du système d'information afin d'identifier les vulnérabilités par rapport à la criticité du système de technologie de l'information, des communications (TIC) et des ressources disponibles (par exemple fonds attribués, technologie disponible, personnes détenant le savoir-faire nécessaire pour mener les essais). Les méthodes de tests comprennent :

- outil automatisé d'analyse de vulnérabilités,
- test et évaluation de sécurité,
- tests d'intrusion,
- revue de code.

L'outil automatisé d'analyse de vulnérabilités est utilisé pour analyser un groupe d'hôtes, ou un réseau, afin de détecter les services vulnérables connus (par exemple, un système permettant un protocole de transfert de fichier (FTP), un relais sendmail. Toutefois, il convient de noter que certaines vulnérabilités potentielles identifiées par l'outil automatisé d'analyse peuvent ne pas représenter les vulnérabilités réelles dans le contexte de l'environnement du système. Par exemple, certains outils d'analyse considèrent des vulnérabilités potentielles sans tenir compte de l'environnement et des exigences du site. Certaines vulnérabilités détectées par le logiciel d'analyse automatisé peuvent ne pas être vulnérables pour un site spécifique mais peuvent être configurées de cette manière parce que leur environnement l'exige. Par conséquent, cette méthode de tests peut générer de faux positifs.

Il est également possible d'utiliser une autre technique, celle des tests et de l'évaluation de sécurité (STE), en identifiant les vulnérabilités d'un système TIC lors du processus d'appréciation du risque. Cette méthode comprend l'élaboration et l'exécution d'un protocole de test (à titre d'exemples, script de test, procédures de test et résultats d'essai attendus). L'objectif des tests de sécurité du système est de mettre à essai l'efficacité des mesures de sécurité d'un système TIC telles qu'elles ont été mises en œuvre dans un environnement opérationnel. Le but est de garantir que les mesures appliquées répondent aux spécifications de sécurité validées en termes de matériel et de logiciel, de mettre en œuvre la politique de sécurité de l'organisme ou d'assurer la conformité aux normes de l'industrie.

Les tests d'intrusion peuvent être utilisés pour compléter le réexamen des mesures de sécurité et garantir que les différents aspects du système TIC sont sécurisés. Lorsqu'ils sont utilisés au cours du processus d'appréciation du risque, les tests d'intrusion peuvent être utilisés pour évaluer la capacité d'un système TIC à résister aux tentatives volontaires de contourner la sécurité du système. Leur objectif est de mettre le système TIC à essai du point de vue de la source de menace et d'identifier les défaillances potentielles des schémas de protection du système TIC.

La revue de code est la manière la plus minutieuse (mais également la plus onéreuse) d'apprécier les vulnérabilités.

Les résultats de ce type de tests de sécurité contribuent à identifier les vulnérabilités d'un système.

Il est important de noter que les outils et techniques d'intrusion peuvent donner des résultats erronés, à moins que la vulnérabilité soit exploitée avec succès. Pour exploiter des vulnérabilités spécifiques, il est nécessaire de connaître les correctifs logiciels déployés sur le système/l'application testés. Si ces données sont connues au moment des tests, il peut s'avérer impossible d'exploiter avec succès une vulnérabilité spécifique (par exemple, en obtenant un accès à distance non autorisé à une console) ; toutefois, il est toujours possible d'écraser ou de redémarrer un processus ou un système testé. Dans ce cas, il convient de considérer également comme vulnérable l'objet testé.

Les méthodes peuvent inclure les activités suivantes :

- entretiens avec des utilisateurs et autres personnes,
- questionnaires,
- inspection physique,
- analyse de document.

Annex E
(informative)

Approches d'appréciation du risque en sécurité de l'information

E.1 Appréciation du risque de haut niveau en sécurité de l'information

L'appréciation de haut niveau permet de définir les priorités et la chronologie des actions. Pour différentes raisons, par exemple de budget, il peut s'avérer impossible de mettre en œuvre toutes les mesures de sécurité en même temps ; seuls les risques les plus critiques peuvent alors être abordés par le processus de traitement de risque. Il peut également être précoce de commencer une gestion détaillée de risque si la mise en œuvre n'est envisagée qu'après une ou deux années. Afin d'atteindre cet objectif, l'appréciation de haut niveau peut commencer par une évaluation de haut niveau des conséquences plutôt que par une analyse systématique des menaces, des vulnérabilités, des actifs et des conséquences.

Une autre raison de commencer par l'appréciation de haut niveau est de la synchroniser avec d'autres plans relatifs à la gestion des modifications (ou la continuité de l'activité). Par exemple, il n'est pas conseillé de sécuriser entièrement un système ou une application s'il est prévu de les sous-traiter dans un futur proche, même s'il peut être encore utile de procéder à l'appréciation du risque pour définir le contrat de sous-traitance.

Les caractéristiques de l'itération de l'appréciation de haut niveau du risque peuvent comprendre les points suivants :

- L'appréciation de haut niveau du risque peut considérer un aspect plus général de l'organisme et de ses systèmes d'information, en considérant les aspects technologiques comme indépendants des questions liées à l'activité. De cette manière, l'analyse du contexte est davantage axée autour de l'environnement d'exploitation et de l'entreprise plutôt qu'autour des éléments technologiques.

- L'appréciation de haut niveau du risque peut traiter une liste plus limitée de menaces et de vulnérabilités regroupées dans des domaines définis ou peut, afin de faciliter le processus, se concentrer sur le risque ou sur des scénarii d'attaque plutôt que sur leurs éléments.

- Les risques présentés dans l'appréciation de haut niveau du risque sont souvent des domaines de risque plus généraux plutôt que des risques spécifiques identifiés. Dans la mesure où les scénarii ou les menaces sont regroupés en domaines, le traitement du risque propose des listes de mesures dans ce domaine. Les activités liées au traitement du risque tentent d'abord de proposer et de choisir des mesures de sécurité communes qui sont valables dans l'ensemble du système.

- Cependant, l'appréciation de haut niveau du risque, parce qu'elle traite rarement des détails technologiques, est plus appropriée pour fournir des mesures de sécurité organisationnelles et non techniques, des aspects liés à la gestion de mesures de sécurité techniques ou des moyens de protection techniques comme des sauvegardes et des anti-virus.

Les avantages de l'appréciation de haut niveau du risque sont :

- l'intégration d'une approche initiale simple est susceptible d'obtenir l'approbation du programme d'appréciation du risque,

- il convient qu'il soit possible d'élaborer une image stratégique du programme organisationnel de sécurité de l'information, c'est-à-dire qui servira d'aide à la planification,

- les ressources et le budget peuvent s'appliquer lorsqu'ils sont très avantageux ; les systèmes susceptibles de requérir le plus haut niveau de protection sont traités en premier.

Puisque les analyses initiales du risque sont de haut niveau et, éventuellement, d'une précision inférieure, le seul inconvénient possible est que certains processus métier ou systèmes ne soient pas identifiés comme nécessitant une seconde appréciation de risque plus détaillée. Cet inconvénient peut être évité s'il existe des informations adaptées relatives à tous les aspects de l'organisme, de ses informations et de ses systèmes, y compris les informations obtenues à partir de l'évaluation des incidents en sécurité de l'information.

L'appréciation de haut niveau du risque considère les valeurs pour l'organisme des actifs informationnels ainsi que les risques du point de vue de l'organisme. Au niveau du premier point de décision (voir figure 1), plusieurs facteurs aident à déterminer si l'appréciation de haut niveau est adaptée au traitement de risque ; ces facteurs peuvent inclure les éléments suivants :

- les objectifs métiers à atteindre en utilisant divers actifs informationnels,
- le degré selon lequel l'activité de l'organisme dépend de chaque actif informationnel, c'est-à-dire si les fonctions que l'organisme juge essentielles à sa survie, ou si son activité, dépendent de chaque actif ou de la confidentialité, l'intégrité, la disponibilité, la non répudiation, l'imputabilité, l'authenticité et la fiabilité des informations stockées et traitées sur cet actif,
- le niveau d'investissement dans chaque actif informationnel, en termes de développement, de conservation ou de remplacement de l'actif,
- les actifs informationnels, pour lesquels l'organisme attribue directement une valeur.

Lorsque ces facteurs sont évalués, la décision devient plus facile. Si les objectifs d'un actif sont extrêmement importants pour la conduite des activités d'un organisme, ou si les actifs présentent un risque élevé, il convient de procéder à une seconde itération de l'appréciation, détaillée, du risque relative à l'actif informationnel spécifique (ou à une partie de cet actif).

La règle générale à appliquer est : si l'absence de sécurité de l'information peut entraîner des conséquences défavorables importantes pour un organisme, ses processus métier ou ses actifs, une seconde itération de l'appréciation du risque est alors nécessaire, à un niveau plus approfondi, pour identifier les risques potentiels.

E.2 Appréciation détaillée du risque en sécurité de l'information

Le processus d'appréciation détaillée du risque en sécurité de l'information implique l'identification et l'évaluation approfondie des actifs, l'appréciation des menaces par rapport à ces actifs et l'appréciation des vulnérabilités. Les résultats obtenus grâce à ces activités sont alors utilisés pour apprécier les risques, puis pour identifier le traitement du risque.

Cette étape détaillée exige en général du temps, des efforts et une expertise considérables et peut, par conséquent, être la plus adaptée aux systèmes d'information présentant un risque élevé.

L'étape finale de l'appréciation détaillée du risque en sécurité de l'information consiste à évaluer les risques globaux, ce qui constitue le sujet central de la présente annexe.

Les conséquences peuvent être appréciées de différentes manières, y compris à l'aide de mesures quantitatives (par exemple, monétaires) et qualitatives (qui peuvent reposer sur l'utilisation d'adjectifs tels que modéré ou grave), ou à l'aide d'une combinaison des deux. Afin d'apprécier la vraisemblance d'une menace, il convient de déterminer la durée au-delà de laquelle l'actif a de la valeur ou exige une protection. La vraisemblance d'une menace spécifique est affectée par les points suivants :

- l'attrait de l'actif ou l'impact possible applicable lorsqu'une menace humaine délibérée est considérée,
- la facilité de conversion d'une personne à l'exploitation d'une vulnérabilité de l'actif par une récompense, applicable si une menace humaine délibérée est considérée,

- les capacités techniques de l'agent de menace, applicable à des menaces humaines délibérées,
- la sensibilité de la vulnérabilité à l'exploitation, applicable à la fois aux vulnérabilités techniques et non techniques.

De nombreuses méthodes utilisent des tableaux et combinent des mesures subjectives et empiriques. Il est important que l'organisme utilise une méthode avec laquelle il est à l'aise, en laquelle il a confiance et qui génère des résultats répétables. Quelques exemples de techniques basées sur des tableaux sont donnés ci-dessous.

E.2.1 Exemple 1 Matrice avec valeurs prédéfinies

Dans les méthodes d'appréciation du risque de ce type, les actifs physiques réels ou proposés sont évalués en termes de coût de remplacement ou de reconstruction (c'est-à-dire des mesures quantitatives). Ces coûts sont ensuite convertis sur une échelle qualitative identique à celle utilisée pour les informations (voir ci-dessous). Les actifs logiciels réels ou proposés sont évalués de la même manière que les actifs physiques, avec des coûts d'achat ou de reconstruction identifiés, puis convertis à une échelle qualitative identique à celle utilisée pour les informations. En outre, si aucun logiciel d'application n'est considéré comme possédant ses propres exigences intrinsèques relatives à la confidentialité et à l'intégrité (par exemple, si le code source est lui-même commercialement sensible), il est évalué avec la même méthode que les informations.

Les valeurs relatives aux informations sont obtenues en organisant des entretiens avec la direction de l'organisme choisi (les « propriétaires de données ») qui peuvent parler des données en toute connaissance de cause, afin de déterminer la valeur et la sensibilité des données en cours d'utilisation ou devant être stockées, traitées ou consultées. Ces entretiens facilitent l'appréciation de la valeur et de la sensibilité des informations en termes de scénarii les plus défavorables susceptibles de survenir, résultant de conséquences défavorables liées à l'activité et dues à une divulgation ou à une modification non autorisées, à une indisponibilité pendant diverses durées et à une destruction.

L'évaluation est effectuée à l'aide des lignes directrices relatives à l'évaluation des informations, qui abordent des questions telles que :

- la sûreté personnelle,
- les informations personnelles,
- les obligations légales et réglementaires,
- l'application des lois,
- les intérêts commerciaux et économiques,
- les pertes financières/l'interruption d'activités,
- l'ordre public,
- la politique métier et le fonctionnement,
- la perte de réputation,
- les contrats ou les accords avec un client.

Ces lignes directrices facilitent l'identification des valeurs sur une échelle numérique, par exemple l'échelle de 0 à 4 présentée dans l'exemple de matrice ci-dessous, permettant ainsi de reconnaître, si possible, des valeurs quantitatives et des valeurs qualitatives, lorsque les valeurs quantitatives sont impossibles, par exemple, pour une atteinte à la vie humaine.

L'activité principale suivante consiste à constituer des paires de questionnaires pour chaque type de menace, pour chaque groupe d'actifs auquel est associé un type de menace, afin de pouvoir apprécier les niveaux de menaces (la vraisemblance) et les niveaux de vulnérabilité (facilité d'exploitation par les menaces afin de créer des conséquences défavorables). La réponse à chaque question est notée. Ces notes sont rassemblées dans une base de connaissances, puis comparées à des niveaux définis. Ce système permet d'identifier des niveaux de menace sur une échelle allant du plus faible au plus élevé puis, de la même manière, des niveaux de vulnérabilité, comme le montre l'exemple de matrice ci-dessous, en établissant le cas échéant des différences entre les types de conséquences. Il convient de réunir les informations nécessaires pour remplir les questionnaires à partir des entretiens avec le personnel technique concerné, des inspections physiques des sites et des revues de documentation.

Les valeurs des actifs, ainsi que les niveaux de menace et de vulnérabilité associés à chaque type de conséquence, sont appariés dans une matrice semblable à celle présentée ci-dessous, afin d'identifier pour chaque combinaison la mesure de risque correspondante sur une échelle de 0 à 8. Les valeurs sont placées dans la matrice de manière structurée. Un exemple est donné ci-après :

Tableau E.1a)

	Vraisemblance – Menace	**Faible**			**Moyenne**			**Élevée**		
	Facilité d'exploitation	**F**	**M**	**E**	**F**	**M**	**E**	**F**	**M**	**E**
Valeur de l'actif	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Pour chaque actif, on considère les vulnérabilités pertinentes et leurs menaces correspondantes. Si une vulnérabilité n'a pas de menace correspondante ou si une menace n'a pas de vulnérabilité correspondante, il n'existe actuellement aucun risque (mais il convient de prêter une attention particulière au cas où la situation change). La rangée appropriée de la matrice est désormais identifiée grâce à la valeur de l'actif et la colonne appropriée grâce à la vraisemblance de la menace et la facilité d'exploitation. Par exemple, si la valeur de l'actif est égale à **3**, la menace est « **élevée** » et la vulnérabilité est « **faible** », la mesure du risque est égale à **5**. A supposer que la valeur d'un actif soit égale à 2, par exemple pour une modification, le niveau de menace est « faible », la facilité d'exploitation est « élevée » et la mesure de risque est alors égale à 4. La taille de la matrice, en termes du nombre de catégories de vraisemblance de menace et de catégories d'exploitation, et du nombre de catégories d'évaluation des actifs, peut être ajustée selon les besoins de l'organisme. Des colonnes et rangées supplémentaires exigent des mesures de risque supplémentaires. La valeur de cette approche consiste à classer les risques à traiter.

Une matrice identique à celle du tableau E.1 b) provient de la considération de la vraisemblance d'un scénario d'incident, mise en correspondance avec l'impact estimé sur l'activité. La vraisemblance d'un scénario d'incident est donnée par une menace qui exploite une vulnérabilité avec une certaine probabilité. Le tableau met cette vraisemblance en correspondance avec l'impact sur l'activité, associé au scénario d'incident. Le risque obtenu est mesuré sur une échelle de 0 à 8 qui peut être évaluée par rapport aux critères d'acceptation du risque. Cette échelle de risques peut également être mise en correspondance avec une simple évaluation du risque global, par exemple :

- risque faible : 0-2
- risque moyen : 3-5
- risque élevé : 6-8

Tableau E.1b)

	Vraisemblance d'un scénario d'incident	Très faible (Très peu probable)	Faible (Peu probable)	Moyenne (Possible)	Élevée (Probable)	Très élevée (Fréquente)
Impact sur l'activité	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Élevé	3	4	5	6	7
	Très élevé	4	5	6	7	8

E.2.2 Exemple 2 – Classement des menaces par mesures de risque

Une matrice, ou un tableau identique au tableau E.2, peut être utilisée pour relier les facteurs des conséquences (valeur des actifs) et la vraisemblance des menaces (en tenant compte des aspects des vulnérabilités). La première étape consiste à évaluer les conséquences (valeur de l'actif) de chaque actif menacé sur une échelle prédéfinie, allant par exemple de 1 à 5 (colonne « b » dans le tableau). La seconde étape consiste à évaluer la vraisemblance de chaque menace sur une échelle prédéfinie, allant par exemple de 1 à 5 (colonne « c » dans le tableau). La troisième étape consiste à calculer la mesure du risque en multipliant (b x c). Les menaces peuvent finalement être classées selon l'ordre de leur mesure de risque associée. Noter que dans cet exemple, 1 est considéré comme la conséquence et la vraisemblance la plus faible.

Tableau E.2

Descripteur de menace (a)	Valeur de la conséquence (actif) (b)	Vraisemblance de la menace (c)	Mesure du risque (d)	Classement des menaces (e)
Menace A	5	2	10	2
Menace B	2	4	8	3
Menace C	3	5	15	1
Menace D	1	3	3	5
Menace E	4	1	4	4
Menace F	2	4	8	3

Comme présenté ci-dessus, il s'agit d'une procédure permettant de comparer et de classer différentes menaces présentant différentes conséquences et vraisemblance par ordre de priorité. Dans certains cas, il sera nécessaire d'associer des valeurs monétaires aux échelles empiriques utilisées ici.

E.2.3 Exemple 3 – Appréciation d'une valeur relative à la vraisemblance et aux conséquences possibles des risques

Dans cet exemple, l'accent est mis sur les conséquences des incidents en sécurité de l'information (c'est-à-dire les scénarii d'incident), et sur la détermination des systèmes qu'il convient de considérer comme prioritaires. Cette appréciation s'effectue en appréciant deux valeurs pour chaque actif et risque, ce qui permet de déterminer la note correspondant à chaque actif. Lors de l'ajout de l'ensemble des notes des actifs du système, la mesure de risque de ce système est déterminée.

Une valeur est d'abord attribuée à chaque actif. Cette valeur correspond aux conséquences défavorables éventuelles susceptibles d'apparaître si l'actif est menacé. Pour chaque menace applicable à l'actif, cette valeur est attribuée à l'actif.

Une valeur de vraisemblance est ensuite appréciée. Elle est appréciée en combinant la vraisemblance de la menace et la facilité d'exploitation de la vulnérabilité, voir le Tableau E.3 exprimant la vraisemblance d'un scénario d'incident.

Tableau E.3

Vraisemblance de la menace	**Faible**			**Moyenne**			**Élevée**		
Niveaux de vulnérabilité	F	M	E	F	M	E	F	M	E
Valeur de la vraisemblance d'un scénario d'incident	0	1	2	1	2	3	2	3	4

Une note d'actif/de menace est ensuite attribuée en repérant dans le tableau E.4 l'intersection entre la valeur de l'actif et la valeur de la vraisemblance. Les notes d'actif/de menace sont ajoutées pour donner un score total d'actifs. Ce chiffre peut être utilisé pour établir une différence entre les actifs faisant partie d'un système.

Tableau 4

Valeur de l'actif	**0**	**1**	**2**	**3**	**4**
Valeur de la vraisemblance					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

L'étape finale consiste à ajouter toutes les notes des actifs du système, donnant ainsi une note système. Cette note peut être utilisée pour établir une différence entre les systèmes et pour déterminer quelle protection système il convient de considérer comme prioritaire.

Dans les exemples suivants, toutes les valeurs sont choisies au hasard.

En supposant que le système S possède trois actifs A1, A2 et A3. En supposant également qu'il existe deux menaces T1 et T2 applicables au système S. La valeur de A1 est 3, la valeur de A2 est 2 et la valeur de l'actif de A3 est 4.

Si la vraisemblance de la menace est faible pour A1 et T1 et si la facilité d'exploitation de la vulnérabilité est moyenne, alors la valeur de la vraisemblance est 1 (voir le Tableau E.3).

La note actif/menace A1/T1 peut être obtenue à partir du Tableau E.4 puisque l'intersection de la valeur de l'actif 3 et de la valeur de la vraisemblance 1 est 4. De la même manière, pour A1/T2, la vraisemblance de la menace est moyenne et la facilité d'exploitation de la vulnérabilité est élevée, ce qui donne une note A1/T2 de 6.

La note totale de l'actif peut alors être calculée, c'est-à-dire 10. La note totale de l'actif est calculée pour chaque actif et pour chaque menace applicable. La note totale du système est calculée en ajoutant A1T + A2T + A3T, ce qui donne ST.

Il est désormais possible de comparer différents systèmes afin d'établir des priorités ainsi que différents actifs dans un système.

L'exemple ci-dessus se présente en termes de systèmes d'information ; cependant, une approche identique peut être appliquée à des processus métier.

Annex F
(informative)
Contraintes liées à la réduction du risque

Il convient de contenir compte des contraintes suivantes tout en considérant les contraintes liées à la réduction du risque :

Contraintes de temps :

De nombreux types de contraintes de temps peuvent exister. Par exemple, il convient de mettre en œuvre des mesures dans un délai acceptable pour les dirigeants de l'organisme. Un autre type de contrainte de temps concerne, peut être, la possibilité de mettre en œuvre une mesure au cours du cycle de vie de l'information ou d'un système. Un troisième type de contrainte de temps consiste en la durée que les dirigeants de l'organisme considèrent comme un délai acceptable d'exposition à un risque spécifique.

Contraintes financières :

Il convient que les mesures de sécurité ne soient pas plus onéreuses à mettre en œuvre, ou à maintenir, que la valeur des risques qu'elles doivent protéger, sauf si la conformité est obligatoire (par exemple, la conformité à la législation). Il convient de s'efforcer de ne pas dépasser les budgets alloués et d'en tirer un avantage financier grâce à l'utilisation des mesures. Cependant, il peut, dans certains cas, s'avérer impossible d'atteindre la sécurité et le seuil d'acceptation des risques souhaités, en raison de contraintes budgétaires. Par conséquent, la résolution de cette situation relève alors de la décision des dirigeants de l'organisme.

Il convient de prêter une attention toute particulière à une réduction du nombre, ou de la qualité des mesures de sécurité à mettre en œuvre par le budget, puisque cela peut entraîner le maintien implicite d'un risque plus important que prévu. Il convient d'utiliser uniquement avec précaution le budget défini comme un facteur de limitation des mesures de sécurité.

Contraintes techniques :

Il est possible d'éviter facilement des problèmes techniques, comme la compatibilité des programmes ou du matériel, s'ils sont pris en considération lors du choix des mesures de sécurité. En outre, la mise en œuvre rétrospective de mesures de sécurité, concernant un processus ou un système, est souvent freinée en raison de contraintes techniques. Ces difficultés peuvent déplacer l'équilibre des types de mesures de sécurité vers des aspects physiques et des procédures de sécurité. Il peut s'avérer nécessaire de réviser le programme de sécurité de l'information afin d'atteindre les objectifs liés à la sécurité. Cela peut arriver lorsque les mesures de sécurité ne répondent pas aux résultats attendus en matière de réduction des risques sans affaiblir la productivité.

Contraintes opérationnelles

Les contraintes opérationnelles, telle que la nécessité de fonctionner 24 heures sur 24 et 7 jours sur 7 pour des sauvegardes, peuvent entraîner la mise en œuvre complexe et onéreuse de mesures de sécurité, sauf si ces mesures sont élaborées dès la conception.

Contraintes culturelles :

Les contraintes culturelles, liées au choix des mesures de sécurité, peuvent être spécifiques à un pays, un secteur, un organisme ou même au service d'un organisme. Toutes les mesures de sécurité ne peuvent s'appliquer à tous les pays. Par exemple, il peut être possible de mettre en œuvre des fouilles de sacs dans certaines parties d'Europe, mais pas dans certaines parties du Moyen-Orient. Ces aspects culturels ne peuvent être ignorés car de nombreuses mesures de sécurité reposent sur le soutien actif du personnel. Si le personnel ne comprend pas la nécessité d'une mesure de sécurité, ou ne la considère pas comme acceptable au niveau culturel, la mesure perdra de son efficacité au fil du temps.

Contraintes éthiques :

Les contraintes éthiques peuvent avoir des implications majeures sur les mesures de sécurité puisque l'éthique évolue selon des normes sociales. Ces contraintes peuvent empêcher, dans certains pays, la mise en œuvre de mesures de sécurité telle que l'analyse des courriers électroniques. La confidentialité des informations peut également varier selon l'éthique de la région ou du gouvernement. Ces questions peuvent être d'un plus grand intérêt dans certains secteurs industriels que dans d'autres, par exemple le gouvernement et la santé.

Contraintes environnementales :

Des facteurs liés à l'environnement peuvent avoir une influence sur le choix des mesures de sécurité, à titre d'exemples la disponibilité de l'espace, des conditions climatiques extrêmes, la géographie naturelle et urbaine environnante. Par exemple, un contrôle parasismique peut être requis dans certains pays mais inutile dans d'autres.

Contraintes légales :

Des facteurs légaux, comme la protection des données personnelles ou les dispositions du code pénal relatives au traitement de l'information peuvent affecter le choix des mesures de sécurité. La conformité législative et réglementaire peut nécessiter certains types de mesure, notamment la protection des données et un audit financier ; elle peut également empêcher l'utilisation de certaines mesures de sécurité, par exemple, le chiffrement. D'autres lois et règlements comme la législation relative aux relations professionnelles, au service incendie, à la santé et à la sécurité ou des règlements du secteur économique peuvent également affecter le choix des mesures de sécurité.

Facilité d'utilisation :

Une mauvaise interface homme-machine entraînera des erreurs humaines et pourra rendre la mesure de sécurité inutile. Il convient de choisir les mesures de sécurité afin d'en optimiser la facilité d'utilisation tout en atteignant un niveau acceptable de risque résiduel sur l'activité. Les difficultés d'utilisation de certaines mesures de sécurité auront un impact sur leur efficacité, puisque les utilisateurs peuvent tenter de les contourner ou de les ignorer autant que possible. Des contrôles d'accès complexes au sein d'un organisme pourraient encourager les utilisateurs à trouver d'autres méthodes d'accès non autorisées.

Contraintes liées au personnel :

Il convient de tenir compte de la disponibilité et du coût salarial des compétences spécialisées nécessaires pour mettre des mesures de sécurité en œuvre, ainsi que de la capacité de faire déplacer le personnel entre des sites présentant des conditions d'exploitation défavorables. L'expertise peut ne pas être facilement accessible pour la mise en œuvre des mesures de sécurité prévues, ou peut être onéreuse pour l'organisme. D'autres aspects, comme la tendance de certains membres du personnel à discriminer d'autres membres qui ne sont pas soumis à une enquête relative à la sécurité, peuvent avoir des implications majeures sur les politiques et les pratiques liées à la sécurité. La nécessité de trouver et de recruter les bonnes personnes pour un poste peut conduire à procéder au recrutement avant la fin de l'enquête sur la sécurité. L'exigence relative à l'enquête sur la sécurité à effectuer avant le recrutement est la pratique normale et la plus sécurisée.

Contraintes liées à l'intégration de mesures de sécurité nouvelles et existantes :

L'intégration de nouvelles mesures de sécurité dans l'infrastructure existante, et les interdépendances entre ces mesures, sont souvent négligées. De nouvelles mesures de sécurité peuvent ne pas être facilement mises en œuvre s'il existe une incohérence ou une incompatibilité avec les mesures existantes. Par exemple, un plan prévoyant l'utilisation de jetons biométriques pour le contrôle d'accès physique peut créer un conflit avec un système existant basé sur un clavier d'identification personnelle destiné au contrôle d'accès. Il convient que le coût destiné à transformer les mesures de sécurité existantes en mesures prévues comprenne des éléments à ajouter aux coûts globaux de traitement du risque. Il peut s'avérer impossible de mettre en œuvre une mesure de sécurité choisie en raison d'une interférence avec les mesures en place.

Bibliographie

[1] ISO/CEI Guide 73:2002, *Management du risque — Vocabulaire — Principes directeurs pour l'utilisation dans les normes*.

[2] ISO/CEI 16085:2006, *Ingénierie des systèmes et du logiciel — Processus du cycle de vie — Gestion des risques*.

[3] AS/NZS 4360:2004, *Management du risque*.

[4] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

[5] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology