INTERNATIONAL STANDARD

ISO/CEI 27005

Quatrième édition
2022-10

Sécurité de l'information, cybersécurité et protection de la vie privée — Conseils sur la gestion des risques liés à la sécurité de l'information

Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information

Numéro de réference
ISO/CEI 27005:2022(F)

Bureau du droit d'auteur
ISO CP 401 • Ch. de Blandonnet 8

CH-1214 Vernier, Genève
Téléphone : +41 22 749 01 11

E-mail : copyright@iso.org Site

Internet : www.iso.org

Publié en Suisse

Contenu

Page

Avant-propos

L'ISO (l'Organisation internationale de normalisation) et la CEI (la Commission électrotechnique internationale) forment le système spécialisé pour la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent à l'élaboration de normes internationales par l'intermédiaire de comités techniques établis par l'organisation respective pour traiter de domaines particuliers d'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt mutuel. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI, participent également aux travaux.

Les procédures utilisées pour élaborer ce document et celles destinées à sa maintenance ultérieure sont décrites dans les Directives ISO/CEI, Partie 1. En particulier, les différents critères d'approbation nécessaires pour les différents types de documents doivent être notés. Ce document a été rédigé conformément aux règles éditoriales des Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'attention est attirée sur la possibilité que certains éléments de ce document puissent faire l'objet de droits de brevet. L'ISO et la CEI ne peuvent être tenues responsables de l'identification de tout ou partie de ces droits de brevet. Les détails de tous les droits de brevet identifiés lors de l'élaboration du document figureront dans l'introduction et/ou sur la liste ISO des déclarations de brevet reçues (voir www.iso.org/patents). ou la liste CEI des déclarations de brevet reçues (voir https://patents.iec.ch).

Tout nom commercial utilisé dans ce document est une information donnée pour la commodité des utilisateurs et ne constitue pas une approbation.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques à l'ISO liés à l'évaluation de la conformité, ainsi que des informations sur l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) dans les obstacles techniques au commerce (OTC), voir www. .iso.org/iso/avant-propos.html. Pour la CEI, voir www.iec.ch/understanding-standards.

Ce document a été préparé par le comité technique mixte ISO/IEC JTC 1, Technologies de l'information, sous-comité SC 27, Sécurité de l'information, cybersécurité et protection de la vie privée.

Cette quatrième édition annule et remplace la troisième édition (ISO/IEC 27005:2018), qui a été techniquement révisée.

Les principaux changements sont les suivants :

— tous les textes d'orientation ont été alignés sur les normes ISO/IEC 27001:2022 et ISO 31000:2018 ;

— la terminologie a été alignée sur la terminologie de l'ISO 31000:2018 ;

— la structure des articles a été adaptée à la présentation de l'ISO/IEC 27001:2022 ;

— des concepts de scénarios de risque ont été introduits ;

— l'approche basée sur les événements s'oppose à l'approche basée sur les actifs pour l'identification des risques ;

— le contenu des annexes a été révisé et restructuré en une seule annexe.

Tout commentaire ou question sur ce document doit être adressé à l'organisme de normalisation national de l'utilisateur. Une liste complète de ces organismes est disponible sur www.iso.org/members.html et www.iec.ch/comités-nationaux.

Introduction

Ce document fournit des conseils sur :

— mise en œuvre des exigences relatives aux risques liés à la sécurité de l'information spécifiées dans la norme ISO/IEC 27001 ;

— références essentielles dans les normes élaborées par l'ISO/IEC JTC 1/SC 27 pour étayer les informations activités de gestion des risques de sécurité ;

— les actions qui répondent aux risques liés à la sécurité de l'information (voir ISO/IEC 27001:2022, 6.1 et Article 8) ;

— mise en œuvre des lignes directrices en matière de gestion des risques dans l'ISO 31000 dans le contexte de la sécurité de l'information.

Ce document contient des orientations détaillées sur la gestion des risques et complète les orientations de la norme ISO/IEC 27003.

Ce document est destiné à être utilisé par :

— les organisations qui ont l'intention d'établir et de mettre en œuvre un système de gestion de la sécurité de l'information (ISMS) conformément à la norme ISO/IEC 27001 ;

— les personnes qui effectuent ou sont impliquées dans la gestion des risques liés à la sécurité de l'information (par exemple, SMSI professionnels, propriétaires de risques et autres parties intéressées) ;

— les organisations qui souhaitent améliorer leur processus de gestion des risques liés à la sécurité de l'information.

Sécurité de l'information, cybersécurité et protection de la vie privée — Conseils sur la gestion des risques liés à la sécurité de l'information

1 Portée

Ce document fournit des conseils pour aider les organisations à :

— satisfaire aux exigences de la norme ISO/IEC 27001 concernant les actions visant à faire face aux risques liés à la sécurité de l'information ;

— effectuer des activités de gestion des risques liés à la sécurité de l'information, en particulier le risque lié à la sécurité de l'information évaluation et traitement.

Ce document est applicable à toutes les organisations, quel que soit leur type, leur taille ou leur secteur.

2 Références normatives

Les documents suivants sont mentionnés dans le texte de telle manière que tout ou partie de leur contenu constitue des exigences de ce document. Pour les références datées, seule l'édition citée applique. Pour les références non datées, la dernière édition du document référencé (y compris les modifications éventuelles) s'applique.

ISO/IEC 27000, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Présentation générale et vocabulaire

3Termes et définitions

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

L'ISO et la CEI maintiennent des bases de données terminologiques destinées à la normalisation aux adresses suivantes :

— Plateforme de navigation ISO Online : disponible sur https://www.iso.org/obp

— IEC Electropedia : disponible sur https://www.electropedia.org/

3.1 Termes liés au risque de sécurité des informations

3.1.1
contexte externe

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

Note 1 à l'article : Le contexte externe peut inclure les éléments suivants :

— l'environnement social, culturel, politique, juridique, réglementaire, financier, technologique, économique, géologique, qu'il soit international, national, régional ou local ;

— les principaux facteurs et tendances affectant les objectifs de l'organisation ;

— les relations, perceptions, valeurs, besoins et attentes des parties intéressées externes ;

— les relations et engagements contractuels ;

— la complexité des réseaux et des dépendances.

[SOURCE : Guide ISO 73:2009, 3.3.1.1, modifié — La note 1 à l'article a été modifiée.]

3.1.2
contexte interne

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

Note 1 à l'article : Le contexte interne peut inclure :

— vision, mission et valeurs;

— gouvernance, structure organisationnelle, rôles et responsabilités ;

— stratégie, objectifs et politiques;

— la culture de l'organisation;

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

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

— les données, les systèmes d'information et les flux d'informations;

— les relations avec les parties intéressées internes, en tenant compte de leurs perceptions et valeurs ;

— les relations et engagements contractuels ;

— les interdépendances et interconnexions internes.

[SOURCE : Guide ISO 73:2009, 3.3.1.2, modifié — La note 1 à l'article a été modifiée.]

3.1.3
risque

effet de l'incertitude sur les objectifs

Note 1 à l'article: Un effet est un écart par rapport à l'attendu, positif ou négatif.

Note 2 à l'article: Les objectifs peuvent avoir différents aspects et catégories, et peuvent être appliqués à différents niveaux.

Note 3 à l'article: L'incertitude est l'état, même partiel, de déficit d'information relatif à, à la compréhension ou à la connaissance d'un événement (3.1.11), de sa conséquence (3.1.14) ou de sa probabilité (3.1.13).

Note 4 à l'article: Le risque est généralement exprimé en termes de sources de risque (3.1.6), d'événements potentiels, de leurs conséquences et de leur probabilité.

Note 5 à l'article: Dans le contexte des systèmes de gestion de la sécurité de l'information, les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.

Note 6 à l'article: Les risques liés à la sécurité des informations sont généralement associés à un effet négatif de l'incertitude sur les objectifs de sécurité des informations.

Note 7 à l'article: Les risques liés à la sécurité des informations peuvent être associés à la possibilité que des menaces (3.1.9) exploitent les vulnérabilités (3.1.10) d'un actif informationnel ou d'un groupe d'actifs informationnels et causent ainsi un préjudice à une organisation.

[SOURCE : ISO 31000 :2018, 3.1, modifiée — la phrase : « Cela peut être positif, négatif ou les deux, et peut traiter, créer ou entraîner des opportunités et des menaces » a été remplacée par « positif ou négatif » dans la note 1 de entrée; la Note 3 à l'article originale a été renumérotée Note 4 à l'article ; et les notes 3, 5, 6 et 7 de l'article ont été ajoutées.]

3.1.4
scénario de risque

séquence ou combinaison d' événements (3.1.11) menant de la cause initiale à la conséquence indésirable (3.1.14)

[SOURCE : ISO 17666:2016, 3.1.13, modifiée — La note 1 à l'article a été supprimée.]

3.1.5
propriétaire du
risque, personne ou entité ayant la responsabilité et l'autorité nécessaires pour gérer un risque (3.1.3)

[SOURCE : Guide ISO 73:2009, 3.5.1.5]

3.1.6
élément source
de risque qui, seul ou en combinaison, est susceptible de donner lieu à un risque (3.1.3)

Note 1 à l'article: Une source de risque peut être de l'un de ces trois types :

- humain;

— environnemental;

- technique.

Note 2 à l'article: Un type de source de risque humain peut être intentionnel ou non intentionnel.

[SOURCE : ISO 31000:2018, 3.4, modifiée — Les notes 1 et 2 à l'article ont été ajoutées.]

3.1.7
critères de risque
termes de référence par rapport auxquels l'importance d'un risque (3.1.3) est évaluée

Note 1 à l'article: Les critères de risque sont basés sur les objectifs organisationnels, ainsi que sur le contexte externe (3.1.1) et interne (3.1.2).

Note 2 à l'article : Les critères de risque peuvent être dérivés de normes, lois, politiques et autres exigences.

[SOURCE : Guide ISO 73:2009, 3.3.1.3]

3.1.8
montant de
l'appétit pour le risque et type de risque (3.1.3) qu'une organisation est prête à poursuivre ou à conserver

[SOURCE : Guide ISO 73:2009, 3.7.1.2]

3.1.9
menace
cause potentielle d'un incident de sécurité de l'information (3.1.12) pouvant entraîner des dommages à un système ou un préjudice à une organisation

3.1.10
vulnérabilité
faiblesse d'un actif ou d' un contrôle (3.1.16) qui peut être exploitée pour qu'un événement (3.1.11) ayant une conséquence négative (3.1.14) se produise

3.1.11

survenance d'un événement ou changement d'un ensemble particulier de circonstances

Note 1 à l'article: Un événement peut avoir une ou plusieurs occurrences, et peut avoir plusieurs causes et plusieurs conséquences (3.1.14).

Note 2 à l'article: Un événement peut également être quelque chose qui est attendu et qui ne se produit pas, ou quelque chose qui n'est pas attendu et qui se produit.

[SOURCE : ISO 31000:2018, 3.5, modifiée — La note 3 à l'article a été supprimée.]

3.1.12

incident de sécurité des informations

un seul ou une série d'événements de sécurité des informations indésirables ou inattendus qui ont une probabilité significative de compromettre les opérations commerciales et de menacer la sécurité des informations

3.1.13

probabilité

chance que quelque chose se passe

Note 1 à l'article : Dans la terminologie de la gestion des risques, le mot « probabilité » est utilisé pour désigner la probabilité que quelque chose se produise, qu'elle soit définie, mesurée ou déterminée objectivement ou subjectivement, qualitativement ou quantitativement, et décrite en utilisant des termes généraux ou mathématiquement (tels que une probabilité ou une fréquence sur une période de temps donnée).

Note 2 à l'article: Le terme anglais « likelihood » n'a pas d'équivalent direct dans certaines langues ; au lieu de cela, l'équivalent du terme « probabilité » est souvent utilisé. Cependant, en anglais, le terme « probabilité » est souvent interprété de manière étroite comme un terme mathématique. Par conséquent, dans la terminologie de la gestion des risques, le terme « vraisemblance » est utilisé dans le but d'avoir la même interprétation large que le terme « probabilité » dans de nombreuses langues autres que l'anglais.

[SOURCE : ISO 31000 : 2018, 3.7]

3.1.14

conséquence

résultat d'un événement (3.1.11) affectant les objectifs

Note 1 à l'article: Une conséquence peut être certaine ou incertaine et peut avoir des effets directs ou indirects positifs ou négatifs sur les objectifs.

Note 2 à l'article : Les conséquences peuvent être exprimées qualitativement ou quantitativement.

Note 3 à l'article: Toute conséquence peut dégénérer en raison d'effets en cascade et cumulatifs.

[SOURCE : ISO 31000 : 2018, 3.6]

3.1.15

niveau de risque

importance d'un risque (3.1.3), exprimée en termes de combinaison de conséquences (3.1.14) et de leur probabilité (3.1.13)

[SOURCE : Guide ISO 73:2009, 3.6.1.8, modifié — l'expression : « ampleur d'un risque ou d'une combinaison de risques » a été remplacée par « importance d'un risque ».]

3.1.16

contrôle

mesure qui maintient et/ou modifie le risque (3.1.3)

Note 1 à l'article : Les contrôles incluent, sans s'y limiter, tout processus, politique, dispositif, pratique ou autres conditions et/ou actions qui maintiennent et/ou modifient le risque.

Note 2 à l'article: Les contrôles peuvent ne pas toujours exercer l'effet modificateur prévu ou supposé.

[SOURCE : ISO 31000 : 2018, 3.8]

3.1.17

risque résiduel

risque (3.1.3) restant après le traitement du risque (3.2.7)

Note 1 à l'article : Le risque résiduel peut contenir un risque non identifié.

Note 2 à l'article : Les risques résiduels peuvent également contenir des risques conservés.

[SOURCE : Guide ISO 73:2009, 3.8.1.6, modifié — La Note 2 à l'article a été modifiée.]

3.2 Termes liés à la gestion des risques liés à la sécurité de l'information

3.2.1

processus de gestion des risques

application systématique des politiques, procédures et pratiques de gestion aux activités de communication, de consultation, d'établissement du contexte et d'identification, d'analyse, d'évaluation, de traitement, de surveillance et d'examen des risques (3.1.3)

[SOURCE : Guide ISO 73:2009, 3.1]

3.2.2

communication et consultation sur les risques

ensemble de processus continus et itératifs qu'une organisation mène pour fournir, partager ou obtenir des informations et engager un dialogue avec les parties intéressées concernant la gestion des risques (3.1.3)

Note 1 à l'article: Les informations peuvent porter sur l'existence, la nature, la forme, la probabilité (3.1.13), l'importance, l'évaluation, l'acceptation et le traitement du risque.

Note 2 à l'article : La consultation est un processus bidirectionnel de communication éclairée entre une organisation et ses parties intéressées sur une question avant de prendre une décision ou de déterminer une orientation sur cette question. La consultation c'est :

— un processus qui influe sur une décision par l'influence plutôt que par le pouvoir ;

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

3.2.3

l'évaluation des risques

processus global d' identification des risques (3.2.4), d'analyse des risques (3.2.5) et d'évaluation des risques (3.2.6)

[SOURCE : Guide ISO 73:2009, 3.4.1]

3.2.4

identification des risques

processus de recherche, de reconnaissance et de description des risques (3.1.3)

Note 1 à l'article: L'identification des risques implique l'identification des sources de risques (3.1.6), des événements (3.1.11), de leurs causes et de leurs conséquences potentielles (3.1.14).

Note 2 à l'article: L'identification des risques peut impliquer des données historiques, une analyse théorique, des opinions éclairées et d'experts, ainsi que les besoins des parties intéressées.

[SOURCE : Guide ISO 73:2009, 3.5.1, modifié — « partie intéressée » a remplacé « partie prenante » dans la note 2 à l'article.]

3.2.5

analyse de risque

processus permettant de comprendre la nature du risque (3.1.3) et de déterminer le niveau de risque (3.1.15)

Note 1 à l'article: L'analyse des risques fournit la base de l'évaluation des risques (3.2.6) et des décisions concernant le traitement des risques (3.2.7).

Note 2 à l'article: L'analyse des risques comprend l'estimation des risques.

[SOURCE : Guide ISO 73:2009, 3.6.1]

3.2.6

évaluation du risque

processus de comparaison des résultats de l'analyse des risques (3.2.5) avec les critères de risque (3.1.7) pour déterminer si le risque (3.1.3) et/ou son importance est acceptable ou tolérable

Note 1 à l'article: L'évaluation des risques aide à la décision concernant le traitement des risques (3.2.7).

[SOURCE : Guide ISO 73:2009, 3.7.1, modifié — « signification » a remplacé « ampleur ».]

3.2.7
processus de traitement
des risques pour modifier le risque (3.1.3)

Note 1 à l'article : Le traitement des risques peut impliquer :

— éviter le risque en décidant de ne pas démarrer ou poursuivre l'activité qui donne naissance au risque;

— prendre ou augmenter des risques afin de saisir une opportunité ;

— éliminer la source de risque (3.1.6);

— modifier la vraisemblance (3.1.13) ;

— modifier les conséquences (3.1.14) ;

— partager le risque avec une ou plusieurs autres parties (y compris les contrats et le financement des risques) ; et

— conserver le risque par une décision éclairée.

Note 2 à l'article : Le traitement des risques liés à la sécurité de l'information n'inclut pas « la prise ou l'augmentation de risques afin de saisir une opportunité », mais l'organisation peut disposer de cette option pour la gestion générale des risques.

Note 3 à l'article : Les traitements des risques qui traitent des conséquences négatives sont parfois appelés « atténuation des risques », « élimination des risques », « prévention des risques » et « réduction des risques ».

Note 4 à l'article : Le traitement des risques peut créer de nouveaux risques ou modifier des risques existants.

[SOURCE : Guide ISO 73:2009, 3.8.1, modifié ─ La note 1 à l'article a été ajoutée et les notes 1 et 2 à l'article d'origine ont été renumérotées en notes 2 et 3 à l'article.]

3.2.8
acceptation du risque
décision éclairée de prendre un risque particulier (3.1.3)

Note 1 à l'article: L'acceptation du risque peut se produire sans traitement du risque (3.2.7) ou pendant le processus de traitement du risque.

Note 2 à l'article : Les risques acceptés sont soumis à un suivi et à un examen.

[SOURCE : Guide ISO 73:2009, 3.7.1.6]

3.2.9
partage des
risques forme de traitement des risques (3.2.7) impliquant la répartition convenue des risques (3.1.3) avec d'autres parties

Note 1 à l'article : Les exigences légales ou réglementaires peuvent limiter, interdire ou imposer le partage des risques.

Note 2 à l'article : Le partage des risques peut être effectué par le biais d'une assurance ou d'autres formes de contrat.

Note 3 à l'article: Le degré de répartition du risque peut dépendre de la fiabilité et de la clarté des accords de partage.

Note 4 à l'article : Le transfert de risque est une forme de partage des risques.

[SOURCE : Guide ISO 73:2009, 3.8.1.3]

3.2.10
rétention du risque
acceptation temporaire du bénéfice potentiel du gain, ou du fardeau de la perte, découlant d'un risque particulier (3.1.3)

Note 1 à l'article : La conservation peut être limitée à une certaine période de temps.

Note 2 à l'article: Le niveau de risque (3.1.15) retenu peut dépendre de critères de risque (3.1.7).

[SOURCE : Guide ISO 73:2009, 3.8.1.5, modifié — le mot « temporaire » a été ajouté au début de la définition et de l'expression ; « La rétention des risques inclut l'acceptation des risques résiduels » a remplacé « La rétention peut être limitée à une certaine durée dans la note 1 de l'article.]

4 Structure de ce document

Ce document est structuré comme suit :

— Article 5 : Gestion des risques liés à la sécurité des informations ;

— Article 6 : Établissement du contexte ;

— Article 7 : Processus d'évaluation des risques liés à la sécurité des informations ;

— Article 8 : Processus de traitement des risques liés à la sécurité des informations ;

— Article 9 : Fonctionnement ;

— Article 10 : Tirer parti des processus SMSI associés.

À l'exception des descriptions données dans les paragraphes généraux, toutes les activités de gestion des risques présentées de l'Article 7 à l'Article 10 sont structurées comme suit :

Entrée : identifie toute information requise pour effectuer l'activité.

Action : Décrit l'activité.

Déclencheur : Fournit des indications sur le moment où démarrer l'activité, par exemple en raison d'un changement au sein de l'organisation ou selon un plan ou un changement dans le contexte externe de l'organisation.

Résultat : identifie toute information dérivée après l'exécution de l'activité, ainsi que tous les critères auxquels un tel résultat doit satisfaire.

Conseils : fournit des conseils sur la réalisation de l'activité, du mot-clé et du concept clé.

5 Gestion des risques liés à la sécurité de l'information

5.1 Processus de gestion des risques liés à la sécurité de l'information

Le processus de gestion des risques liés à la sécurité de l'information est présenté dans la figure 1.

NOTE Ce processus est basé sur le processus général de gestion des risques défini dans l'ISO 31000.

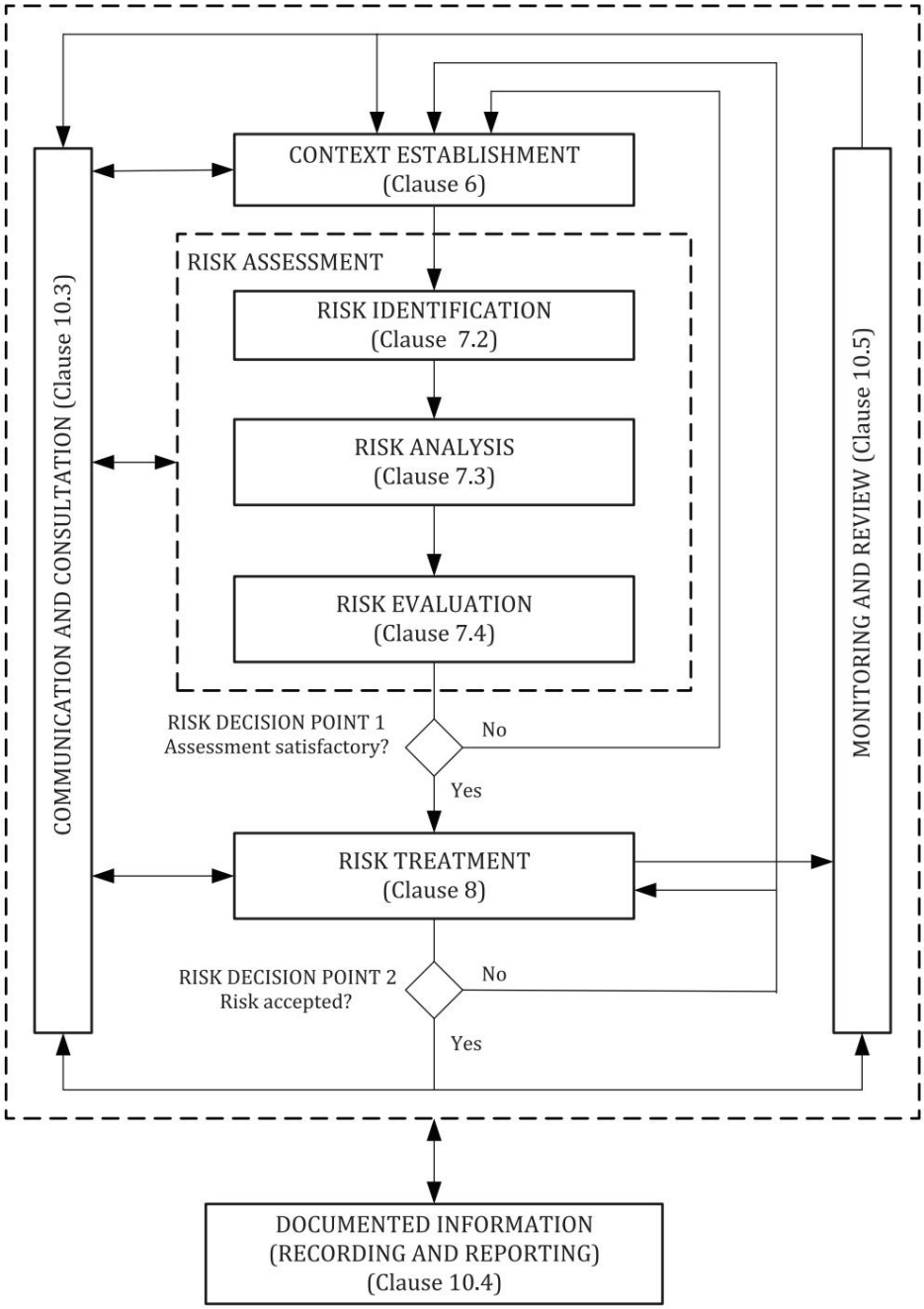


Figure 1 — Processus de gestion des risques liés à la sécurité de l'information

Comme l'illustre la figure 1 , le processus de gestion des risques liés à la sécurité de l'information peut être itératif pour les activités d'évaluation et/ou de traitement des risques. Une approche itérative pour mener une évaluation des risques peut accroître la profondeur et le détail de l'évaluation à chaque itération. L'approche itérative offre un bon équilibre entre la minimisation du temps et des efforts consacrés à l'identification des contrôles, tout en garantissant que les risques sont correctement évalués.

L'établissement du contexte signifie assembler le contexte interne et externe pour la gestion des risques de sécurité de l'information ou une évaluation des risques de sécurité de l'information.

Si l'évaluation des risques fournit suffisamment d'informations pour déterminer efficacement les actions requises pour modifier les risques à un niveau acceptable, alors la tâche est terminée et le traitement des risques suit.
Si les informations sont insuffisantes, une autre itération de l'évaluation des risques doit être effectuée. Cela peut impliquer un changement de contexte de l'évaluation des risques (par exemple, une portée révisée), l'implication d'une expertise dans

le champ pertinent, ou d'autres moyens de collecter les informations requises pour permettre une modification du risque à un niveau acceptable (voir « point de décision en matière de risque 1 » dans la figure 1).

Le traitement des risques implique un processus itératif de :

— formuler et sélectionner des options de traitement des risques ;

— planifier et mettre en œuvre le traitement des risques ;

— évaluer l'efficacité de ce traitement;

— décider si le risque restant est acceptable;

— suivre un traitement supplémentaire s'il n'est pas acceptable.

Il est possible que le traitement des risques ne conduise pas immédiatement à un niveau acceptable de risques résiduels. Dans cette situation, une autre tentative pour trouver un traitement des risques plus approfondi peut être effectuée, ou il peut y avoir une autre itération de l'évaluation des risques, soit dans son intégralité, soit par parties. Cela peut impliquer un changement de contexte de l'évaluation des risques (par exemple par un champ d'application révisé) et la participation d'experts dans le domaine concerné. La connaissance des menaces ou des vulnérabilités pertinentes peut conduire à de meilleures décisions concernant les activités de traitement des risques appropriées lors de la prochaine itération de l'évaluation des risques (voir « Point de décision en matière de risque 2 » dans la figure 1).

L'établissement du contexte est discuté en détail à l'Article 6, les activités d'évaluation des risques à l' Article 7 et les activités de traitement des risques à l' Article 8.

D'autres activités nécessaires à la gestion des risques liés à la sécurité des informations sont abordées à l'Article 10.

5.2 Cycles de gestion des risques liés à la sécurité de l'information

L'évaluation des risques et le traitement des risques doivent être mis à jour régulièrement et en fonction des changements. Cela devrait s'appliquer à l'ensemble de l'évaluation des risques et les mises à jour peuvent être divisées en deux cycles de gestion des risques :

— cycle stratégique, dans lequel les actifs de l'entreprise, les sources de risques et les menaces, les objectifs cibles ou les conséquences des événements liés à la sécurité de l'information évoluent à partir des changements survenus dans le contexte global de l'organisation. Cela peut donner lieu à une mise à jour globale de la ou des évaluations des risques et des traitements des risques. Cela peut également servir à identifier de nouveaux risques et à lancer de toutes nouvelles évaluations des risques ;

— cycle opérationnel, dans lequel les éléments mentionnés ci-dessus servent d'informations d'entrée ou de critères modifiés qui affecteront une évaluation des risques ou une évaluation dans laquelle les scénarios doivent être révisés et mis à jour. L'examen doit inclure la mise à jour du traitement des risques correspondant, le cas échéant.

Le cycle stratégique doit être mené sur une base plus longue ou lorsque des changements majeurs se produisent, tandis que le cycle opérationnel doit être plus court en fonction des risques détaillés identifiés et évalués ainsi que du traitement des risques associé.

Le cycle stratégique s'applique à l'environnement dans lequel l'organisation cherche à atteindre ses objectifs, tandis que le cycle opérationnel s'applique à toutes les évaluations des risques compte tenu du contexte du processus de gestion des risques. Dans les deux cycles, il peut y avoir de nombreuses évaluations des risques avec des contextes et une portée différents dans chaque évaluation.

6 Établissement du contexte

6.1 Considérations organisationnelles

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 4.1.

Une organisation est définie comme une personne ou un groupe de personnes qui a ses propres fonctions avec des responsabilités, des autorités et des relations pour atteindre ses objectifs. Une organisation n'est pas nécessairement une entreprise,

autre personne morale ou entité juridique, il peut également s'agir d'un sous-ensemble d'une entité juridique (par exemple le service informatique d'une entreprise), et peut être considéré comme « l'organisation » dans le contexte du SMSI.

Il est important de comprendre que l'appétit pour le risque, défini comme le niveau de risque qu'une organisation est prête à poursuivre ou à accepter, peut varier considérablement d'une organisation à l'autre. Par exemple, les facteurs affectant l'appétit pour le risque d'une organisation comprennent la taille, la complexité et le secteur. L'appétit pour le risque doit être défini et régulièrement examiné par la haute direction.

L'organisation doit s'assurer que le rôle du propriétaire du risque est déterminé en termes d'activités de gestion concernant les risques identifiés. Les propriétaires de risques doivent avoir une responsabilité et une autorité appropriées pour gérer les risques identifiés.

6.2 Identifier les exigences fondamentales des parties intéressées

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 4.2.

Les exigences fondamentales des parties intéressées concernées doivent être identifiées, ainsi que l'état de conformité à ces exigences. Cela inclut l'identification de tous les documents de référence qui définissent les règles et contrôles de sécurité et qui s'appliquent dans le cadre de l'évaluation des risques en matière de sécurité de l'information.

Ces documents de référence peuvent inclure, sans toutefois s'y limiter :

a) ISO/CEI 27001:2022, Annexe A ;

b) des normes supplémentaires couvrant le SMSI ;

c) des normes supplémentaires applicables à un secteur spécifique (par exemple financier, soins de santé) ;

d) réglementations internationales et/ou nationales spécifiques ;

e) les règles de sécurité interne de l'organisation ;

f) les règles de sécurité et les contrôles issus des contrats ou accords ;

g) les contrôles de sécurité mis en œuvre sur la base des activités antérieures de traitement des risques.

Tout non-respect des exigences fondamentales doit être expliqué et justifié. Ces exigences de base et leur respect devraient constituer la base de l'évaluation de la probabilité et du traitement des risques.

6.3 Application de l'évaluation des risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 4.3.

Les organisations peuvent effectuer des évaluations des risques intégrées à de nombreux processus différents, tels que la gestion de projet, la gestion des vulnérabilités, la gestion des incidents, la gestion des problèmes, ou même de manière impromptue pour un sujet spécifique identifié. Quelle que soit la manière dont les évaluations des risques sont réalisées, elles doivent couvrir collectivement toutes les questions pertinentes pour l'organisation dans le cadre de un SMSI.

L'évaluation des risques doit aider l'organisation à prendre des décisions concernant la gestion des risques qui affectent la réalisation de ses objectifs. Il convient donc de cibler les risques et les contrôles qui, s'ils sont gérés avec succès, amélioreront la probabilité que l'organisation atteigne ses objectifs.

De plus amples informations sur le contexte d'un SMSI et les questions à comprendre grâce à l'évaluation des risques sont données dans la norme ISO/IEC 27003.

6.4 Établir et maintenir des critères de risque pour la sécurité de l'information

6.4.1 Général

ISO/IEC 27001:2022, 6.1.2 a), spécifie les exigences permettant aux organisations de définir leurs critères de risque, c'est-à-dire les termes de référence par lesquels ils évaluent l'importance des risques qu'ils identifient et prennent des décisions concernant les risques.

La norme ISO/IEC 27001 spécifie les exigences imposées à une organisation pour établir et maintenir des critères de risque en matière de sécurité de l'information, notamment :

a) les critères d'acceptation des risques ;

b) les critères pour effectuer des évaluations des risques liés à la sécurité de l'information.

En général, pour définir des critères de risque, les éléments suivants doivent être pris en compte :

— la nature et le type d'incertitudes qui peuvent affecter les résultats et les objectifs (tant tangibles que intangible);

— comment les conséquences et la probabilité seront définies, prévues et mesurées ;

— les facteurs liés au temps ;

— cohérence dans l'utilisation des mesures ;

— comment le niveau de risque sera déterminé ;

— comment les combinaisons et séquences de risques multiples seront prises en compte ;

— la capacité de l'organisation.

D'autres considérations sur les critères de risque sont présentées à l'annexe A.

6.4.2 Critères d'acceptation des risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 a) 1).

Lors de l'évaluation des risques, des critères d'acceptation des risques doivent être utilisés pour déterminer si un risque est acceptable ou non. pas.

Dans le traitement des risques, les critères d'acceptation des risques peuvent être utilisés pour déterminer si le traitement des risques proposé est suffisant pour atteindre un niveau de risque acceptable, ou si un traitement des risques supplémentaire est nécessaire.

Une organisation doit définir des niveaux d'acceptation des risques. Les éléments suivants doivent être pris en compte lors du développement :

a) cohérence entre les critères d'acceptation des risques liés à la sécurité de l'information et les critères de l'organisation critères généraux d'acceptation des risques ;

b) le niveau de direction ayant le pouvoir délégué pour prendre des décisions en matière d'acceptation des risques est identifié ;

c) les critères d'acceptation des risques peuvent inclure plusieurs seuils, et l'autorité d'acceptation peut être attribuée à différents niveaux de gestion ;

d) les critères d'acceptation des risques peuvent être fondés uniquement sur la probabilité et les conséquences, ou peuvent être étendus pour prendre également en compte l'équilibre coûts/avantages entre les pertes potentielles et le coût des contrôles ;

e) différents critères d'acceptation des risques peuvent s'appliquer à différentes classes de risques (par exemple, les risques pouvant entraîner le non-respect des réglementations ou des lois ne sont pas toujours retenus, tandis que l'acceptation des risques peut être autorisée si l'acceptation résulte d'une exigence contractuelle) ;

f) les critères d'acceptation des risques peuvent inclure des exigences relatives à un traitement supplémentaire futur (par exemple, un risque peut être conservé à court terme même lorsque le niveau de risque dépasse les critères d'acceptation des risques s'il existe une approbation et un engagement à prendre des mesures pour mettre en œuvre un ensemble choisi de contrôles pour atteindre un niveau acceptable dans un délai défini) ;

g) les critères d'acceptation des risques doivent être définis sur la base de l'appétit pour le risque qui indique le montant et le type de risque que l'organisation est prête à poursuivre ou à conserver ;

h) les critères d'acceptation du risque peuvent être absolus ou conditionnels selon le contexte.

Les critères d'acceptation des risques doivent être établis en tenant compte des facteurs d'influence suivants :

— les objectifs organisationnels;

— les opportunités organisationnelles;

— les aspects juridiques et réglementaires ;

- les activités opérationnelles;

— les contraintes technologiques ;

- contraintes financières;

— les processus ;

— les relations avec les fournisseurs ;

— les facteurs humains (par exemple liés à la vie privée).

La liste des facteurs d'influence n'est pas exhaustive. L'organisation doit prendre en compte les facteurs d'influence en fonction du contexte.

Un simple critère d'acceptation (oui/non) ne suffit pas toujours en pratique.

Dans de nombreux cas, la décision d'accepter un risque peut être prise à des niveaux de risque spécifiques (combinaisons spécifiques de probabilité et de conséquences). Cependant, il peut y avoir des circonstances où il est nécessaire de fixer des seuils d'acceptation pour des conséquences extrêmes, quelle que soit leur probabilité, ou des probabilités extrêmement élevées, quelle que soit les conséquences, lorsque l'effet sur l'organisation résulte principalement de l'une ou de l'autre.

Par exemple, l'acceptation d'un événement rare qui anéantit la valeur boursière d'une entreprise, ou une ponction constante sur les ressources résultant de la nécessité de contrôler de fréquentes infractions mineures à une politique, doivent être considérées principalement en fonction du facteur qui a le plus d'importance. effet dominant sur l'organisation.

Par conséquent, les critères d'acceptation des risques devraient idéalement prendre en compte la probabilité et les conséquences de manière indépendante, ainsi que les coûts de gestion, plutôt que simplement le niveau de risque en tant que combinaison de probabilité et de conséquences.

Une organisation ayant un fort appétit pour le risque peut fixer un seuil d'acceptation plus élevé, acceptant ainsi plus de risques qu'une organisation ayant un appétit pour le risque plus faible. Cela protège l'organisation d'un contrôle excessif, c'est-à-dire d'un trop grand nombre de contrôles de sécurité de l'information qui empêchent l'organisation d'atteindre ses objectifs.

Les critères d'acceptation des risques peuvent différer en fonction de la durée pendant laquelle les risques sont attendus (par exemple, les risques peuvent être associés à une activité temporaire ou à court terme).

Les critères de risque doivent être régulièrement révisés et mis à jour si nécessaire à la suite de tout changement dans le contexte de la gestion des risques liés à la sécurité de l'information.

EXEMPLE Une petite entreprise peut initialement avoir un fort appétit pour le risque, mais à mesure qu'elle se développe, elle peut réduire son appétit pour le risque.

Les critères d'acceptation des risques doivent être approuvés par le niveau de gestion autorisé.

6.4.3 Critères pour effectuer des évaluations des risques liés à la sécurité de l'information

6.4.3.1 Général

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 a) 2).

Les critères d'évaluation des risques précisent comment l'importance d'un risque est déterminée en termes de conséquences, de probabilité et de niveau de risque.

Les critères d'évaluation des risques liés à la sécurité de l'information doivent prendre en compte le caractère approprié des activités de gestion des risques.

Les considérations pour y parvenir comprennent :

a) le niveau de classification des informations ;

b) la quantité et toute concentration d'informations ;

c) la valeur stratégique des processus commerciaux qui utilisent l'information ;

d) le caractère critique des informations et des actifs liés aux informations impliquées ;

e) importance opérationnelle et commerciale de la disponibilité, de la confidentialité et de l'intégrité ;

f) les attentes et perceptions des parties intéressées (par exemple la haute direction) ;

g) des conséquences négatives telles qu'une perte de clientèle et de réputation ;

h) cohérence avec les critères de risque organisationnels.

Les critères d'évaluation des risques, ou une base formelle pour leur définition, doivent être standardisés dans toute l'organisation pour tous les types d'évaluation des risques, car cela peut faciliter la communication, la comparaison et l'agrégation des risques associés à plusieurs domaines d'activité.

Les critères d'évaluation des risques liés à la sécurité de l'information comprennent généralement :

- conséquences;

- probabilité;

— niveau de risque.

6.4.3.2 Critères de conséquence

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 a) 2).

L'ISO/IEC 27001 concerne les conséquences qui sont directement ou indirectement affectées par la préservation ou la perte de la confidentialité, de l'intégrité et de la disponibilité des informations dans le cadre du SMSI.
Des critères de conséquences devraient être élaborés et spécifiés en termes d'étendue des dommages ou des pertes, ou du préjudice causé à une organisation ou à un individu résultant de la perte de confidentialité, d'intégrité et de disponibilité des informations. Lors de la définition des critères de conséquences, les éléments suivants doivent être particulièrement pris en compte :

a) perte de vie ou préjudice causé à des individus ou à des groupes ;

b) perte de liberté, de dignité ou de droit à la vie privée ;

c) perte de personnel et de capital intellectuel (compétences et expertise) ;

d) altération des opérations internes ou de tiers (par exemple, dommages à une fonction ou à un processus commercial) ;

e) les effets sur les plans et les délais ;

f) perte de valeur commerciale et financière ;

g) perte d'un avantage commercial ou d'une part de marché ;

h) atteinte à la confiance ou à la réputation du public ;

i) violations des exigences légales, réglementaires ou statutaires ;

j) ruptures de contrats ou de niveaux de service ;

k) impact négatif sur les parties intéressées ;

l) impact négatif sur l'environnement, pollution.

Les critères de conséquence définissent la manière dont une organisation catégorise l'importance des événements potentiels de sécurité des informations pour l'organisation. Il est essentiel de déterminer combien de catégories de conséquences sont utilisées, comment elles sont définies et quelles conséquences sont associées à chaque catégorie. Habituellement, les critères de conséquences sont différents pour différentes organisations en fonction du contexte interne et externe de l'organisation.

EXEMPLE 1 Le montant maximum que l'organisation est prête à radier au cours d'un exercice et le montant minimum au cours de la même période qui la forcerait à la liquidation peuvent créer des limites supérieures et inférieures réalistes de l'échelle des conséquences d'une organisation exprimée en termes monétaires.

Cet éventail dépendant du contexte peut ensuite être divisé en plusieurs catégories de conséquences, dont le nombre et la répartition doivent dépendre de la perception du risque et de l'appétit de l'organisation. Les échelles de conséquences monétaires sont généralement exprimées sur une échelle logarithmique, par exemple en décennies ou en puissances de 10 (par exemple 100 à 1 000 ; 1 à 10 000, etc.), mais d'autres schémas de quantification peuvent être utilisés lorsqu'ils correspondent mieux au contexte de l'organisation.

Étant donné que les conséquences dans différents domaines ou départements d'une organisation peuvent initialement être exprimées de différentes manières plutôt qu'en termes strictement monétaires, il est utile que ces diverses expressions puissent être croisées avec une échelle d'ancrage commune pour garantir des niveaux de conséquences à peu près équivalents dans l'organisation. les différents domaines sont correctement comparés les uns aux autres. Cela devrait permettre d’effectuer une agrégation des risques entre domaines.

EXEMPLE 2 Une violation de données, en plus d'avoir éventuellement un impact sur la vie privée des individus, peut entraîner une perte de confidentialité, d'intégrité ou de disponibilité des informations dans le cadre du SMSI. Cela peut également conduire au non-respect de la législation applicable en matière de protection des données. Les conséquences potentielles vont de la perte d'informations, de la perte d'actifs liés à l'information et du processus d'information, à la perte des objectifs commerciaux opérationnels et des activités projetées.

6.4.3.3 Critères de vraisemblance

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 a) 2).

La détermination des critères de vraisemblance dépend d’aspects tels que :

a) les événements accidentels ou naturels ;

b) le degré d'exposition des informations pertinentes ou des actifs liés aux informations à la menace ;

c) le degré d'exploitation de la vulnérabilité de l'organisation ;

d) échec technologique ;

e) actes ou omissions humains.

La probabilité peut être exprimée en termes probabilistes (la probabilité qu'un événement se produise dans une période donnée) ou en termes fréquentistes (le nombre moyen notionnel d'occurrences dans une période donnée). La vraisemblance exprimée en termes liés à la fréquence est souvent utilisée lorsqu'elle est communiquée, même si seule la vraisemblance exprimée en termes probabilistes peut être utilisée lors de l'agrégation des vraisemblances.

Les critères de vraisemblance doivent couvrir la gamme prévisible et gérable des probabilités d'événements anticipés. Au-delà des limites de la gérabilité pratique, il suffit généralement de reconnaître que l'une ou l'autre limite a été dépassée pour prendre une décision adéquate en matière de gestion des risques (désignation comme cas extrême). Si les échelles finies sont trop larges, cela entraîne généralement une quantification trop grossière et peut conduire à des erreurs d'évaluation. C'est particulièrement le cas lorsque les probabilités se situent dans l'extrémité supérieure des échelles représentées de manière exponentielle, car les incréments dans les fourchettes supérieures sont intrinsèquement très larges.

Même si presque tout est « possible », les sources de risques auxquelles il convient d'accorder une attention prioritaire sont celles dont les probabilités sont les plus pertinentes au contexte de l'organisation et à la portée de son SMSI.

6.4.3.4 Critères de détermination du niveau de risque

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 a) 2).

L'objectif des échelles de niveau de risque est d'aider les propriétaires de risques à décider de conserver ou de traiter autrement les risques et de les hiérarchiser en matière de traitement des risques. Le niveau évalué d'un risque particulier devrait aider l'organisation à déterminer l'urgence de traiter ce risque.

Selon la situation, il est recommandé de considérer le niveau de risque inhérent (sans tenir compte d'aucun contrôle) ou le niveau de risque actuel (en tenant compte de l'efficacité des contrôles déjà mis en œuvre). L'organisation doit élaborer un classement des risques, en tenant compte des éléments suivants :

a) les critères de conséquence et les critères de probabilité ;

b) les conséquences que les événements liés à la sécurité de l'information peuvent avoir aux niveaux stratégique, tactique et opérationnel (cela peut être défini comme le pire des cas ou en d'autres termes à condition que la même base soit utilisée de manière cohérente) ;

c) les exigences légales et réglementaires et les obligations contractuelles ;

d) les risques qui apparaissent au-delà des limites du périmètre de l'organisation, y compris les effets imprévus sur les tiers.

Des critères de niveau de risque sont nécessaires pour évaluer les risques analysés.

Les critères de niveau de risque peuvent être qualitatifs (par exemple très élevé, élevé, moyen, faible) ou quantitatifs (par exemple exprimés en termes de valeur attendue de perte monétaire, de perte de vies ou de part de marché sur une période de temps donnée).

EXEMPLE Les risques peuvent être quantifiés sous forme d'espérance de perte annuelle, c'est-à-dire la valeur monétaire moyenne de la conséquence par année subie au cours de l'année suivante.

Que des critères quantitatifs ou qualitatifs soient utilisés, les échelles d'évaluation doivent en fin de compte être ancrées sur une échelle de référence comprise par toutes les parties intéressées, et l'analyse et l'évaluation des risques doivent inclure au moins un calibrage formel périodique par rapport à l'échelle de référence pour garantir la validité, la cohérence et comparabilité des résultats.

Si une approche qualitative est utilisée, les niveaux de toute échelle qualitative doivent être sans ambiguïté, ses incréments doivent être clairement définis, les descriptions qualitatives de chaque niveau doivent être exprimées dans un langage objectif et les niveaux ne doivent pas se chevaucher. Lorsque différentes échelles sont utilisées (par exemple pour aborder les risques dans différents domaines d'activité), il doit y avoir une équivalence pour permettre des résultats comparables.

6.5 Choisir une méthode appropriée

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 b).

En général, l'approche et les méthodes de gestion des risques liés à la sécurité de l'information doivent être alignées sur l'approche et les méthodes utilisées pour gérer les autres risques de l'organisation.

L'approche choisie doit être documentée.

Selon la norme ISO/IEC 27001 :2022, 6.1.2 b), l'organisation entrant dans le champ d'application du SMSI est tenue de garantir que les évaluations répétées des risques liés à la sécurité de l'information produisent des résultats cohérents, valides et comparables. Cela signifie que la méthode choisie doit garantir les propriétés de résultats suivantes :

— cohérence : évaluations des mêmes risques réalisées par des personnes différentes ou par les mêmes personnes à différentes occasions, dans le même contexte, devrait produire des résultats similaires ;

— comparabilité: des critères d'évaluation des risques devraient être définis pour garantir que les évaluations effectuées pour différents risques produisent des résultats comparables lorsqu'elles représentent des niveaux de risque équivalents;

— validité: les évaluations doivent produire des résultats aussi proches que possible de la réalité.

Les méthodes de gestion des risques opérationnels sont généralement utilisées pour la gestion des risques liés à la sécurité de l'information. La méthode choisie peut utiliser toute approche appropriée en ce qui concerne l'utilisation du risque résiduel. Les approches les plus couramment utilisées pour la gestion des risques liés à la sécurité de l'information utilisent le risque actuel pour évaluer la probabilité et les conséquences des risques.

7 Processus d'évaluation des risques liés à la sécurité de l'information

7.1 Général

L'organisation doit utiliser le processus d'évaluation des risques organisationnels (s'il est établi) pour évaluer les risques liés aux informations ou pour définir un processus d'évaluation des risques liés à la sécurité de l'information.

L'évaluation des risques permet aux propriétaires de risques de hiérarchiser les risques en fonction de la perspective du traitement, en fonction principalement de leurs conséquences et de leur probabilité ou d'autres critères établis.

Le contexte de l'évaluation des risques doit être déterminé, y compris une description de la portée et de l'objectif.
ainsi que les problèmes internes et externes qui affectent l'évaluation des risques.

L'évaluation des risques comprend les activités suivantes :

a) l'identification des risques, qui est un processus permettant de trouver, reconnaître et décrire les risques (plus de détails sur les risques l'identification sont fournies en 7.2) ;

b) l'analyse des risques, qui est un processus permettant de comprendre les types de risques et de déterminer le niveau de risque. L'analyse des risques implique la prise en compte des causes et sources du risque, de la probabilité qu'un événement spécifique se produise, de la probabilité que cet événement ait des conséquences et de la gravité de ces conséquences (de plus amples détails sur l'analyse des risques sont fournis au point 7.3) ;

c) l'évaluation des risques, qui est un processus permettant de comparer les résultats de l'analyse des risques avec des critères de risque afin de déterminer si le risque et/ou son importance est acceptable et de hiérarchiser les risques analysés pour le traitement des risques. Sur la base de cette comparaison, la nécessité d'un traitement peut être envisagée (des détails supplémentaires sur l'évaluation des risques sont fournis en 7.4).

Le processus d'évaluation des risques doit être basé sur des méthodes (voir 6.5) et des outils conçus de manière suffisamment détaillée pour garantir, dans la mesure du possible, des résultats cohérents, valides et reproductibles. En outre, les résultats doivent être comparables, par exemple pour déterminer si le niveau de risque a augmenté ou diminué.

L'organisation doit s'assurer que son approche de gestion des risques liés à la sécurité de l'information s'aligne sur l'approche de gestion des risques organisationnels, afin que tout risque de sécurité de l'information puisse être comparé à d'autres risques organisationnels et non seulement considéré de manière isolée.

L'ISO/IEC 27001 n'exige pas qu'une approche particulière soit utilisée pour satisfaire aux exigences de l'ISO/IEC 27001:2022, 6.1.2. Il existe néanmoins deux principales approches d'évaluation : une approche basée sur les événements et une approche basée sur les actifs. Ils sont abordés plus en détail au point 7.2.1.

7.2 Identifier les risques liés à la sécurité des informations

7.2.1 Identifier et décrire les risques liés à la sécurité des informations

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 c) 1).

Entrée : événements pouvant influencer négativement la réalisation des objectifs de sécurité de l'information dans l'organisation ou dans d'autres organisations.

Action : Les risques associés à la perte de confidentialité, d'intégrité et de disponibilité des informations doivent être identifiés.

Déclencheur : les propriétaires de risques, les parties intéressées et/ou les experts détectent ou ont besoin de rechercher des événements ou des situations nouveaux ou modifiés qui peuvent affecter la réalisation des objectifs de sécurité de l'information.

Résultat : Une liste des risques identifiés.

Conseils de mise en œuvre :

L'identification des risques est le processus de recherche, de reconnaissance et de description des risques. Cela implique l'identification des sources et des événements de risque.

L'objectif de l'identification des risques est de générer une liste de risques basée sur les événements susceptibles d'empêcher, d'affecter ou de retarder la réalisation des objectifs de sécurité de l'information.

Les risques identifiés doivent être ceux qui, s'ils se matérialisent, peuvent avoir un effet sur la réalisation des objectifs.

ISO/IEC 27001:2022, 6.1.2 c), exige que l'organisation définisse et applique un processus d'évaluation des risques liés à la sécurité de l'information qui identifie les risques liés à la sécurité de l'information. Il existe deux approches couramment utilisées pour effectuer l'identification des risques.

a) Approche basée sur les événements : identifier des scénarios stratégiques en tenant compte des sources de risques et de la manière dont elles utilisent ou impactent les parties intéressées pour atteindre l'objectif souhaité de ces risques.

b) Approche basée sur les actifs : identifier des scénarios opérationnels détaillés en termes d'actifs et de menaces. et les vulnérabilités.

Dans une approche basée sur les événements, le concept sous-jacent est que les risques peuvent être identifiés et évalués grâce à une évaluation des événements et de leurs conséquences. Les événements et les conséquences peuvent souvent être déterminés par la découverte des préoccupations de la haute direction, des propriétaires des risques et des exigences identifiées lors de la détermination du contexte de l'organisation (ISO/IEC 27001:2022, Article 4). Les entretiens avec la haute direction et les personnes de l'organisation qui ont la responsabilité d'un processus métier peuvent aider à identifier non seulement les événements et les conséquences pertinents, mais également les propriétaires du risque.

Une approche basée sur les événements peut établir des scénarios stratégiques ou de haut niveau sans consacrer beaucoup de temps à l'identification des actifs à un niveau détaillé. Cela permet à l'organisation de concentrer ses efforts de traitement des risques sur les risques critiques. L'évaluation des événements selon cette approche peut utiliser des données historiques où les risques restent inchangés pendant de longues périodes et permet aux parties intéressées d'atteindre leurs objectifs. Toutefois, dans le cas de risques pour lesquels des données historiques ne sont pas disponibles ou fiables, les conseils fondés sur les connaissances et l'expérience d'experts ou l'enquête sur les sources de risques peuvent faciliter l'évaluation.

Avec une approche basée sur les actifs, le concept sous-jacent est que les risques peuvent être identifiés et évalués grâce à une inspection des actifs, des menaces et des vulnérabilités. Un actif est tout ce qui a de la valeur pour l'organisation et qui nécessite donc une protection. Les actifs doivent être identifiés, en tenant compte du fait qu'un système d'information est constitué d'activités, de processus et d'informations à protéger. Les actifs peuvent être identifiés comme étant les actifs principaux et les actifs de support en fonction de leur type et de leur priorité, en mettant en évidence leurs dépendances, ainsi que leurs interactions avec leurs sources de risques et les parties intéressées de l'organisation. Une menace exploite une vulnérabilité d'un actif pour compromettre la confidentialité, l'intégrité et/ou la disponibilité des informations correspondantes. Si toutes les combinaisons valides d'actifs, de menaces et de vulnérabilités

peuvent être répertoriés dans le cadre du SMSI, alors, en théorie, tous les risques seraient identifiés. Pour les étapes ultérieures de l'évaluation des risques, une liste des actifs associés aux informations et aux installations de traitement de l'information doit être établie.

L'approche basée sur les actifs peut identifier les menaces et les vulnérabilités spécifiques aux actifs et permet à l'organisation de déterminer le traitement des risques spécifiques à un niveau détaillé.

De plus amples informations sur les deux approches sont données dans l'Annexe A.

En principe, les deux approches ne diffèrent que par le niveau auquel l'identification est initiée.
Les deux approches peuvent décrire le même scénario de risque, par exemple lorsqu'un actif informationnel se situe au niveau détaillé et qu'une exposition commerciale se situe au niveau général. L'identification des sources de risque contributives à l'aide d'une évaluation basée sur les événements nécessite généralement d'explorer le niveau général du scénario jusqu'au niveau détaillé, mais une évaluation basée sur les actifs recherche généralement vers le haut, de l'actif au scénario, afin de fournir une visibilité sur la façon dont les conséquences s'accumulent.

L'identification des risques est essentielle, car un risque de sécurité de l'information qui n'est pas identifié à ce stade n'est pas inclus dans une analyse plus approfondie.

L'identification des risques doit prendre en compte les risques, que leur source soit ou non sous le contrôle de l'organisation, même si aucune source de risque spécifique n'est évidente. En particulier lors de l'évaluation de scénarios de risques complexes, une évaluation itérative des risques doit être menée. Le premier cycle devrait se concentrer sur des observations de haut niveau et les cycles suivants devraient aborder des niveaux de détail supplémentaires jusqu'à ce que les causes profondes des risques puissent être identifiées.

Toute autre approche d'identification des risques peut être utilisée à condition qu'elle garantisse la production de résultats cohérents, valides et comparables, répondant aux exigences de la norme ISO/IEC 27001:2022, 6.1.2 b).

La gestion des risques liés à la sécurité de l'information ne doit pas être limitée par des vues arbitraires ou restrictives sur la manière dont les risques doivent être structurés, regroupés, agrégés, divisés ou décrits. Les risques peuvent sembler se chevaucher ou être des sous-ensembles ou des instances spécifiques d'autres risques. Toutefois, les contrôles des risques individuels doivent être considérés et identifiés séparément des risques plus larges ou des risques agrégés aux fins de l'analyse des risques.
traitement.

EXEMPLE 1 Un exemple de deux risques qui se chevauchent : (1) il existe un risque d'incendie au siège social ; (2) il existe un risque d'incendie affectant le fonctionnement du service comptable où la comptabilité est située au siège social mais également dans plusieurs autres bâtiments.

Un exemple de cas spécifiques de risque : (1) il y a un incident de perte de données ; (2) il y a un incident de perte de données personnelles.

Le deuxième risque est une instance spécifique du premier risque, mais il est susceptible d'avoir des attributs et des contrôles différents de ceux du premier risque, et il peut être important de le gérer séparément du premier risque, beaucoup plus large.

Le regroupement des risques ne doit pas être entrepris à moins qu'ils ne soient pertinents les uns par rapport aux autres au niveau auquel le contexte de l'organisation est pris en compte. Il peut être nécessaire de considérer séparément les risques qui sont fusionnés aux fins de la budgétisation globale de la gestion des risques, lors de la planification des options de traitement, car différents contrôles peuvent être nécessaires pour les gérer.

EXEMPLE 2 Un centre de données peut être soumis à plusieurs risques indépendants : inondation, incendie, pics de tension électrique et vandalisme.

Pour estimer le niveau global de risque d'entreprise, les risques individuels de ces événements peuvent être combinés en un niveau de risque global, mais comme chacun de ces événements nécessite des contrôles différents pour gérer le risque, ils doivent être considérés et identifiés séparément aux fins de traitement des risques. Les risques (combinaisons de probabilités et de conséquences) ne peuvent pas toujours être regroupés directement.

7.2.2 Identification des propriétaires de risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 c) 2).

Entrée : Liste des risques identifiés.

Action : Les risques doivent être associés aux propriétaires des risques.

~~Déclencheu~~r : L'identification des propriétaires de risques devient nécessaire lorsque :

— cela n'a jamais été fait auparavant;

— il y a un changement de personnel dans le domaine d'activité concerné où résident les risques ;

~~Résultat :~~ Liste des propriétaires de risques avec les risques associés.

~~Conseils de mise en œuvre :~~

La haute direction, le comité de sécurité, les propriétaires de processus, les propriétaires fonctionnels, les chefs de service et les propriétaires d'actifs peuvent être les propriétaires des risques.

Une organisation doit utiliser le processus d'évaluation des risques organisationnels (s'il est établi) pour identifier les propriétaires de risques, sinon elle doit définir des critères d'identification des propriétaires de risques. Ces critères devraient tenir compte du fait que les propriétaires de risques :

— sont responsables et disposent de l'autorité nécessaire pour gérer les risques qu'ils possèdent, c'est-à-dire qu'ils doivent occuper un poste au sein de l'organisation qui leur permet d'exercer effectivement cette autorité ;

— comprendre les problèmes en jeu et être en mesure de prendre des décisions éclairées (par exemple sur la manière dont pour traiter les risques).

Le niveau de risque et l'actif auquel le risque doit s'appliquer peuvent servir de base à l'identification du risque.
les propriétaires.

L'attribution devrait avoir lieu dans le cadre du processus d'évaluation des risques.

7.3 Analyse des risques liés à la sécurité des informations

7.3.1 Général

L'analyse des risques a pour objectif de déterminer le niveau du risque.

L'ISO 31000 est référencée dans l'ISO/IEC 27001 comme modèle général. ISO/IEC 27001:2022, 6.1.2, exige que pour chaque risque identifié, l'analyse des risques soit basée sur l'évaluation des conséquences résultant du risque et sur l'évaluation de la probabilité du risque pour déterminer un niveau de risque.

Les techniques d'analyse des risques basées sur les conséquences et la probabilité peuvent être :

a) qualitatif, en utilisant une échelle d'attributs qualificatifs (par exemple élevé, moyen, faible) ; ou

b) quantitatif, en utilisant une échelle avec des valeurs numériques (par exemple coût monétaire, fréquence ou probabilité de occurrence); ou

c) semi-quantitatif, utilisant des échelles qualitatives avec des valeurs attribuées.

L'analyse des risques doit être ciblée sur les risques et les contrôles qui, s'ils sont gérés avec succès, améliorent la probabilité que l'organisation atteigne ses objectifs. Il est facile de consacrer beaucoup de temps à une évaluation des risques, notamment à l'évaluation des probabilités et des conséquences. Pour permettre une prise de décision efficace en matière de gestion des risques, il peut suffire d'utiliser des estimations initiales et approximatives de la probabilité et des conséquences.

7.3.2 Évaluation des conséquences potentielles

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 d) 1).

~~Entrée :~~ Une liste d'événements ou de scénarios de risques pertinents identifiés, y compris l'identification des sources de risques, ainsi que les processus commerciaux, les objectifs commerciaux et les critères de conséquences. En outre, des listes de tous les contrôles existants, leur efficacité, leur mise en œuvre et leur état d'utilisation.

Action : Les conséquences résultant de l'incapacité à préserver de manière adéquate la confidentialité, l'intégrité ou la disponibilité des informations doivent être identifiées et évaluées.

Déclencheur : L'évaluation des conséquences devient nécessaire lorsque :

— cela n'a jamais été fait auparavant;

— la liste produite par « identification des risques » est modifiée ;

— les propriétaires de risques ou les parties intéressées ont modifié les unités dans lesquelles ils souhaitent que les conséquences soient appliquées spécifié; ou

— des changements dans la portée ou le contexte sont déterminés et affectent les conséquences.

Résultat : Une liste de conséquences potentielles liées aux scénarios de risque avec leurs conséquences liées aux actifs ou aux événements, selon l'approche appliquée.

Conseils de mise en œuvre :

Le fait de ne pas préserver adéquatement la sécurité des informations peut entraîner la perte de leur confidentialité, de leur intégrité ou de leur disponibilité. La perte de confidentialité, d'intégrité ou de disponibilité peut avoir d'autres conséquences sur l'organisation et ses objectifs. L'analyse des conséquences peut être effectuée de bas en haut à partir des conséquences sur la sécurité de l'information en considérant ce qui peut se produire en cas de perte de confidentialité, d'intégrité ou de disponibilité des informations en question. En règle générale, le propriétaire du risque peut estimer les conséquences si l'événement se produit. Les éléments suivants doivent être pris en considération :

— estimation (ou mesure basée sur l'expérience) des pertes (de temps ou de données) dues à l'événement suite à l'interruption ou à la perturbation des opérations ;

— estimation/perception de la gravité de la conséquence (par exemple exprimée en argent) ;

— les coûts de recouvrement selon que le recouvrement peut être effectué en interne (par l'équipe propriétaire du risque) ou s'il est nécessaire de faire appel à une entité externe.

7.3.3 Évaluation de la probabilité

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 d) 2).

Entrée : Une liste d'événements ou de scénarios de risques pertinents identifiés, y compris l'identification des sources de risques, ainsi que les processus commerciaux, les objectifs commerciaux et les critères de probabilité. De plus, des listes de tous les contrôles existants, leur efficacité, leur mise en œuvre et leur état d'utilisation.

Action : La probabilité d'occurrence de scénarios possibles ou réels doit être évaluée et exprimée à l'aide de critères de probabilité établis.

Déclencheur : Outre les conséquences, l'évaluation de la probabilité est une activité clé du processus d'évaluation des risques lors de la détermination du niveau de risque.

L'évaluation de la probabilité devient nécessaire lorsque :

— cela n'a jamais été fait auparavant;

— des changements dans la portée ou le contexte sont déterminés et peuvent affecter la probabilité ;

— des vulnérabilités sont découvertes dans les contrôles mis en œuvre ;

— les tests/audits d'efficacité des contrôles aboutissent à des résultats inattendus ;

— des changements sont découverts dans l'environnement de la menace (par exemple, de nouveaux acteurs/sources de menace).

Résultat : Une liste d'événements ou de scénarios de risque complétée par les probabilités qu'ils se produisent.

Conseils de mise en œuvre :

Après avoir identifié les scénarios de risque, il est nécessaire d'analyser la probabilité que chaque scénario et conséquence se produise, à l'aide de techniques d'analyse qualitative ou quantitative. Évaluer la probabilité n'est pas toujours facile et doit être exprimé de différentes manières. Cela devrait prendre en compte la fréquence à laquelle les sources de risque surviennent ou la facilité avec laquelle certaines d'entre elles (par exemple les vulnérabilités) peuvent être exploitées, en considérant :

— l'expérience et les statistiques applicables concernant la probabilité de source de risque ;

— pour les sources de risque délibérées: le degré de motivation [par exemple la viabilité (coût/bénéfice) de l'attaque] et les capacités (par exemple le niveau de compétence des attaquants potentiels), qui évoluent dans le temps, les ressources disponibles pour les attaquants potentiels et les influences sur d'éventuels attaquants tels que la grande criminalité, les organisations terroristes ou les services de renseignement étrangers, ainsi que sur la perception de l'attrait et de la vulnérabilité des informations pour un éventuel attaquant ;

— pour les sources de risques accidentels: facteurs géographiques (par exemple, proximité d'installations ou d'activités dangereuses), possibilité de catastrophes naturelles telles que conditions météorologiques extrêmes, activité volcanique, tremblements de terre, inondations, tsunamis et facteurs pouvant influencer les erreurs humaines et le dysfonctionnement des équipements;

— les faiblesses connues et les éventuels contrôles compensatoires, tant individuellement que globalement;

— les contrôles existants et leur efficacité pour réduire les faiblesses connues.

L'estimation de la vraisemblance est intrinsèquement incertaine, non seulement parce qu'elle prend en compte des choses qui ne se sont pas encore produites et ne sont donc pas entièrement connues, mais aussi parce que la vraisemblance est une mesure statistique et n'est pas directement représentative d'événements individuels. Les trois sources fondamentales d'incertitude d'évaluation sont :

— l'incertitude personnelle provenant du jugement de l'évaluateur, qui découle de la variabilité de l'heuristique mentale de la prise de décision ;

— l'incertitude méthodologique, qui découle de l'utilisation d'outils qui modélisent inévitablement les événements de manière simpliste ;

— l'incertitude systémique sur l'événement anticipé lui-même, qui découle d'une connaissance insuffisante (en particulier si les preuves sont limitées ou si une source de risque change avec le temps).

Pour augmenter la fiabilité de l'estimation de la probabilité, les organisations devraient envisager d'utiliser :

a) des évaluations d'équipe plutôt que des évaluations individuelles ;

b) des sources externes, telles que des rapports sur les violations de la sécurité des informations ;

c) des échelles avec une portée et une résolution adaptées à l'approche de l'organisation ;

d) des catégories sans ambiguïté, telles que « une fois par an » plutôt que « peu fréquent ».

Lors de l'évaluation de la probabilité d'événements, il est important de reconnaître la différence entre les événements indépendants et dépendants. La probabilité d'événements qui dépendent les uns des autres est conditionnée par la relation entre eux (par exemple, un deuxième événement peut être inévitable si un premier événement se produit), de sorte qu'une évaluation séparée de leurs deux probabilités n'est pas nécessaire. La probabilité d'événements indépendants pertinents contribue de manière essentielle à la probabilité d'une conséquence à laquelle ils contribuent.

EXEMPLE La probabilité d'une attaque par déni de service sur un serveur dépend du paysage actuel des menaces ainsi que de la vulnérabilité et de l'accessibilité du serveur. Cependant, la probabilité de paquets malveillants peut atteindre 100 % une fois l'attaque lancée et son évaluation ne permet pas d'évaluer la probabilité d'une attaque par déni de service.

Pour éviter une complexité inutile de l'évaluation, il est important d'identifier toutes les dépendances entre les événements contribuant à un scénario de risque et, en premier lieu, d'évaluer les probabilités de ces événements qui sont indépendants les uns des autres.

La probabilité globale des conséquences commerciales d'un événement de sécurité de l'information dépend généralement de la probabilité de plusieurs événements contributifs de niveau inférieur et de leurs conséquences. Plutôt que de tenter d'estimer la probabilité des conséquences commerciales dans le cadre d'une seule évaluation de haut niveau,

il peut être plus valable de commencer par regrouper les probabilités des niveaux inférieurs évalués individuellement. événements qui y contribuent.

7.3.4 Détermination des niveaux de risque

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 d) 3).

Entrée : Une liste de scénarios de risque avec leurs conséquences liées aux actifs ou aux événements et leur probabilité (quantitative ou qualitative).

Action : Le niveau de risque doit être déterminé comme une combinaison de la probabilité évaluée et des conséquences évaluées pour tous les scénarios de risque pertinents.

Déclencheur : La détermination des niveaux de risque devient nécessaire si les risques liés à la sécurité des informations doivent être évalués.

Résultat : Une liste de risques avec des valeurs de niveau attribuées.

Conseils de mise en œuvre :

Le niveau de risque peut être déterminé de plusieurs manières possibles. Elle est généralement déterminée comme une combinaison de la probabilité évaluée et des conséquences évaluées pour tous les scénarios de risque pertinents. Des calculs alternatifs peuvent inclure une valeur d'actif ainsi que la probabilité et les conséquences. De plus, le calcul n'est pas nécessairement linéaire, par exemple il peut s'agir d'un carré de vraisemblance combiné à une conséquence. Dans tous les cas, le niveau de risque doit être déterminé à l'aide des critères établis comme décrit au point 6.4.3.4.

7.4 Évaluation des risques liés à la sécurité des informations

7.4.1 Comparaison des résultats de l'analyse des risques avec les critères de risque

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 e) 1).

Entrée : Une liste de critères de risque et de risques avec des valeurs de niveau attribuées.

Action : Le niveau de risque doit être comparé aux critères d'évaluation des risques, en particulier aux critères d'acceptation des risques.

Déclencheur : La comparaison des résultats de l'analyse des risques avec les critères de risque devient nécessaire si les risques liés à la sécurité de l'information doivent être traités en priorité.

Résultat : Une liste de suggestions de décisions sur des actions supplémentaires concernant la gestion des risques.

Conseils de mise en œuvre :

Une fois les risques identifiés et les valeurs de probabilité et de gravité des conséquences attribuées, les organisations doivent appliquer leurs critères d'acceptation des risques pour déterminer si les risques peuvent ou non être acceptés. S'ils ne peuvent pas être acceptés, ils doivent alors être traités en priorité.

Pour évaluer les risques, les organisations doivent comparer les risques évalués avec les critères de risque définis lors de l'établissement du contexte.

Les décisions en matière d'évaluation des risques doivent être fondées sur la comparaison du risque évalué avec des critères d'acceptation définis, idéalement en tenant compte du degré de confiance dans l'évaluation. Dans certains cas, comme la survenue fréquente d'événements aux conséquences relativement faibles, il peut être utile de considérer leur effet cumulatif sur une certaine période d'intérêt, plutôt que le risque de chaque événement considéré individuellement, car cela peut fournir une représentation plus réaliste de l'ensemble de la situation. des risques.

Il peut y avoir des incertitudes quant à la définition de la frontière entre les risques qui nécessitent un traitement et ceux qui n'en nécessitent pas. Dans certaines circonstances, l'utilisation d'un niveau unique comme niveau de risque acceptable qui sépare les risques qui nécessitent un traitement de ceux qui n'en nécessitent pas n'est pas toujours approprié. Dans certains cas,

il peut être plus efficace d'inclure un élément de flexibilité dans les critères en incorporant des paramètres supplémentaires tels que le coût et l'efficacité des contrôles possibles.

Les niveaux de risque peuvent être validés sur la base d'un consensus entre les propriétaires de risques et les spécialistes commerciaux et techniques. Il est important que les propriétaires de risques aient une bonne compréhension des risques dont ils sont responsables, ce qui concorde avec les résultats d'une évaluation objective. Par conséquent, toute disparité entre les niveaux de risque évalués et ceux perçus par les propriétaires du risque doit être étudiée afin de déterminer lequel se rapproche le mieux de la réalité.

7.4.2 Priorisation des risques analysés pour le traitement des risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.2 e) 2).

Entrée : Une liste des résultats des risques comparés aux critères de risque.

Action : Les risques figurant sur la liste doivent être traités en priorité en fonction des niveaux de risques évalués.

Déclencheur : la priorisation des risques analysés pour le traitement des risques devient nécessaire si les risques liés à la sécurité de l'information doivent être traités.

Résultat : Une liste de risques prioritaires avec des scénarios de risque qui conduisent à ces risques.

Conseils de mise en œuvre :

L'évaluation des risques utilise la compréhension du risque obtenue par l'analyse des risques pour faire des propositions permettant de décider de la prochaine étape à franchir. Ceux-ci doivent faire référence à :

— si un traitement des risques est nécessaire ;

— les priorités en matière de traitement des risques compte tenu des niveaux de risques évalués.

Les critères de risque utilisés pour prioriser les risques doivent tenir compte des objectifs de l'organisation, des exigences contractuelles, légales et réglementaires et des points de vue des parties intéressées concernées. Les priorités telles qu'elles sont prises dans le cadre de l'activité d'évaluation des risques reposent principalement sur les critères d'acceptation.

8 Processus de traitement des risques liés à la sécurité de l'information

8.1 Général

L'entrée du traitement des risques liés à la sécurité de l'information est basée sur les résultats du processus d'évaluation des risques sous la forme d'un ensemble hiérarchisé de risques à traiter, sur la base de critères de risque.

Le résultat de ce processus est un ensemble de contrôles de sécurité des informations nécessaires [voir ISO/IEC 27001:2022, 6.1.3 b)] qui doivent être déployés ou améliorés les uns par rapport aux autres, conformément au plan de traitement des risques [voir ISO/CEI 27001:2022, 6.1.3 e)]. Déployé de cette manière, l'efficacité du plan de traitement des risques est de modifier le risque de sécurité de l'information auquel l'organisation est confrontée afin qu'il réponde aux critères d'acceptation de l'organisation.

8.2 Sélection des options appropriées de traitement des risques liés à la sécurité de l'information

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 a).

Entrée : une liste de risques prioritaires avec des scénarios d'événements ou de risques qui conduisent à ces risques.

Action : Des options de traitement des risques doivent être choisies.

Déclencheur : La sélection d'options appropriées de traitement des risques en matière de sécurité de l'information devient nécessaire si aucun plan de traitement des risques n'existe ou si le plan est incomplet.

Résultat : Une liste de risques prioritaires avec les options de traitement des risques sélectionnées.

Conseils de mise en œuvre :

Plusieurs options de traitement des risques comprennent :

— l'évitement du risque, en décidant de ne pas démarrer ou poursuivre l'activité qui donne naissance au risque;

— modification du risque, en modifiant la probabilité de survenance d'un événement ou d'une conséquence ou en modifiant la gravité de la conséquence ;

— la rétention des risques, par un choix éclairé ;

— le partage des risques, en répartissant les responsabilités avec d'autres parties, soit en interne, soit en externe (par exemple partage des conséquences via une assurance) ;

EXEMPLE 1 Un exemple d'évitement des risques est un bureau situé dans une zone inondable, où il existe un risque d'inondation et les dommages qui en résultent pour le bureau et des restrictions à la disponibilité et/ou à l'accès au bureau. Les contrôles physiques pertinents peuvent s'avérer insuffisants pour réduire ce risque, auquel cas l'option thérapeutique consistant à éviter le risque peut être la meilleure option disponible. Cela peut impliquer la fermeture ou l'arrêt des activités de ce bureau.

EXEMPLE 2 Un autre exemple d'évitement des risques consiste à choisir de ne pas collecter certaines informations auprès des individus afin qu'il ne soit pas nécessaire à l'organisation de gérer, stocker et transmettre les informations dans ses systèmes d'information.

Dans le cas du partage des risques, au moins un contrôle est requis pour modifier la probabilité ou la conséquence, mais l'organisation délègue la responsabilité de mettre en œuvre le contrôle à une autre partie.

Les options de traitement des risques doivent être sélectionnées en fonction des résultats de l'évaluation des risques, des coûts attendus pour la mise en œuvre de ces options et des avantages attendus de ces options, à la fois individuellement et dans le contexte d'autres contrôles. Le traitement des risques doit être hiérarchisé en fonction des niveaux de risque tels que définis, des contraintes de temps et de la séquence nécessaire de mise en œuvre, ainsi que des résultats de l'évaluation des risques établis au point 7.4. Lors du choix de l'option, il peut être tenu compte de la manière dont un risque particulier est perçu par les parties concernées et des moyens les plus appropriés de communiquer le risque à ces parties.

8.3 Déterminer tous les contrôles nécessaires à la mise en œuvre des options de traitement des risques liés à la sécurité de l'information

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 b).

Entrée : Une liste de risques prioritaires avec les options de traitement des risques sélectionnées.

Action : Déterminer tous les contrôles, à partir des ensembles de contrôles choisis à partir d'une source appropriée, qui sont nécessaires au traitement des risques en fonction des options de traitement des risques choisies, telles que modifier, conserver, éviter ou partager les risques.

Déclencheur : conformité au SMSI ; gérer les risques liés à la sécurité de l'information.

Résultat : Tous les contrôles nécessaires.

Conseils de mise en œuvre :

Une attention particulière doit être accordée à la détermination des contrôles nécessaires. Chaque contrôle doit être vérifié pour déterminer s'il est nécessaire en posant les questions :

— quel effet ce contrôle a sur la probabilité ou les conséquences de ce risque ;

— de quelle manière le contrôle maintient le niveau de risque.

Seuls les contrôles qui ont un effet plus que négligeable sur le risque doivent être qualifiés de « nécessaires ».
Un ou plusieurs contrôles doivent être appliqués à chaque risque évalué comme nécessitant un traitement.

Il existe de nombreuses sources d'ensembles de contrôle. Ils peuvent être trouvés dans la norme ISO/IEC 27001:2022, Annexe A, dans les codes de bonnes pratiques spécifiques au secteur (par exemple ISO/IEC 27017) et dans d'autres ensembles de contrôles industriels nationaux, régionaux. Une organisation peut également déterminer un ou plusieurs contrôles « personnalisés » (voir ISO/IEC 27003).

Si un contrôle personnalisé est défini, le libellé du contrôle doit décrire avec précision et équité ce qu'est le contrôle et comment il fonctionne. Le cas échéant, cette formulation peut utilement inclure des aspects tels que :

— s'agit-il d'un contrôle documenté ;

— à qui appartient le contrôle ;

— comment il est surveillé ;

— comment cela peut-il être démontré ;

— les éventuelles exceptions ;

— fréquence de fonctionnement du contrôle ;

— la tolérance pour le contrôle ;

— si ce n'est pas évident, la raison pour laquelle le contrôle existe.

Si le contrôle se situe en dehors de la tolérance, cela signifie qu'il ne fonctionne pas suffisamment efficacement pour gérer le risque identifié.

EXEMPLE 1 « Un processus documenté de gestion des logiciels malveillants est en place et appartient au responsable de la sécurité informatique. Cela exclut les Mac et est surveillé via la console du fournisseur avec des rapports sur les performances envoyés chaque semaine au CIO.

Une telle approche détaillée de la formulation des contrôles peut être utile si les contrôles personnalisés sont également destinés à aider l'organisation dans le reporting d'assurance des contrôles. Cependant, il est plus important que la formulation des contrôles ait un sens pour les personnes au sein de l'organisation et les aide à prendre des décisions concernant la gestion de ces contrôles et des risques associés.

La détermination des contrôles peut inclure de nouveaux contrôles non encore mis en œuvre, ou peut inclure l'utilisation de contrôles qui existent dans l'organisation. Toutefois, un contrôle déjà opérationnel ne devrait pas être automatiquement inclus dans l'évaluation des risques car :

— le contrôle n'est pas nécessaire pour gérer un ou plusieurs risques liés à la sécurité de l'information ;

— il peut s'agir d'un contrôle qui aide d'une manière ou d'une autre à gérer un ou plusieurs risques liés à la sécurité de l'information, mais qui n'est pas suffisamment efficace pour être inclus dans l'évaluation des risques ou géré par le SMSI, ou ;

— il peut être actuellement opérationnel pour des raisons non liées à la sécurité de l'information (par exemple qualité, efficacité, efficacité ou conformité), ou ;

— il est actuellement opérationnel mais, du point de vue de la sécurité de l'information, il peut être supprimé car il n'a pas suffisamment d'effet pour justifier son maintien en tant que contrôle essentiel.

Si un contrôle est utilisé à des fins autres que la seule gestion des risques liés à la sécurité de l'information, il convient de veiller à ce que le contrôle soit géré de manière à atteindre les objectifs de sécurité de l'information ainsi que les objectifs non liés à la sécurité de l'information.

EXEMPLE 2 CCTV interne pour contrôler la qualité du processus de production ainsi que pour des raisons de sécurité des informations (pour se protéger contre la fraude).

Lors de la détermination des contrôles à partir d'un ensemble de contrôles existant (par exemple ISO/IEC 27001:2022, Annexe A ou une liste de contrôles spécifique au secteur), le libellé du contrôle doit correspondre à ce qui est nécessaire pour gérer le risque et refléter avec précision ce qu'est ou devrait être le contrôle. être. Si l'approche globale consiste à utiliser un ensemble de contrôles existant (par exemple ISO/IEC 27001:2022, Annexe A ou une liste de contrôles spécifique au secteur) et que l'ensemble de contrôles ne contient pas de contrôle décrivant avec précision le contrôle nécessaire, il convient alors d'envisager donné à la définition d'un contrôle personnalisé qui décrit avec précision le contrôle.

Les contrôles peuvent être classés comme préventifs, détectifs et correctifs :

a) contrôle préventif : un contrôle destiné à empêcher la survenance d'un problème de sécurité de l'information
événement pouvant entraîner la survenance d'une ou plusieurs conséquences ;

b) contrôle de détection : un contrôle destiné à détecter l'apparition d'un problème de sécurité de l'information.
événement;

c) contrôle correctif : un contrôle qui vise à limiter les conséquences d'une sécurité de l'information
événement.

Le type de contrôle décrit si un contrôle agit, ou a l'intention d'agir, pour prévenir ou détecter un événement ou réagir à ses conséquences.

EXEMPLE 3 Une politique de sécurité de l'information est un contrôle qui maintient le risque, mais la conformité à la politique vise à réduire la probabilité d'apparition d'un risque et peut donc être classée comme étant préventive.

L'utilité de catégoriser les contrôles en préventifs, détectives et correctifs réside dans leur utilisation, pour garantir que la construction de plans de traitement des risques est résiliente aux défaillances des contrôles. À condition qu'il existe une combinaison appropriée de contrôles préventifs, de détection et correctifs :

— les contrôles de détection devraient atténuer les risques en cas d'échec des contrôles préventifs ;

— les contrôles correctifs devraient atténuer les risques en cas d'échec des contrôles de détection ;

— les contrôles préventifs devraient réduire la probabilité que les contrôles correctifs soient un jour nécessaires
utilisé.

Lorsqu'elles utilisent des contrôles, les organisations doivent d'abord décider s'il est possible de détecter l'occurrence d'un événement. Si tel est le cas, des contrôles de détection doivent être mis en œuvre. S'il n'est pas possible de détecter un événement, les contrôles de détection peuvent s'avérer inefficaces, sans aucun moyen de savoir si un contrôle préventif fonctionne.

EXEMPLE 4 S'il n'est pas clair si un ordinateur fait partie d'un « botnet », on ne peut pas savoir si les contrôles utilisés pour l'empêcher de devenir partie d'un botnet fonctionnent comme prévu.

Les contrôles de détection peuvent fonctionner comme il convient, mais ils peuvent néanmoins être inefficaces.

EXEMPLE 5 La mise en œuvre de systèmes de détection/prévention des intrusions peut être un moyen efficace d'empêcher les logiciels malveillants de traverser le réseau, mais ils ne sont d'aucune utilité s'il n'y a pas de surveillance des systèmes/d'alertes d'action en cas d'épidémie non maîtrisée.

En général, les contrôles de détection sont finalement inefficaces dans les cas où ils peuvent être contournés ou lorsque leur notification n'aboutit pas à une action appropriée. Il faudra ensuite envisager des contrôles correctifs. Si les contrôles de détection échouent, il est probable qu'il y ait une ou plusieurs conséquences indésirables.
La mise en œuvre de contrôles correctifs peut contribuer à limiter ces conséquences. Même si les contrôles correctifs prennent effet après l'apparition des conséquences, il est souvent nécessaire de les déployer bien avant la survenance d'un événement.

EXEMPLE 6 Le chiffrement du disque dur n'empêche pas le vol d'un ordinateur portable ni les tentatives ultérieures d'extraction des données. Cela réduit toutefois la gravité des conséquences liées à une divulgation. Bien entendu, le contrôle doit être déployé avant que l'ordinateur portable ne soit volé.

La catégorisation des contrôles n'est pas absolue et dépend du contexte dans lequel l'utilisation d'un contrôle est effectuée.
décrit.

EXEMPLE 7 La sauvegarde n'empêche pas l'apparition d'un événement qui entraînerait autrement une perte de données (par exemple un crash de tête de disque ou la perte d'un ordinateur portable), mais elle contribue à réduire les conséquences. Certaines organisations peuvent donc considérer qu'il s'agit d'un contrôle correctif plutôt que d'un contrôle préventif. De même, le chiffrement n'empêche pas la perte d'informations, mais si l'événement est décrit comme « des données personnelles révélées à un attaquant », alors le chiffrement est un contrôle préventif plutôt que correctif.

L'ordre dans lequel sont organisés les contrôles portant sur les risques dépend de différents facteurs. De nombreuses techniques peuvent être utilisées. Il incombe aux propriétaires de risques respectifs de décider de l'équilibre entre les coûts d'investissement dans les contrôles et l'acceptation des conséquences au cas où les risques se matérialiseraient.

L'identification des contrôles existants peut déterminer que ces contrôles dépassent les besoins actuels. Un coût-
une analyse des avantages doit être entreprise avant de supprimer les contrôles redondants ou inutiles (surtout si les contrôles ont des coûts de maintenance élevés). Étant donné que les contrôles peuvent s'influencer mutuellement, la suppression des contrôles redondants peut réduire la sécurité globale en place. Les contrôles ne doivent pas être inclus dans le traitement des risques, à moins qu'ils ne soient des contrôles nécessaires pour gérer un ou plusieurs des risques identifiés en matière de sécurité de l'information.
Un contrôle doit avoir un effet sur les conséquences ou la probabilité des risques identifiés en matière de sécurité des informations. Les contrôles ne doivent pas être inclus dans le traitement des risques s'ils fonctionnent pour des raisons non liées à la sécurité de l'information.

Il convient de prêter attention aux contrôles mis en œuvre mais dont on sait qu'ils présentent certaines faiblesses.
Si l'évaluation de tous les risques gérés par un contrôle présentant des faiblesses se situe dans les critères d'acceptation, alors il n'est pas nécessaire d'améliorer le contrôle. Même si le contrôle ne fonctionne pas pleinement, il n'est pas toujours nécessaire de l'améliorer pour le rendre pleinement efficace. Il ne faut pas présumer que tous les contrôles doivent fonctionner avec leur pleine efficacité pour que l'organisation puisse gérer ses risques avec succès.
Il est possible de préciser que chaque contrôle individuel a un niveau de tolérance de défaillance en dessous duquel le contrôle peut être considéré comme ne fonctionnant pas suffisamment efficacement pour gérer les risques identifiés. Tant que le contrôle fonctionne à l'intérieur de la tolérance, il n'a besoin d'aucune amélioration.

8.4 Comparaison des contrôles déterminés avec ceux de la norme ISO/IEC 27001:2022, Annexe A

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 c).

Entrée : Tous les contrôles nécessaires (voir 8.3).

Action : Comparez tous les contrôles nécessaires avec ceux répertoriés dans la norme ISO/IEC 27001:2022, Annexe A.

Déclencheur : l'identification de tout contrôle manquant devient nécessaire si des plans de traitement des risques sont formulés.

Résultat : Tous les contrôles applicables au traitement des risques.

Conseils de mise en œuvre :

L'ISO/IEC 27001:2022, 6.1.3 c), exige qu'un organisme compare les contrôles qu'il a déterminés comme étant nécessaires pour mettre en œuvre les options de traitement des risques qu'il a choisies avec les contrôles répertoriés dans l'ISO/IEC 27001:2022, Annexe A. le but est d'agir comme un contrôle de sécurité pour vérifier qu'aucun contrôle nécessaire n'a été omis dans l'évaluation des risques. Ce contrôle de sécurité n'est pas en place pour identifier les contrôles omis de la norme ISO/IEC 27001:2022, Annexe A, dans l'évaluation des risques. Il s'agit d'un contrôle de sécurité visant à identifier tout contrôle nécessaire manquant, quelle qu'en soit la source, en comparant les contrôles avec d'autres normes et listes de contrôles. Les contrôles omis identifiés lors de cette vérification peuvent être des contrôles spécifiques au secteur ou personnalisés ou issus de la norme ISO/IEC 27001:2022, Annexe A. Les lignes directrices pour déterminer les contrôles en 8.3
doivent être suivies pour déterminer si des contrôles manquants doivent être ajoutés à l'évaluation des risques.

EXEMPLE Il est important qu'un contrôle déjà opérationnel dans l'organisation ne soit pas automatiquement ajouté à l'évaluation des risques sans autre examen.

Il est important de rappeler que cette comparaison des contrôles est effectuée à l'aide de l'évaluation des risques et non à l'aide de la déclaration d'applicabilité. Le principe est d'examiner chaque risque tour à tour et de comparer les contrôles déterminés comme nécessaires pour le risque avec les contrôles de la norme ISO/IEC 27001:2022, Annexe A, pour aider à identifier s'il manque des contrôles nécessaires pour chaque risque.

8.5 Produire une déclaration d'applicabilité

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 d).

Entrée : Tous les contrôles applicables au traitement des risques (voir 8.4).

Action : Produire une déclaration d'applicabilité.

Déclencheur : Documentation de tous les contrôles nécessaires, de leur justification et de leur état de mise en œuvre.

Résultat : Déclaration d'applicabilité.

Conseils de mise en œuvre :

Conformément à la norme ISO/IEC 27001:2022, 6.1.3 d), la déclaration d'applicabilité (SOA) doit contenir au moins :

a) les contrôles nécessaires ;

b) la justification de leur inclusion ;

c) s'ils sont mis en œuvre ou non ;

d) justification des exclusions de contrôles de la norme ISO/IEC 27001:2022, Annexe A.

La SOA peut facilement être produite en examinant l'évaluation des risques pour identifier les contrôles nécessaires et le plan de traitement des risques pour identifier ceux dont la mise en œuvre est prévue. Seuls les contrôles identifiés dans l'évaluation des risques peuvent être inclus dans la SOA. Des contrôles ne peuvent pas être ajoutés à la SOA indépendamment de l'évaluation des risques. Il doit y avoir une cohérence entre les contrôles nécessaires à la mise en œuvre des options de traitement des risques sélectionnées et la SOA. La SOA peut déclarer que la justification de l'inclusion d'un contrôle est la même pour tous les contrôles et qu'ils ont été identifiés dans l'évaluation des risques comme étant nécessaires pour traiter un ou plusieurs risques à un niveau acceptable. Aucune autre justification pour l'inclusion d'un contrôle n'est nécessaire pour aucun des contrôles. Le statut de mise en œuvre de tous les contrôles contenus dans la SOA peut être indiqué comme « mis en œuvre », « partiellement mis en œuvre » ou « non mis en œuvre ». Cela peut être soit individuellement pour chaque contrôle, soit sous la forme d'une déclaration globale.

EXEMPLE La SOA contient la déclaration : « Tous les contrôles ont été implémentés ». Aucune analyse ou information supplémentaire n'est requise pour compléter la SOA.

8.6 Plan de traitement des risques liés à la sécurité de l'information

8.6.1 Formulation du plan de traitement des risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 e).

Entrée : Résultats des évaluations des risques.

Action : Formuler un plan de traitement des risques.

Déclencheur : La nécessité pour l'organisation de traiter les risques.

Résultat : Plan de traitement des risques.

Conseils de mise en œuvre :

Le but de cette activité est de créer un ou plusieurs plans pour traiter des ensembles spécifiques de risques qui figurent sur la liste des risques prioritaires (voir Article 7). Un plan de traitement des risques est un plan visant à modifier le risque de telle sorte qu'il réponde aux critères d'acceptation des risques de l'organisation (voir 6.4.2). Il existe deux interprétations possibles du terme « plan » dans le contexte du traitement des risques. Le premier est un plan de projet, c'est-à-dire un plan pour mettre en œuvre les contrôles nécessaires de l'organisation. Le second est un plan de conception, c'est-à-dire le plan qui non seulement identifie les contrôles nécessaires mais décrit également comment les contrôles interagissent avec leur environnement et entre eux pour modifier les risques. En pratique, les deux peuvent être utilisés.

Une fois les contrôles en place, le plan de projet cesse d'avoir toute valeur autre que celle d'un document historique, alors que le plan de conception reste utile.

Chaque risque nécessitant un traitement doit être traité dans l'un des plans de traitement des risques. Une organisation peut choisir de disposer de plusieurs plans de traitement des risques, qui mettent ensemble en œuvre tous les aspects requis du traitement des risques. Ceux-ci peuvent être organisés en fonction de l'endroit où résident les informations (par exemple, un plan

pour le data center, un autre pour l'informatique mobile, etc.), par actif (par exemple différents plans pour différentes classifications d'actifs) ou par événements (comme ceux utilisés lors de l'évaluation des risques selon la méthode événementielle).

Lors de la création du plan de traitement des risques, les organisations doivent prendre en compte les éléments suivants :

— les priorités en fonction du niveau de risque et de l'urgence du traitement ;

— si différents types de contrôles (préventifs, détectives, correctifs) ou leur composition sont en vigueur;

— s'il est nécessaire d'attendre qu'un contrôle soit réglé avant de commencer à en mettre en œuvre un nouveau sur le même actif ;

— s'il existe un délai entre le moment où le contrôle est mis en œuvre et le moment où il est pleinement efficace et opérationnel.

Pour chaque risque traité, le plan de traitement doit inclure les informations suivantes :

— la justification du choix des options de traitement, y compris les bénéfices attendus ;

— ceux qui sont responsables de l'approbation et de la mise en œuvre du plan ;

— les actions proposées;

— les ressources nécessaires, y compris les imprévus;

— les indicateurs de performance ;

— les contraintes ;

— les rapports et le suivi requis ;

— quand les actions devraient être entreprises et achevées ;

— état de mise en œuvre.

Les actions du plan de traitement des risques doivent être classées par priorité en fonction du niveau de risque et de l'urgence du traitement. Plus le niveau de risque et, dans certains cas, la fréquence de survenance du risque sont élevés, plus le contrôle doit être mis en œuvre rapidement.

Pour chaque risque répertorié dans le plan de traitement des risques, des informations détaillées sur la mise en œuvre doivent être suivies et peuvent inclure, sans toutefois s'y limiter :

— les noms des propriétaires des risques et des personnes responsables de la mise en œuvre ;

— les dates ou délais de mise en œuvre ;

— les activités de contrôle prévues pour tester le résultat de la mise en œuvre ;

— état d'avancement de la mise en œuvre ;

— niveau de coût (investissement, fonctionnement).

8.6.2 Approbation par les propriétaires de risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 f).

Entrée : Plan(s) de traitement des risques.

Action : Approbation du ou des plans de traitement des risques par les propriétaires des risques.

Déclencheur : La nécessité d'approuver un ou plusieurs plans de traitement des risques.

Résultat : Plan(s) de traitement des risques approuvé(s).

Conseils de mise en œuvre :

Le plan de traitement des risques liés à la sécurité de l'information doit être approuvé par les propriétaires des risques une fois formulé. Les propriétaires de risques devraient également décider de l'acceptation des risques résiduels en matière de sécurité de l'information. Cette décision doit être basée sur des critères d'acceptation des risques définis.

Les résultats de l'évaluation des risques, le plan de traitement des risques et les risques restants doivent être compréhensibles pour les propriétaires des risques afin qu'ils puissent s'acquitter correctement de leurs responsabilités.

8.6.3 Acceptation des risques résiduels en matière de sécurité des informations

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 6.1.3 f).

Entrée : Plan(s) de traitement des risques approuvé(s) et critères d'acceptation des risques.

Action : Déterminez si les risques résiduels sont acceptables.

Déclencheur : La nécessité pour l'organisation de décider de conserver les risques résiduels.

Résultat : Risques résiduels acceptés.

Conseils de mise en œuvre :

Afin de déterminer les risques résiduels, les plans de traitement des risques doivent être intégrés à l'évaluation de suivi de la probabilité résiduelle et des conséquences. Les contrôles proposés décrits dans les plans de traitement des risques et leur efficacité associée doivent être examinés en fonction de la question de savoir s'ils réduiront la probabilité ou la conséquence, ou les deux, et si le niveau de risques résiduels est attribué aux risques. Le niveau des risques résiduels est ensuite examiné par le propriétaire du risque pour déterminer si les risques résiduels sont acceptables.

Les plans de traitement des risques doivent décrire la manière dont les risques évalués doivent être traités pour répondre aux critères d'acceptation des risques.

Dans certains cas, le niveau de risque résiduel ne répond pas toujours aux critères d'acceptation du risque, car les critères appliqués ne tiennent pas compte des circonstances du moment.

EXEMPLE On peut affirmer qu'il est nécessaire de conserver les risques parce que les avantages qui les accompagnent constituent une opportunité commerciale importante, ou parce que le coût de la modification des risques est trop élevé.

Cependant, il n'est pas toujours possible de réviser les critères d'acceptation des risques en temps opportun. Dans de tels cas, les propriétaires de risques peuvent conserver les risques qui ne répondent pas aux critères d'acceptation normaux. Si cela est nécessaire, le propriétaire du risque doit formuler des commentaires explicites sur les risques et inclure une justification de la décision de passer outre les critères normaux d'acceptation des risques.

L'acceptation du risque peut impliquer un processus visant à obtenir l'approbation des traitements avant une décision finale d'acceptation du risque. Il est important que les propriétaires de risques examinent et approuvent les plans de traitement des risques proposés et les risques résiduels qui en résultent, et enregistrent toutes les conditions associées à une telle approbation. En fonction du processus d'évaluation des risques et des critères d'acceptation des risques, cela peut nécessiter qu'un gestionnaire doté d'un niveau d'autorité plus élevé que le propriétaire du risque accepte l'acceptation du risque.

La mise en œuvre d'un plan de traitement des risques évalués peut prendre un certain temps. Les critères de risque peuvent permettre aux niveaux de risque de dépasser un seuil souhaité dans une mesure définie s'il existe un plan en place pour réduire ce risque dans un délai acceptable. Les décisions d'acceptation des risques peuvent tenir compte des délais fixés dans les plans de traitement des risques et de la conformité ou non des progrès de la mise en œuvre du traitement des risques avec ce qui est prévu.

Certains risques peuvent varier dans le temps (que cette évolution soit ou non due à la mise en œuvre d'un plan de traitement des risques). Les critères d'acceptation des risques peuvent en tenir compte et avoir des seuils d'acceptation des risques qui dépendent de la durée pendant laquelle une organisation peut être exposée à un risque évalué.

9 Fonctionnement

9.1 Exécution du processus d'évaluation des risques liés à la sécurité de l'information

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 8.2.

Entrée : Documents sur le processus d'évaluation des risques liés à la sécurité de l'information, y compris les critères d'évaluation des risques et d'acceptation des risques.

Action : Le processus d'évaluation des risques doit être effectué conformément à l'article 7.

Déclencheur : besoin de l'organisation d'évaluer les risques, à intervalles planifiés ou en fonction d'événements.

Résultat : Risques évalués.

Conseils de mise en œuvre :

Le processus d'évaluation des risques liés à la sécurité de l'information défini et appliqué dans la norme ISO/IEC 27001:2022, 6.1 doit être intégré aux opérations organisationnelles et doit être effectué à intervalles planifiés ou lorsque des changements importants sont proposés ou se produisent. Le processus d'évaluation des risques liés à la sécurité de l'information doit prendre en compte les critères établis dans la norme ISO/IEC 27001:2022, 6.1.2 a). Les intervalles auxquels l'évaluation des risques est effectuée doivent être adaptés au SMSI. Lorsqu'un changement significatif du SMSI (ou de son contexte) ou un changement dans le paysage des menaces (par exemple un nouveau type d'attaque contre la sécurité des informations) se produit, l'organisation doit déterminer si ce changement nécessite une évaluation supplémentaire des risques en matière de sécurité des informations.

Lorsqu'elles planifient des évaluations de risques de routine, les organisations doivent tenir compte de tout calendrier s'appliquant à leurs processus opérationnels généraux et aux cycles budgétaires associés.

EXEMPLE S'il existe un cycle budgétaire annuel, l'organisation peut être tenue de soumettre des demandes de financement à une certaine période de l'année. Les fonds sont ensuite accordés (diminués ou refusés) plus tard.

Si les processus de passation des marchés sont impliqués, il peut y avoir un autre cycle budgétaire avant que les recommandations en matière de traitement des risques puissent être mises en œuvre et que leur efficacité puisse être évaluée avant la prochaine évaluation des risques de routine. Dans de tels cas, des évaluations des risques doivent être programmées :

a) faire leurs recommandations en matière de traitement des risques à temps pour la demande de financement ;

b) à réévaluer suite aux résultats des allocations budgétaires ;

c) effectuer la prochaine évaluation de routine, une fois les recommandations mises en œuvre, après toute activité de passation de marchés.

9.2 Exécution du processus de traitement des risques liés à la sécurité de l'information

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 8.3.

Entrée : Risque(s) évalué(s).

Action : Le processus de traitement des risques doit être effectué conformément à l'Article 8.

Déclencheur : besoin de l'organisation de traiter les risques, à intervalles planifiés ou en fonction d'événements.

Résultat : Risques résiduels retenus ou acceptés.

Conseils de mise en œuvre :

ISO/IEC 27001:2022, 8.3 spécifie les exigences imposées aux organisations pour mettre en œuvre leurs plans de traitement des risques. Les considérations incluses en 8.6 sont également pertinentes pour ce paragraphe.

10 Tirer parti des processus SMSI associés

10.1 Contexte de l'organisation

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, Article 4.

Entrée : Informations sur l'organisation, son contexte interne et externe.

Action : Toutes les données pertinentes doivent être prises en compte pour identifier et décrire les problèmes internes et externes influençant la gestion des risques liés à la sécurité de l'information et les exigences des parties intéressées.

Déclencheur : ISO/IEC 27001 : 2022 spécifie les exigences relatives à ces informations afin de pouvoir établir des objectifs de sécurité de l'information.

Résultat : Problèmes internes et externes liés aux risques qui influencent la gestion des risques liés à la sécurité de l'information.

Conseils de mise en œuvre :

L'organisation doit avoir une compréhension de haut niveau (par exemple stratégique) des questions importantes qui peuvent affecter le SMSI, que ce soit de manière positive ou négative. Il doit en outre connaître le contexte interne et externe pertinent par rapport à son objectif et qui affecte sa capacité à atteindre le résultat escompté de son SMSI.
Les résultats escomptés devraient garantir la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations en appliquant le processus de gestion des risques et en sachant quels risques sont gérés de manière adéquate.

Pour identifier les risques de manière fiable, l'organisation doit comprendre de manière suffisamment détaillée les circonstances dans lesquelles elle opère. Cela signifie que l'organisation doit recueillir des informations concernant le contexte interne et externe de l'organisation, ses parties intéressées et leurs exigences (voir ISO/IEC 27001:2022, 4.1 et 4.2). La collecte de ces informations doit être effectuée avant toute tentative par l'organisation d'évaluer ses risques en matière de sécurité de l'information, ou même tout autre risque pouvant affecter le résultat attendu du SMSI (voir ISO/IEC 27001:2022, 6.1.1).

L'organisation doit prendre en compte toutes les sources de risques internes et externes. La compréhension qu'a l'organisation des parties intéressées qui s'opposent à l'organisation et à leurs intérêts est très pertinente.

EXEMPLE 1 Un exemple de partie intéressée dont les intérêts sont opposés aux objectifs de l'organisation est l'attaquant. L'attaquant souhaite une organisation avec un niveau de sécurité faible. L'organisation prend en compte l'intérêt de cette partie en ayant le contraire (niveau de sécurité fort), c'est-à-dire qu'elle considère d'éventuels conflits avec les objectifs du SMSI. L'organisation veille, grâce à des contrôles efficaces de sécurité de l'information, à ce que ces intérêts ne soient pas respectés.

Les interfaces avec des services ou des activités qui n'entrent pas entièrement dans le champ d'application du SMSI doivent être prises en compte dans l'évaluation des risques liés à la sécurité des informations de l'organisation.

EXEMPLE 2 Un exemple d'une telle situation est le partage d'actifs (par exemple des installations, des systèmes informatiques et des bases de données) avec d'autres organisations ou l'externalisation d'une fonction commerciale.

La manière dont d'autres facteurs pertinents influençant la sécurité de l'information sont pris en compte dépend du choix de l'organisation en matière de méthodes d'identification et d'analyse des risques.

Les objectifs de sécurité de l'information de l'organisation (voir ISO/IEC 27001:2022, 6.2) peuvent contraindre les critères d'acceptation des risques (par exemple, le niveau de risque acceptable peut être fonction des récompenses potentielles associées aux différentes activités commerciales). En outre, la politique de sécurité de l'information peut limiter le traitement des risques (par exemple, certaines options de traitement des risques peuvent être exclues par cette politique).

10.2 Leadership et engagement

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 5.1.

Entrée : informations sur les résultats de l'évaluation des risques liés à la sécurité de l'information ou les résultats du traitement des risques liés à la sécurité de l'information nécessitant une approbation ou une approbation.

Action : un niveau de direction approprié doit prendre en compte les résultats liés aux risques liés à la sécurité de l'information, afin de décider ou d'approuver d'autres actions.

Déclencheur : ISO/IEC 27001 exige qu'un niveau de direction approprié soit impliqué dans toutes les activités liées aux risques liés à la sécurité de l'information.

Résultat : Décisions ou approbation liées aux risques liés à la sécurité de l'information.

Conseils de mise en œuvre :

La haute direction est responsable de la gestion des risques et doit diriger et piloter les évaluations des risques, notamment :

— s'assurer que les ressources nécessaires sont allouées à la gestion des risques;

— attribuer l'autorité, la responsabilité et l'imputabilité aux niveaux appropriés au sein de l'organisation en ce qui concerne la gestion des risques ;

— communiquer avec les parties intéressées appropriées.

10.3 Communication et consultation

NOTE 1 Ce paragraphe concerne l'ISO/IEC 27001:2022, 7.4.

NOTE 2 L'ISO/IEC 27001 fait directement référence à la partie communication de cette activité.

Entrée : informations sur les risques, leurs causes, leurs conséquences et leur probabilité identifiés grâce aux processus de gestion des risques.

Action : Les informations sur les risques, leurs causes, leurs conséquences, leur probabilité et les contrôles pris pour les traiter doivent être communiquées ou obtenues auprès des parties intéressées externes et internes.

Déclencheur : ISO/IEC 27001 exige une telle communication.

Résultat : perceptions des parties intéressées pertinentes et compréhension continue du processus et des résultats de gestion des risques liés à la sécurité de l'information de l'organisation.

Conseils de mise en œuvre :

L'activité de communication et de consultation vise à parvenir à un accord sur la manière de gérer les risques en échangeant et/ou en partageant des informations sur les risques avec les propriétaires des risques et d'autres parties intéressées concernées. Les informations comprennent, sans toutefois s'y limiter, l'existence, la nature, la forme, la probabilité, la conséquence, l'importance, le traitement et l'acceptation des risques.

ISO/IEC 27001:2022, 6.1.2 c) 2), exige que les propriétaires des risques liés à la sécurité des informations soient identifiés.
La propriété du risque peut être délibérément confondue ou dissimulée. Même lorsque les propriétaires des risques peuvent être identifiés, ils peuvent être réticents à reconnaître qu'ils sont responsables des risques qu'ils possèdent, et il peut être difficile d'obtenir leur participation au processus de gestion des risques. Il devrait y avoir une procédure de communication définie pour informer les personnes concernées sur la propriété des risques.

ISO/IEC 27001:2022, 6.1.3 f), exige que les propriétaires de risques approuvent le(s) plan(s) de traitement des risques et décident de l'acceptation des risques résiduels. La communication entre les propriétaires de risques et le personnel responsable de la mise en œuvre du SMSI est une activité importante. Il devrait y avoir un accord sur la manière de gérer les risques en échangeant et/ou en partageant des informations sur les risques avec les propriétaires des risques et peut-être avec d'autres parties intéressées et décideurs. Les informations comprennent, sans toutefois s'y limiter, l'existence, la nature, la forme, la probabilité, l'importance, le traitement et l'acceptation des risques. La communication doit être bidirectionnelle.

En fonction de la nature et de la sensibilité du ou des risques, il peut s'avérer nécessaire de limiter certaines informations sur les risques, leur évaluation et leur traitement, sur la base du besoin d'en connaître, aux personnes responsables de leur identification, de leur évaluation et de leur traitement. La communication sur les risques doit être contrôlée sur la base du « besoin de savoir », en tenant compte du niveau de détail requis par les différentes parties intéressées, en consultation avec les propriétaires de risques ou les propriétaires potentiels, dans le but d'éviter de rendre publics les risques les plus sensibles et leurs associés. faiblesses connues.

Les perceptions du risque peuvent varier en raison des différences dans les hypothèses, les concepts, les besoins, les problèmes et les préoccupations des parties intéressées concernées en ce qui concerne le risque ou les questions en discussion. Les parties intéressées sont susceptibles de porter des jugements sur l'acceptation du risque, en fonction de leur perception du risque.
Ceci est particulièrement important pour garantir que les perceptions des risques par les parties intéressées, ainsi que leurs perceptions des avantages, puissent être identifiées et documentées et que les raisons sous-jacentes soient clairement comprises et traitées.

La communication et la consultation concernant les risques peuvent aboutir à un meilleur engagement des parties intéressées dans ce qui est fait et à une appropriation par les parties intéressées appropriées des décisions et des résultats. La communication et la consultation des parties intéressées, à mesure que les critères sont élaborés et que les méthodes d'évaluation des risques sont sélectionnées, peuvent également améliorer l'appropriation des résultats par les parties intéressées. Les parties intéressées sont moins susceptibles de remettre en question les résultats des processus qu'elles ont contribué à concevoir. En conséquence, la probabilité qu'ils acceptent les conclusions et soutiennent les plans d'action est souvent accrue. Dans les cas où les parties intéressées sont des gestionnaires, cela peut renforcer l'engagement à atteindre les objectifs de gestion des risques et à fournir les ressources nécessaires.

La communication sur les risques doit être effectuée afin de :

— fournir une assurance sur les résultats de la gestion des risques de l'organisation;

— collecter des informations sur les risques ;

— partager les résultats de l'évaluation des risques et présenter le plan de traitement des risques;

— éviter ou réduire à la fois l'apparition et les conséquences de violations de la sécurité des informations dues au manque de compréhension mutuelle entre les propriétaires de risques et les parties intéressées;

— soutenir les propriétaires de risques;

— acquérir de nouvelles connaissances en matière de sécurité de l'information;

— se coordonner avec les autres parties et planifier les réponses pour réduire les conséquences de tout incident ;

— responsabiliser les propriétaires de risques et les autres parties ayant un intérêt légitime à risque ;

— améliorer la sensibilisation.

Une organisation doit élaborer des plans de communication des risques pour les opérations normales ainsi que pour les urgences. Les activités de communication et de consultation sur les risques doivent être menées en permanence.

La coordination entre les principaux propriétaires de risques et les parties intéressées concernées peut être réalisée par la formation d'un comité où un débat sur les risques, leur hiérarchisation, leur traitement approprié et leur acceptation peut avoir lieu.

Les communications sur les risques peuvent être volontairement transmises à des tiers externes pour permettre une meilleure gestion des risques ou une meilleure coordination ou sensibilisation des réponses et peuvent également être exigées par les régulateurs ou les partenaires commerciaux dans certaines circonstances.

Il est important de coopérer avec l'unité de relations publiques ou de communication appropriée au sein de l'organisation pour coordonner toutes les tâches liées à la communication sur les risques. Ceci est crucial en cas d'activation de la communication de crise, par exemple en réponse à des incidents particuliers.

10.4 Informations documentées

10.4.1 Général

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 7.5.

L'ISO/IEC 27001 spécifie les exigences imposées aux organismes pour qu'ils conservent des informations documentées concernant le processus d'évaluation des risques (voir ISO/IEC 27001:2022, 6.1.2) et les résultats (voir ISO/IEC 27001:2022, 8.2) ; le processus de traitement des risques (ISO/IEC 27001:2022, 6.1.3) et les résultats (ISO/IEC 27001:2022, 8.3).

10.4.2 Informations documentées sur les processus

Entrée : Connaissance des processus d'évaluation et de traitement des risques en matière de sécurité de l'information conformément aux articles 7 et 8, définis par l'organisation.

Action : Les informations sur les processus d'évaluation et de traitement des risques liés à la sécurité de l'information doivent être documentées et conservées.

Déclencheur : ISO/IEC 27001 exige des informations documentées sur les processus d'évaluation et de traitement des risques liés à la sécurité de l'information.

Résultat : informations documentées requises par les parties intéressées (par exemple, un organisme de certification) ou déterminées par l'organisation comme étant nécessaires à l'efficacité du processus d'évaluation des risques de sécurité de l'information ou du processus de traitement des risques de sécurité de l'information.

Conseils de mise en œuvre :

Les informations documentées sur le processus d'évaluation des risques liés à la sécurité de l'information doivent contenir :

a) une définition des critères de risque (y compris les critères d'acceptation des risques et les critères de réalisation)
évaluations des risques liés à la sécurité de l'information);

b) raisonner pour la cohérence, la validité et la comparabilité des résultats ;

c) une description de la méthode d'identification des risques (y compris l'identification des propriétaires des risques) ;

d) une description de la méthode d'analyse des risques liés à la sécurité de l'information (y compris l'évaluation des conséquences potentielles, de la probabilité réaliste et du niveau de risque qui en résulte) ;

e) une description de la méthode de comparaison des résultats avec les critères de risque et la priorisation des risques pour le traitement des risques.

Les informations documentées sur le processus de traitement des risques liés à la sécurité de l'information doivent contenir des descriptions de :

— la méthode de sélection des options appropriées de traitement des risques liés à la sécurité de l'information ;

— la méthode permettant de déterminer les contrôles nécessaires ;

— comment l'ISO/IEC 27001:2022, Annexe A, est utilisée pour déterminer que les contrôles nécessaires n'ont pas été négligé par inadvertance ;

— comment sont élaborés les plans de traitement des risques ;

— comment est obtenue l'approbation des propriétaires de risques.

10.4.3 Informations documentées sur les résultats

Entrée : l'évaluation des risques liés à la sécurité de l'information et les résultats du traitement.

Action : Les informations sur l'évaluation des risques liés à la sécurité des informations et les résultats du traitement doivent être documentés et conservés.

~~Déclencheur~~ : ISO/IEC 27001 exige des informations documentées sur le risque de sécurité des informations résultats de l'évaluation et du traitement.

~~Résultat :~~ Informations documentées sur l'évaluation des risques liés à la sécurité de l'information et les résultats du traitement.

~~Conseils de mise en œuvre :~~

Étant donné que les organisations sont tenues d'effectuer des évaluations des risques à intervalles planifiés ou lorsque des changements importants sont proposés ou se produisent, il devrait au moins y avoir la preuve d'un calendrier et d'évaluations des risques effectuées conformément à ce calendrier. Si un changement est proposé ou s'est produit, il doit alors y avoir des preuves de la réalisation d'une évaluation des risques associée. Sinon, l'organisation doit expliquer pourquoi le changement est important ou non.

Les informations documentées sur les résultats de l'évaluation des risques liés à la sécurité de l'information doivent contenir :

a) les risques identifiés, leurs conséquences et leur probabilité ;

b) l'identité du ou des propriétaires du risque ;

c) les résultats de l'application des critères d'acceptation des risques ;

d) la priorité du traitement des risques.

Il est également recommandé d'enregistrer la justification des décisions en matière de risques, afin à la fois de tirer les leçons des erreurs commises dans des cas individuels et de faciliter l'amélioration continue.

Les informations documentées sur les résultats du traitement des risques liés à la sécurité de l'information doivent contenir :

— identification des contrôles nécessaires;

— le cas échéant et disponible, la preuve que ces contrôles nécessaires agissent pour modifier les risques, de manière à répondre aux critères d'acceptation des risques de l'organisation.

10.5 Surveillance et examen

10.5.1 Général

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 9.1.

Le processus de surveillance de l'organisme (voir ISO/IEC 27001:2022, 9.1) doit englober tous les aspects des processus d'évaluation et de traitement des risques aux fins de :

a) garantir que les traitements des risques sont efficaces, efficients et économiques, tant dans leur conception que dans leur conception. opération;

b) obtenir des informations pour améliorer les futures évaluations des risques ;

c) analyser et tirer les leçons des incidents (y compris les quasi-accidents), des changements, des tendances et des succès et les échecs ;

d) détecter les changements dans le contexte interne et externe, y compris les changements dans les critères de risque et les les risques eux-mêmes, ce qui peut nécessiter une révision des traitements et des priorités en matière de risques ;

e) identifier les risques émergents.

Les scénarios de risques retenus, issus des activités de gestion des risques, peuvent être transposés en scénarios de surveillance afin d'assurer un processus de surveillance efficace. De plus amples détails sur les scénarios de surveillance sont donnés en A.2.7.

10.5.2Surveillance et examen des facteurs influençant les risques

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 9.1.

Entrée : Toutes les informations sur les risques obtenues à partir des activités de gestion des risques.

Action : Les risques et leurs facteurs (c'est-à-dire la valeur des actifs, les conséquences, les menaces, les vulnérabilités, la probabilité d'occurrence) doivent être surveillés et examinés pour identifier tout changement dans le contexte de l'organisation à un stade précoce et pour maintenir une vue d'ensemble de l'ensemble. image du risque.

Déclencheur : examen de la politique organisationnelle et toute détection de changements dans l'environnement opérationnel ou de menace actuel.

Résultat : Alignement continu de la gestion des risques avec les objectifs commerciaux de l'organisation et avec les critères d'acceptation des risques.

Conseils de mise en œuvre :

La norme ISO/IEC 27001:2022, 9.1 exige que les organisations évaluent leurs performances en matière de sécurité de l'information (et l'efficacité du SMSI). Conformément à cette exigence, les organisations doivent utiliser leur(s) plan(s) de traitement des risques comme sujet de leurs évaluations de performance. Pour ce faire, une organisation doit d'abord définir un ou plusieurs besoins d'information, par exemple pour décrire ce que la direction souhaite savoir sur la capacité de l'organisation à se défendre contre les menaces. En utilisant cela comme spécification de niveau supérieur, une organisation doit ensuite déterminer les mesures qu'elle doit effectuer et comment ces mesures doivent être combinées afin de satisfaire le besoin d'informations.

Les risques ne sont pas statiques. Les scénarios d'événements, les valeurs des actifs, les menaces, les vulnérabilités, les probabilités et les conséquences peuvent changer brusquement sans aucune indication. Une surveillance constante doit être effectuée pour détecter ces changements. Cela peut être pris en charge par des services externes qui fournissent des informations sur les nouvelles menaces ou vulnérabilités. Les organisations doivent assurer la surveillance continue des facteurs pertinents, tels que :

a) de nouvelles sources de risque, y compris des vulnérabilités informatiques récemment signalées ;

b) les nouveaux actifs qui ont été inclus dans le périmètre de gestion des risques ;

c) modification nécessaire de la valeur des actifs (par exemple en raison de changements dans les exigences commerciales) ;

d) identifié les vulnérabilités afin de déterminer celles qui sont exposées à des menaces nouvelles ou réémergentes ;

e) les changements dans les modes d'utilisation des technologies existantes ou nouvelles qui peuvent ouvrir de nouvelles possibilités opportunités d'attaque;

f) les changements dans les lois et réglementations ;

g) les changements dans l'appétit pour le risque et les perceptions de ce qui est désormais acceptable et de ce qui ne l'est plus ;

h) incidents de sécurité de l'information, tant à l'intérieur qu'à l'extérieur de l'organisation.

De nouvelles sources de risque ou des changements dans la probabilité ou les conséquences peuvent accroître les risques précédemment évalués. L'examen des risques faibles et retenus doit examiner chaque risque séparément, ainsi que tous ces risques dans leur ensemble, afin d'évaluer leurs conséquences potentielles accumulées. Si les risques ne rentrent plus dans la catégorie de risque faible ou acceptable, ils doivent être traités en utilisant une ou plusieurs des options de 8.2.

Les facteurs qui affectent la probabilité de survenance d'événements et leurs conséquences correspondantes peuvent changer, tout comme les facteurs qui affectent l'adéquation ou le coût des différentes options de traitement. Les changements majeurs affectant l'organisation devraient justifier une révision plus spécifique. Les activités de surveillance des risques doivent être régulièrement répétées et les options sélectionnées pour le traitement des risques doivent être revues périodiquement.

De nouvelles menaces, vulnérabilités ou changements de probabilité ou de conséquences peuvent accroître les risques précédemment évalués comme faibles. L'examen des risques faibles et retenus doit considérer chaque risque séparément, ainsi que tous ces risques dans leur ensemble, afin d'évaluer leurs conséquences cumulées potentielles. Si les risques n'entrent pas dans la catégorie de risque faible ou acceptable, ils doivent être traités en utilisant une ou plusieurs des options envisagées à l' Article 8.

Les facteurs qui affectent la probabilité d'apparition des menaces et leurs conséquences correspondantes peuvent changer, tout comme les facteurs qui affectent l'adéquation ou le coût des différentes options de traitement. Les changements majeurs affectant l'organisation devraient justifier une révision plus spécifique. Les activités de surveillance des risques doivent être régulièrement répétées et les options sélectionnées pour le traitement des risques doivent être revues périodiquement.

Le résultat des activités de surveillance des risques peut être intégré à d'autres activités d'examen des risques. L'organisation doit examiner tous les risques régulièrement et lorsque des changements majeurs sont proposés ou surviennent conformément à la norme ISO/IEC 27001:2022, Article 8.

10.6 Revue de direction

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 9.3.

Entrée : Résultats de la ou des évaluation(s) des risques liés à la sécurité de l'information, état du plan de traitement des risques liés à la sécurité de l'information.

Action : Les résultats de l'évaluation des risques liés à la sécurité de l'information et l'état du plan de traitement des risques liés à la sécurité de l'information doivent être examinés pour confirmer que les risques résiduels répondent aux critères d'acceptation des risques et que le plan de traitement des risques aborde tous les risques pertinents et leurs options de traitement des risques.

Déclencheur : une partie du calendrier planifié des activités de révision.

Résultat : Modifications des critères d'acceptation des risques et des critères d'exécution de l'information
évaluations des risques de sécurité, plan de traitement des risques de sécurité de l'information ou SOA mis à jour.

10.7 Action corrective

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 10.1.

Entrée : Le plan de traitement des risques s'avère inefficace, ce qui signifie que le risque résiduel restera à des niveaux inacceptables une fois le plan de traitement terminé.

Action : Réviser le plan de traitement des risques et le mettre en œuvre pour modifier le risque résiduel à un niveau acceptable.

Déclencheur : La décision de réviser le plan de traitement des risques.

Résultat : Un plan révisé de traitement des risques et sa mise en œuvre.

Conseils de mise en œuvre :

Les non-conformités liées à l'efficacité du plan de traitement des risques peuvent être relevées par un audit interne ou externe, ou par le biais d'un suivi et d'indicateurs. Le plan de traitement doit être révisé pour refléter :

— les résultats du processus de traitement des risques liés à la sécurité de l'information ;

— mise en œuvre progressive du plan (par exemple, un contrôle est mis en œuvre tel que spécifié, tel que conçu, tel que construit);

— difficultés identifiées dans la mise en œuvre des contrôles (par exemple, problèmes techniques ou financiers, incohérences avec des facteurs internes ou externes tels que des considérations de confidentialité).

Il existe également des cas où même si les risques résiduels sont acceptables une fois le plan de traitement terminé, les utilisateurs rejetteront son utilisation, ou tenteront de les contourner parce que ces contrôles ne sont pas acceptés par les utilisateurs en termes de facilité d'utilisation (par exemple, non ergonomiques, trop compliqué ou trop long).

L'organisation doit examiner l'efficacité du plan de traitement révisé.

10.8 Amélioration continue

NOTE Ce paragraphe concerne l'ISO/IEC 27001:2022, 10.2

Entrée : Toutes les informations sur les risques obtenues à partir des activités de gestion des risques.

Action : Le processus de gestion des risques liés à la sécurité de l'information doit être continuellement surveillé, examiné et amélioré si nécessaire.

Déclencheur : l'organisation cherche à s'améliorer et à mûrir à partir des leçons apprises au cours du processus de gestion des risques liés à la sécurité de l'information.

Résultat : Pertinence continue du processus de gestion des risques liés à la sécurité de l'information par rapport aux objectifs commerciaux de l'organisation ou mise à jour du processus.

Conseils de mise en œuvre :

Une surveillance et un examen continus visant à garantir que le contexte, les résultats de l'évaluation et du traitement des risques, ainsi que les plans de gestion, restent pertinents et adaptés aux circonstances sont nécessaires pour garantir que le processus de gestion des risques liés à la sécurité de l'information est correct.

L'organisation doit s'assurer que le processus de gestion des risques liés à la sécurité de l'information et les activités associées restent appropriés dans les circonstances actuelles et sont suivis. Toute amélioration convenue du processus, ou toute action nécessaire pour améliorer le respect du processus, doit être notifiée aux responsables. Ces gestionnaires doivent avoir l'assurance qu'aucun risque ou élément de risque n'est négligé ou sous-estimé et que les actions et décisions nécessaires sont prises pour fournir une compréhension réaliste des risques et une capacité à y répondre.

Il convient de noter que le processus de gestion du changement doit continuellement fournir un retour d'information au processus de gestion des risques afin de garantir que les variations des systèmes d'information capables de modifier les risques soient rapidement prises en compte, voire en modifiant les activités d'évaluation des risques pour les évaluer correctement.

De plus, l'organisation doit vérifier régulièrement les critères utilisés pour mesurer le risque. Cette vérification doit garantir que tous les éléments sont toujours valides et conformes aux objectifs, stratégies et politiques de l'entreprise, et que les changements du contexte commercial sont pris en compte de manière adéquate au cours du processus de gestion des risques liés à la sécurité de l'information. Cette activité de surveillance et d'examen devrait porter sur (sans toutefois s'y limiter) :

— le contexte juridique et environnemental;

— contexte de concurrence;

— approche d'évaluation des risques;

— valeur et catégories des actifs ;

— critères de conséquences ;

— critères de vraisemblance;

— les critères d'évaluation des risques;

— les critères d'acceptation des risques;

- coût total de possession;

— les ressources nécessaires.

L'organisation doit s'assurer que des ressources d'évaluation et de traitement des risques sont continuellement disponibles pour examiner les risques, faire face aux menaces ou vulnérabilités nouvelles ou modifiées et conseiller la direction en conséquence.

Le suivi de la gestion des risques peut conduire à modifier ou compléter l'approche, la méthodologie ou les outils utilisés en fonction :

— la maturité des risques de l'organisation;

— les changements identifiés;

— itération de l'évaluation des risques ;

— l'objectif du processus de gestion des risques liés à la sécurité de l'information (par exemple continuité des activités, résilience aux incidents, conformité) ;

— l'objet du processus de gestion des risques liés à la sécurité de l'information (par exemple, organisation, unité commerciale, processus d'information, sa mise en œuvre technique, son application, sa connexion à Internet).

Les cycles de gestion des risques liés au périmètre d'évaluation des risques et au traitement des risques sont présentés en 5.2.

Annexe A
(informatif)

Exemples de techniques à l'appui du processus d'évaluation des risques

A.1 Critères de risque pour la sécurité des informations

A.1.1 Critères liés à l'évaluation des risques

A.1.1.1 Considérations générales sur l'évaluation des risques

En général, l'incertitude personnelle domine l'évaluation des risques liés à l'information, et différents analystes présentent des tendances différentes à l'incertitude lorsqu'ils interprètent les points sur les échelles de probabilité et de conséquences. Les échelles de référence doivent relier les catégories de conséquences, de probabilité et de risque à des valeurs objectives communes spécifiées sans ambiguïté, éventuellement exprimées en termes tels que la perte financière en unités monétaires et la fréquence notionnelle d'occurrence sur une période finie, spécifiques à l'approche quantitative.

En particulier lorsque l'approche qualitative est adoptée, les analystes des risques doivent suivre une formation et s'entraîner périodiquement par rapport à une échelle de référence d'ancrage pour maintenir l'étalonnage de leur jugement.

A.1.1.2 Approche qualitative

A.1.1.2.1 Échelle des conséquences

~~Le tableau~~ A.1 présente un exemple d'échelle de conséquences.

Tableau A.1 — Exemple d'échelle de conséquences

Conséquences	Description
5 – Catastrophique	Conséquences sectorielles ou réglementaires au-delà de l'organisation Écosystème(s) sectoriel(s) considérablement impacté(s), avec des conséquences qui peuvent être durables. Et/ou : difficulté pour l'Etat, voire incapacité, à assurer une fonction de régulation ou une de ses missions d'importance vitale. Et/ou : conséquences critiques sur la sécurité des personnes et des biens (crise sanitaire, pollution environnementale importante, destruction d'infrastructures essentielles, etc.).
4 – Critique	Des conséquences désastreuses pour l'organisation Incapacité pour l'organisme d'assurer tout ou partie de son activité, avec possibles conséquences graves sur la sécurité des personnes et des biens. L'organisation ne parviendra probablement pas à surmonter la situation (sa survie est menacée), les secteurs d'activité ou les secteurs étatiques dans lesquels elle opère seront probablement légèrement touchés, sans conséquences durables.
3 – Sérieux	Des conséquences importantes pour l'organisation Forte dégradation de l'exercice de l'activité, avec de possibles conséquences importantes sur la sécurité des personnes et des biens. L'organisation surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé), sans aucun impact sectoriel ou étatique.
2 – Important	Des conséquences importantes mais limitées pour l'organisation Dégradation de l'exercice de l'activité sans conséquence sur la sécurité des personnes et des biens. L'organisation saura surmonter la situation malgré quelques difficultés (fonctionnement en mode dégradé).

Tableau A.1 (suite)

Conséquences	Description
1 – Mineur	Des conséquences négligeables pour l'organisation Aucune conséquence sur l'exploitation ou l'exercice de l'activité ni sur la sécurité des personnes et des biens. L'organisation surmontera la situation sans trop de difficultés (les marges seront consommées).

A.1.1.2.2 Échelle de vraisemblance

Le Tableau A.2 et le Tableau A.4 présentent des exemples de façons alternatives de représenter les échelles de vraisemblance. La vraisemblance peut être exprimée soit en termes probabilistes comme dans le tableau A.2 , soit en termes fréquentistes comme dans le tableau A.4. La représentation probabiliste indique la probabilité moyenne qu'un événement à risque se produise au cours d'une période spécifiée, tandis que la représentation fréquentiste indique le nombre de fois où l'événement à risque devrait se produire en moyenne au cours d'une période spécifiée. Comme les deux approches expriment simplement la même chose sous deux perspectives différentes, l'une ou l'autre représentation peut être utilisée, en fonction de celle que l'organisation juge la plus appropriée pour une catégorie de risques donnée.

Toutefois, si les deux approches sont utilisées comme alternatives au sein de la même organisation, il est important que chaque rang théoriquement équivalent sur les deux échelles représente la même probabilité réelle. Autrement, les résultats de l'évaluation dépendent de l'échelle utilisée plutôt que de la probabilité réelle que la source de risque soit évaluée. Si les deux approches sont utilisées, le niveau probabiliste de chaque rang notionnel doit être calculé mathématiquement à partir de la valeur fréquentiste du rang équivalent ou vice versa selon l'approche utilisée pour définir l'échelle primaire.

Si l'une ou l'autre des deux approches est utilisée seule, il n'est pas nécessaire que les incréments de l'échelle soient définis avec autant de précision, car la priorisation des probabilités peut toujours être obtenue quelles que soient les valeurs absolues utilisées. Bien que le tableau A.2 et le tableau A.4 utilisent des incréments et des plages de probabilité complètement différents, selon le contexte de l'organisation et la catégorie de risque évalué, l'un ou l'autre peut être tout aussi efficace pour l'analyse s'il est utilisé exclusivement. Ils ne seraient cependant pas utilisables en toute sécurité comme alternatives dans le même contexte, car les valeurs attachées à des classements équivalents ne sont pas corrélées.

Les catégories et valeurs utilisées dans les tableaux A.2 et A.4 ne sont que des exemples. La valeur la plus appropriée à attribuer à chaque niveau de probabilité dépend du profil de risque et de l'appétit pour le risque de l'organisation.

Tableau A.2 — Exemple d'échelle de vraisemblance

Probabilité	Description
5 – Presque certain	La source de risque atteindra très certainement son objectif en utilisant l'une des méthodes d'attaque envisagées. La probabilité du scénario de risque est très élevée.
4 – Très probable	La source de risque atteindra probablement son objectif en utilisant l'une des méthodes d'attaque envisagées. La probabilité du scénario de risque est élevée.
3 – Probable	La source de risque est capable d'atteindre son objectif en utilisant l'une des méthodes d'attaque envisagées. La probabilité du scénario de risque est importante.
2 – Plutôt improbable	La source de risque a relativement peu de chances d'atteindre son objectif en utilisant l'une des méthodes d'attaque envisagées. La probabilité du scénario de risque est faible.
1 – Peu probable	La source de risque a très peu de chances d'atteindre son objectif en utilisant l'une des méthodes d'attaque envisagées. La probabilité du scénario de risque est très faible.

Des étiquettes verbales telles que « faible », « moyen » et « élevé » peuvent être attachées aux classements lors de l'utilisation de l'une ou l'autre approche d'évaluation de la probabilité. Ceux-ci peuvent être utiles lorsque l'on discute des niveaux de probabilité avec

parties intéressées qui ne sont pas des spécialistes des risques. Cependant, ils sont subjectifs et donc inévitablement ambigus. Par conséquent, ils ne doivent pas être utilisés comme descripteurs principaux lors de la réalisation ou du rapport d'évaluations.

A.1.1.2.3 Niveau de risque

L'utilité des échelles qualitatives et la cohérence des évaluations des risques qui en découlent dépendent entièrement de la cohérence avec laquelle les étiquettes des catégories sont interprétées par toutes les parties intéressées.
Les niveaux de toute échelle qualitative doivent être sans ambiguïté, ses incréments doivent être clairement définis, les descriptions qualitatives de chaque niveau doivent être exprimées dans un langage objectif et les catégories ne doivent pas se chevaucher.

Par conséquent, lorsque vous utilisez des descripteurs verbaux de probabilité, de conséquence ou de risque, ceux-ci doivent être formellement référencés à des échelles sans ambiguïté ancrées à des points de référence numériques (comme dans le tableau A.4) ou ratiométriques (comme dans le tableau A.2) . Toutes les parties intéressées doivent être informées des échelles de référence afin de garantir la cohérence de l'interprétation des données et des résultats de l'évaluation qualitative.

Le tableau A.3 présente un exemple d'approche qualitative.

Tableau A.3 — Exemple d'approche qualitative des critères de risque

Probabilité	Conséquence				
	Catastrophique	Critique	Grave	Important	Mineur
Presque certain	Très élevé	Très élevé	Haut	Haut	Moyen
Très probable	Très haut	Haut	Haut	Moyen	Faible
Probable	Haut	Haut	Moyen	Faible	Faible
Plutôt improbable	Moyen	Moyen	Faible	Faible	Très lent
Peu probable	Faible	Faible	Faible	Très faible	Très faible

La conception d'une matrice qualitative des risques doit être guidée par les critères d'acceptation des risques de l'organisation (voir 6.4.2 et A.1.2).

EXEMPLE Une organisation est parfois plus préoccupée par les conséquences extrêmes, même si leur survenance est peu probable, ou se préoccupe principalement des événements à haute fréquence ayant des conséquences moindres.

Lors de la conception d'une matrice de risques, qu'elle soit qualitative ou quantitative, le profil de risque d'une organisation est normalement asymétrique. Les événements insignifiants sont généralement les plus fréquents et leur fréquence diminue généralement à mesure que les conséquences augmentent, aboutissant à une très faible probabilité de conséquences extrêmes. Il est également rare que le risque commercial représenté par un événement à forte probabilité et à conséquences faibles soit équivalent à celui représenté par un événement à faible probabilité et à conséquences élevées. Même si une matrice de risque symétrique par rapport à sa diagonale faible/faible à élevé/élevé peut sembler facile à créer et naïvement acceptable, il est peu probable qu'elle représente avec précision le profil de risque réel d'une organisation et peut donc produire des résultats invalides. Pour garantir qu'une matrice de risques est réaliste et peut répondre à l'exigence d'amélioration continue (voir ISO/IEC 27001:2022, 10.2), le raisonnement à la fois pour attribuer chaque catégorie aux échelles de probabilité et de conséquence et à la matrice de risque, et concernant la manière dont les catégories correspondent au profil de risque de l'organisation, doivent être documentées lorsque les échelles et la matrice sont définies ou modifiées. Au minimum, les incertitudes inhérentes à l'utilisation de matrices à échelle incrémentielle doivent être décrites avec les précautions nécessaires à l'intention de leurs utilisateurs.

L'utilité des échelles qualitatives et la cohérence des évaluations des risques qui en découlent dépendent entièrement de la cohérence avec laquelle les étiquettes de catégorie sont interprétées par toutes les parties intéressées.
Les niveaux de toute échelle qualitative doivent être sans ambiguïté, ses incréments doivent être clairement définis, les descriptions qualitatives de chaque niveau doivent être exprimées dans un langage objectif et les catégories ne doivent pas se chevaucher.

A.1.1.3 Approche quantitative

A.1.1.3.1 Échelles finies

Le niveau de risque peut être calculé à l'aide de n'importe quelle méthode et en tenant compte de tous les facteurs pertinents, mais il est généralement indiqué en multipliant la probabilité par la conséquence.

La probabilité représente la probabilité ou la fréquence d'un événement se produisant dans un laps de temps donné.
Ce délai est généralement annuel (par an), mais peut être aussi grand (par exemple par siècle) ou aussi court (par exemple par seconde) que l'organisation le souhaite.

Les échelles de vraisemblance doivent être définies en termes pratiques qui reflètent le contexte de l'organisation, afin de l'aider à gérer les risques et d'être faciles à comprendre pour toutes les parties intéressées. Cela signifie principalement fixer des limites réalistes à l'éventail des probabilités représentées. Si les limites maximales et minimales de l'échelle sont trop éloignées, chaque catégorie de celle-ci comprend un éventail de probabilités trop large, ce qui rend l'évaluation incertaine.

EXEMPLE 1 Le point de probabilité finie le plus élevé sur l'échelle peut être utilement défini en termes de temps qu'il faut généralement à l'organisation pour répondre aux événements, et le point fini le plus bas en termes de durée de la planification stratégique à long terme de l'organisation.

Les probabilités supérieures et inférieures aux limites définies de l'échelle peuvent être utilement exprimées comme « supérieures au maximum de l'échelle » et « inférieures au minimum de l'échelle », indiquant ainsi clairement que les probabilités au-delà des limites de l'échelle définie sont des cas extrêmes à considérer exceptionnellement (éventuellement en utilisant des critères spéciaux « hors limites »). En dehors de ces limites, la vraisemblance spécifique est moins importante que le fait qu'il s'agisse d'une exception dans la direction donnée.

Habituellement, il est utile de mesurer les conséquences à l'aide d'un chiffre financier, car cela permet l'agrégation pour le reporting des risques.

EXEMPLE 2 Les échelles de conséquences monétaires sont généralement basées sur des facteurs de 10 (100 à 1 000 ; 1 000 à 10 000, etc.).

Les largeurs des catégories d'une échelle de probabilité doivent être sélectionnées en référence à celles de l'échelle de conséquences choisie pour éviter qu'un éventail excessif de risques ne tombe dans chaque catégorie.

EXEMPLE 3 Si la probabilité et les conséquences sont représentées par les indices d'une échelle exponentielle (c'est-à-dire les logarithmes des valeurs sur l'échelle), il convient de les additionner.

La valeur du risque peut alors être calculée comme suit : antilog [log (valeur de vraisemblance) + log (valeur de conséquence)].

Tableau A.4 — Exemple d'échelle de vraisemblance logarithmique

Fréquence moyenne approximative	Expression du journal	Valeur d'échelle
Toutes les heures	(environ 105) (environ 104)	5
Toutes les 8 heures	(environ 103) (environ 103)	4
Deux fois par semaine	(101) (100)	3
Une fois par mois		2
Une fois par an		1
Une fois par décennie		0

EXEMPLE 4 Dans le Tableau A.4, un exemple d'événement à haute fréquence est une attaque par mot de passe d'événement assistée par ordinateur ou une attaque par déni de service distribué provenant d'un botnet. En effet, les fréquences d'attaque peuvent être bien plus élevées.

EXEMPLE 5 Dans le Tableau A.4, les éruptions volcaniques sont un exemple d'événement de basse fréquence. Même si l'on prévoit qu'un événement ne se produira qu'une fois par siècle, cela ne signifie pas qu'il ne se produira pas pendant la durée de vie d'un SMSI.

Le Tableau A.5 montre un exemple d'échelle de conséquences logarithmique. L'un des objectifs de la prise en compte de la fréquence est de garantir que les mesures de protection sont suffisamment solides pour résister aux séquences d'attaques à haute fréquence, même lorsque la probabilité d'une telle séquence d'attaques est faible.

Tableau A.5 — Exemple d'échelle de conséquences logarithmique

Conséquence (une perte de)	Expression du journal	Valeur d'échelle
1 000 000 £	(106)	6
100 000 £	(105)	5
10 000 £	(104)	4
1 000 £	(103)	3
100 £	(102)	2
Moins de 100 £	(101)	1

Si les échelles de probabilité et de conséquence utilisent une base logarithmique 10 pour attribuer un niveau, les analystes des risques peuvent se retrouver avec trop de risques au même niveau de risque et être incapables de prendre une décision appropriée en matière de priorisation ou d'investissement en sécurité. Dans ce cas, il peut être utile de réduire la base et d'augmenter le nombre de niveaux considérés. Il convient de noter que si différentes bases de probabilité et de conséquences sont choisies, une formule utile pour résumer deux facteurs ne peut pas être appliquée.

EXEMPLE 6 Si la probabilité est doublée en passant d'un niveau au suivant, alors que la conséquence est un facteur 10 plus chère, la formule donnera les risques a) et b), où le risque b) a un niveau de conséquence de 10 fois plus cher que le risque a) mais seulement la moitié de la probabilité que le risque a) se retrouve au même niveau de risque. C'est économiquement incorrect.

Les tableaux A.4 et A.5 répertorient les fourchettes de probabilité et de conséquences qui couvrent la plupart des éventualités dans des organisations très différentes. Aucune organisation n'est susceptible d'être confrontée à elle seule à l'éventail de risques représenté par l'ensemble de ces exemples d'échelles. Le contexte de l'organisation et le champ d'application du SMSI devraient être utilisés pour définir des limites supérieures et inférieures réalistes tant pour les probabilités que pour les conséquences, en gardant à l'esprit que quantifier des fourchettes de risque supérieures à 1 000 pour 1 est susceptible d'avoir une valeur pratique limitée. .

A.1.2 Critères d'acceptation des risques

Le critère d'acceptation du risque peut simplement être une valeur au-dessus de laquelle les risques sont jugés inacceptables.

considérés Dans le tableau A.3, si la valeur moyenne est choisie, tous les risques avec une valeur très faible, faible ou moyenne seraient comme acceptables par l'organisation et tous les risques avec une valeur élevée ou très élevée seraient considérés comme inacceptables.

En utilisant une matrice de risque à code couleur reflétant les échelles de conséquence et de probabilité, les organisations peuvent présenter graphiquement la répartition des risques à partir d'une ou plusieurs évaluations des risques. Une telle matrice de risque peut également être utilisée pour signaler l'attitude de l'organisation chargée du risque à l'égard des valeurs de risque et indiquer si un risque doit normalement être accepté ou traité.

EXEMPLE 2 Une matrice de risque utilisant trois couleurs, par exemple rouge, orange et vert, peut être appliquée pour représenter trois niveaux d'évaluation des risques, comme présenté dans le tableau A.6.

Il peut être avantageux de choisir d'autres modèles en utilisant des couleurs pour une matrice de risques.

EXEMPLE 3 Si une matrice de risque est utilisée pour comparer les résultats d'une évaluation des risques initialement réalisée avec les résultats d'une réévaluation pour les mêmes risques, la réduction du risque peut être plus facilement présentée si davantage de couleurs sont appliquées aux niveaux de risque actuels.

Il est également possible d'ajouter la détermination du niveau de gestion autorisé à accepter un risque avec une certaine valeur de risque pour un tel modèle.

Le tableau A.6 présente un exemple d'échelle d'évaluation.

Tableau A.6 — Exemple d'échelle d'évaluation combinée à une matrice de risque tricolore

Niveau de risque	Évaluation du risque	Description
Faible (vert)	Acceptable tel quel	Le risque peut être accepté sans autre action.
Modéré (orange)	Tolérable sous contrôle	Un suivi en termes de gestion des risques devra être effectué et des actions devront être mises en place dans le cadre d'une amélioration continue à moyen et long terme.
Élevé (rouge)	Inacceptable	Des mesures visant à réduire le risque doivent absolument être prises à court terme. A défaut, tout ou partie de l'activité devra être refusée.

A.2 Techniques pratiques

A.2.1 Composantes du risque lié à la sécurité des informations

Lors de l'identification et de l'évaluation des risques liés à la sécurité de l'information, les éléments suivants doivent être pris en compte :

— éléments liés au passé:

— les événements et incidents de sécurité (tant à l'intérieur qu'à l'extérieur de l'organisation) ;

— sources de risques ;

— les vulnérabilités exploitées;

— les conséquences mesurées ;

— composants liés au futur:

- des menaces;

— les vulnérabilités;

- conséquences;

— des scénarios de risques.

Les relations entre les composantes du risque de sécurité de l'information sont présentées dans la Figure A.1 et discutées dans les sections A.2.2 à A.2.7.

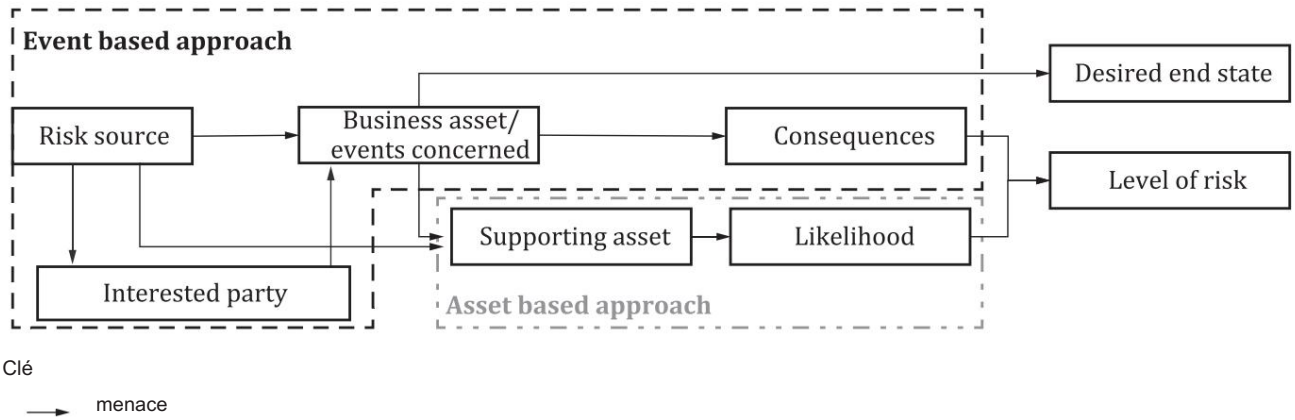


Figure A.1 — Composantes de l'évaluation des risques liés à la sécurité de l'information

Des détails sur « l'état final souhaité » peuvent être trouvés dans A.2.3 b).

A.2.2 Actifs

Lors de l'application de l'approche basée sur les actifs à l'identification des risques, les actifs doivent être identifiés.

Dans le processus d'évaluation des risques, dans le cadre de l'élaboration de scénarios de risque, l'identification des événements, des conséquences, des menaces et des vulnérabilités doit être liée aux actifs.

Dans le processus de traitement des risques, chaque contrôle est applicable à un sous-ensemble d'actifs.

Les actifs peuvent être divisés en deux catégories :

— actifs primaires/commerciaux — informations ou processus présentant de la valeur pour une organisation ;

— actifs supports — composants du système d'information sur lesquels reposent un ou plusieurs actifs de l'entreprise sont basés.

Les actifs primaires/métier sont souvent utilisés dans l'approche événementielle (identification des événements et de leurs conséquences sur le patrimoine de l'entreprise).

Les actifs supports sont souvent utilisés dans l'approche patrimoniale (identification et analyse des vulnérabilités et des menaces sur ces actifs) et dans le processus de traitement des risques (spécification du ou des actifs sur lesquels chaque contrôle doit être appliqué).

L'entreprise et les actifs de support sont liés, par conséquent les sources de risques identifiées pour les actifs de support peuvent avoir un impact sur les actifs de l'entreprise.

Pour cette raison, il est important d'identifier les relations entre les actifs et de comprendre leur valeur pour l'organisation. Une mauvaise évaluation de la valeur de l'actif peut conduire à une mauvaise appréciation des conséquences liées au risque mais peut également affecter la compréhension de la probabilité des menaces considérées.

EXEMPLE 1 Un actif de support héberge un actif métier (information dans ce cas).

Les données sont protégées par des contrôles internes et externes afin d'empêcher une source de risque d'atteindre son objectif lié à l'actif commercial en exploitant une vulnérabilité sur l'actif de support. Lors de la distinction de différents types d'actifs, les dépendances entre les actifs doivent être documentées et la propagation des risques évaluée, de sorte qu'il puisse être documenté que le même risque n'est pas évalué deux fois, une fois lorsqu'il se produit sur l'actif sous-jacent et une fois lorsqu'il affecte les actifs principaux. . Les graphiques de dépendance des actifs sont des outils utiles pour représenter ces dépendances et garantir que toutes les dépendances ont été prises en compte.

EXEMPLE 2 Le graphique de la figure A.2 indique les actifs dépendants pour l'actif métier « montrant le traitement des commandes et des factures » et peut être lu comme suit :

— « Administrateur » (type : ressource humaine), qui, s'il n'est pas correctement formé, propage un risque sur l'actif.

— « Maintenir l'informatique » (type : service), qui propage le risque sur l'actif.

— « Serveur » (type : matériel) ou à l'actif « Réseau » (type connectivité réseau). Le serveur, s'il s'arrête le fonctionnement ou le réseau mal configuré est à l'origine de l'actif.

— « Portail Web » (type : application), pour arrêter de fonctionner ou pour être indisponible.

Sans « portail Web », le processus commercial « montrant le traitement des commandes et des factures » n'offre pas le processus prévu aux clients.

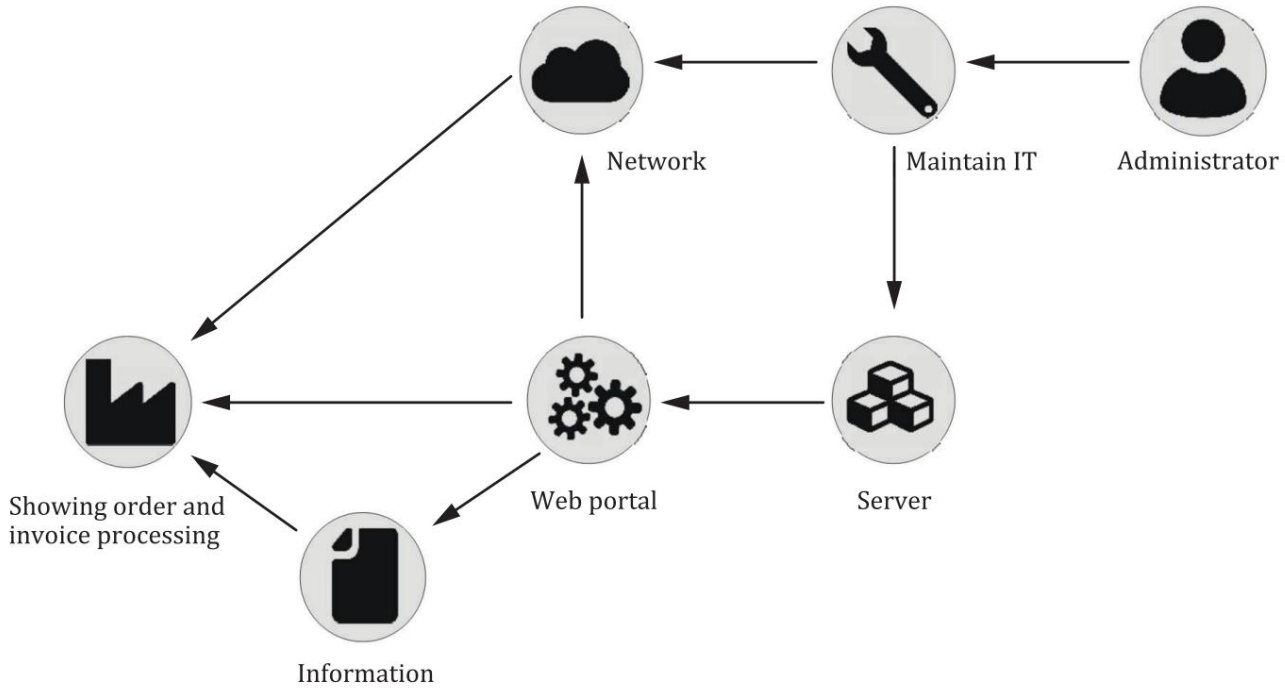


Figure A.2 — Exemple de graphique de dépendance aux actifs

A.2.3 Sources de risques et état final souhaité

Ce paragraphe propose de caractériser ce type de sources de risques. Deux critères principaux structurent cette approche descriptive :

- la motivation;

— la capacité d'agir.

a) Identification de la source du risque

Le tableau A.7 présente des exemples et des méthodes d'attaque habituelles.

Tableau A.7 — Exemples et méthodes d'attaque habituelles

Source de risque	Exemples et méthodes d'attaque habituelles
Lié à l'État	États, agences de renseignement Méthode : Attaques généralement menées par des professionnels, travaillant selon un calendrier et une méthode d'attaque prédéfinis. Ce profil d'attaquant se caractérise par sa capacité à mener une opération offensive sur une longue période (ressources stables, procédures) et à adapter ses outils et méthodes à la topologie de la cible. Par extension, ces acteurs ont les moyens d'acheter ou de découvrir des vulnérabilités 0-Day et certains sont capables d'infiltrer des réseaux isolés et de mener des attaques successives afin d'atteindre une ou plusieurs cibles (par exemple au moyen d'une attaque visant la supply chain) .
Crime organisé Organisations	cybercriminelles (mafias, gangs, groupes criminels) Méthode : escroqueries en ligne ou en personne, demande de rançon ou attaque via un ransomware, utilisation de botnets , etc. En raison notamment de la multiplication des kits d'attaque facilement disponibles en ligne, les cybercriminels mènent des opérations de plus en plus sophistiquées et organisées à des fins lucratives ou frauduleuses. fins. Certains ont les moyens d'acheter ou de découvrir des vulnérabilités 0-Day.

Tableau A.7 (suite)

Source de risque	Exemples et méthodes d'attaque habituelles
Terroriste	Cyber-terroristes, cyber-milices Méthode : Attaques généralement peu sophistiquées mais menées avec détermination dans un but de déstabilisation et de destruction : déni de service (visant par exemple à rendre indisponibles les services d'urgence d'un centre hospitalier, arrêts intempestifs d'une usine de production d'énergie) système), exploitation des vulnérabilités des sites Internet et dégradation.
Activiste idéologique	Cyber-hacktivistes, groupes d'intérêt, sectes Méthode : Les méthodes d'attaque et la sophistication des attaques sont relativement similaires à celles des cyberterroristes mais sont motivées par des intentions moins destructrices. Certains acteurs mènent ces attaques afin de véhiculer une idéologie, un message (par exemple utilisation massive des réseaux sociaux comme caisse de résonance).
Des structures spécialisées	au profil « cyber-mercenaire » avec des capacités informatiques généralement élevées d'un point de vue technique. De ce fait, il faut le distinguer des script-kiddies avec lesquels il partage pourtant l'esprit de challenge et de recherche de reconnaissance mais avec un objectif lucratif. Ces groupes peuvent être organisés en groupes spécialisés proposant de véritables services de hacking. Méthode : Ce type de hacker expérimenté est souvent à l'origine de la conception et de la création de kits et d'outils d'attaque disponibles en ligne (éventuellement payants) qui peuvent ensuite être utilisés « clé en main » par d'autres groupes d'attaquants. Il n'y a pas de motivation particulière autre que le gain financier.
Amateur	Profil du hacker script-kiddies ou qui possède de bonnes connaissances en informatique ; motivé par la quête de reconnaissance sociale, de plaisir, de challenge. Méthode : Attaques basiques mais avec la possibilité d'utiliser les kits d'attaque disponibles en ligne.
Vengeur	Les motivations de ce profil d'attaquant sont guidées par un esprit de vengeance aigu ou un sentiment d'injustice (ex : salarié licencié pour faute grave, prestataire mécontent suite à un contrat non renouvelé, etc.). Méthode : Ce profil d'attaquant se caractérise par sa détermination et sa connaissance interne des systèmes et processus organisationnels. Cela peut le rendre redoutable et lui conférer un pouvoir substantiel pour faire du mal.
Attaquant pathologique	Les motivations de ce profil d'attaquant sont de nature pathologique ou opportuniste et sont parfois guidées par le motif du gain (ex : concurrent déloyal, client malhonnête, escroc et fraudeur). Méthode : Ici, soit les attaquants disposent d'une base de connaissances en informatique qui les amène à tenter de compromettre le SI de leur cible, soit ils utilisent les kits d'attaque disponibles en ligne, soit décident de sous-traiter l'attaque informatique en faisant appel à une société spécialisée. Dans certains cas, les attaquants peuvent porter leur attention sur une source interne (employé mécontent, prestataire peu scrupuleux) et tenter de corrompre cette dernière.

b) Modélisation de la motivation d'une source de risque — état final souhaité

Il existe un large éventail de motivations ; ils peuvent être politiques, financiers, idéologiques, mais aussi sociaux ou encore représenter un état psychologique ponctuel ou pathologique.

Bien qu'il ne soit pas possible d'exprimer directement une motivation, elle peut être illustrée à travers l'intention de la source de risque et exprimée sous la forme d'un état final souhaité (DES) : la situation globale que la source de risque souhaite atteindre après la confrontation. Une classification systématique des situations, associée à des catégories générales d'action, peut guider l'analyse contextualisée.

Le tableau A.8 présente un exemple de classification des motivations pour exprimer le DES.

Tableau A.8 — Exemple de classification des motivations pour exprimer le DES

Conquérir	Capture à long terme des ressources ou des marchés économiques, acquérant le pouvoir politique ou imposant des valeurs
Acquérir	Démarche prédatrice, résolument offensive, axée sur la captation de ressources ou de bénéfices
Prévenir	Approche offensive pour limiter les actions d'un tiers
Maintenir	les efforts visant à maintenir une situation idéologique, politique, économique ou sociale
Défendre	Adopter une position de repli strictement défensive, ou une attitude explicitement menaçante (par exemple intimidation) afin de prévenir le comportement agressif d'un adversaire clairement désigné ou d'empêcher son action en le ralentissant, etc.
Survivre	Protéger une entité à tout prix, ce qui peut conduire à des actions extrêmement agressives

c) Objectifs visés

Pour atteindre le DES, la source de risque se concentre sur un ou plusieurs objectifs impactant les actifs métiers du système cible. Ce sont les objectifs cibles de la source de risque.

Le tableau A.9 présente des exemples d'objectifs cibles.

Tableau A.9 — Exemples d'objectifs cibles

Objectif visé	Description
Espionnage	Opération de renseignement (étatique, économique). Dans de nombreux cas, l'attaquant vise une installation pérenne dans le système d'information et en toute discrétion. L'armement, le spatial, l'aéronautique, le secteur pharmaceutique, l'énergie et certaines activités de l'État (économie, finance et affaires étrangères) sont des cibles privilégiées.
Prépositionnement stratégique	Le prépositionnement vise généralement une attaque sur le long terme, sans que la finalité soit clairement établie (ex : compromission des réseaux des opérateurs télécoms, infiltration de sites internet d'information de masse afin de lancer une opération d'influence politique ou économique à fort écho). La compromission soudaine et massive d'ordinateurs afin de former un botnet peut être affiliée à cette catégorie.
Influence	Opération visant à diffuser de fausses informations ou à les altérer, mobiliser des leaders d'opinion sur les réseaux sociaux, détruire des réputations, divulguer des informations confidentielles, dégrader l' image d'une organisation ou d'un Etat. Le but final est généralement de déstabiliser ou de modifier les perceptions.
Obstacle au fonctionnement	Opération de sabotage visant par exemple à rendre indisponible un site internet, provoquant une saturation d'information, empêchant l'utilisation d'une ressource numérique, rendant indisponible une installation physique. Les systèmes industriels peuvent être particulièrement exposés et vulnérables via les réseaux informatiques avec lesquels ils sont interconnectés (par exemple l'envoi de commandes afin de générer des dommages matériels ou une panne nécessitant une maintenance importante). Les attaques par déni de service distribué (DDoS) sont des techniques couramment utilisées pour neutraliser les ressources numériques.
Lucratif	Opération visant un gain financier, directement ou indirectement. Généralement liés au crime organisé , on peut citer : la fraude sur internet, le blanchiment d'argent, l'extorsion ou le détournement de fonds , les manipulations des marchés financiers, la falsification de documents administratifs, l'usurpation d'identité, etc. Certaines opérations à but lucratif peuvent recourir à une méthode d'attaque faisant partie des catégories ci-dessus (ex. espionnage et vol de données, ransomware afin de neutraliser une activité) mais la finalité reste financière.
Défi, ludique	Opération visant à réaliser un exploit à des fins de reconnaissance sociale, de défi ou simplement pour le plaisir. Bien que l'objectif soit avant tout ludique et sans volonté particulière de nuire, ce type d'opération peut avoir de lourdes conséquences pour la victime.

La différence entre un DES et un objectif cible peut être illustrée par l'exemple d'une source de risque dont le but est de remporter un marché (DES) qui cherche à voler des informations confidentielles sur les négociations à son concurrent (objectif stratégique). Parfois, la cible en question (l'information recherchée) ne débouche finalement pas sur le DES.

On peut considérer que la valeur de la cible du point de vue de la source de risque repose sur son contribution au DES.

De manière très générale, les objectifs cibles de la source de risque se répartissent en deux grandes classes :

— exploiter des ressources ciblées à son propre bénéfice, par exemple espionnage, vol, escroquerie, fraude, trafic ;

— empêcher la cible d'utiliser ses ressources (la confrontation est toujours relative), par exemple la guerre, le terrorisme, sabotage, subversion, déstabilisation.

A.2.4 Approche événementielle

A.2.4.1 Écosystème

Dans une approche basée sur les événements, des scénarios doivent être construits en analysant les différents chemins, pertinents pour les interactions entre l'organisation et les parties intéressées, qui forment tous un écosystème que les sources de risques peuvent utiliser pour atteindre les actifs de l'entreprise et leur DES.

Un nombre croissant de méthodes d'attaque utilisent les maillons les plus vulnérables d'un tel écosystème pour atteindre leurs cibles.

Les parties intéressées dans le cadre du SMSI qui doivent être prises en compte lors de l'analyse des scénarios de risques peuvent être de deux types :

— des parties externes, notamment :

  — les clients ;

  — partenaires, cotraitants ;

  — les prestataires de services (sous-traitants, fournisseurs).

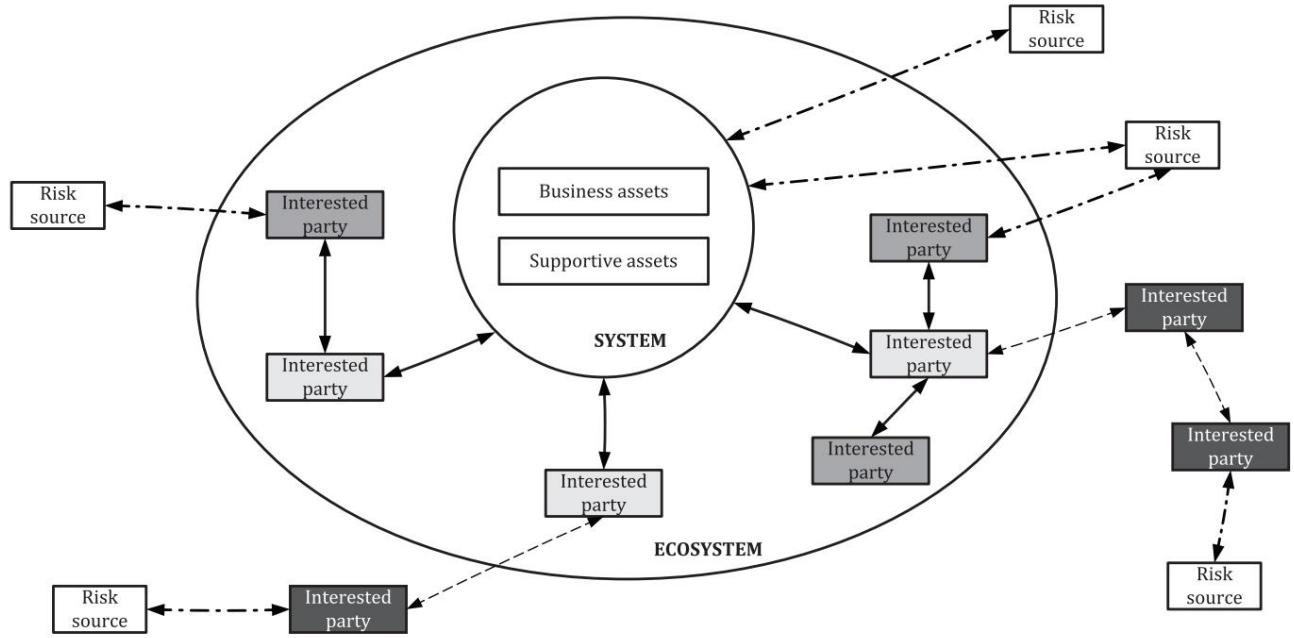
— les parties internes, notamment :

  — les prestataires de services techniques (par exemple les services d'assistance proposés par la direction informatique) ;

  — prestataires de services liés aux entreprises (par exemple, entité commerciale utilisant des données commerciales) ;

  — filiales (notamment situées dans d'autres pays).

L'objectif de l'identification des parties intéressées est d'obtenir une vision claire de l'écosystème, afin d'identifier les plus vulnérables. La sensibilisation aux écosystèmes doit être abordée dans le cadre d'une étude préliminaire des risques. La figure A.3 montre l'identification des parties intéressées de l'écosystème.



Clé

relation au sein de l'écosystème

relation qui traverse les limites de l'écosystème

relation au sein de la source de risque

partie intéressée interne/externe directement connectée au système (1er niveau de relation)

partie intéressée liée à une autre partie intéressée (2ème niveau de relation)

entité hors du périmètre de l'écosystème

Figure A.3 — Identification des parties prenantes de l'écosystème

A.2.4.2 Scénarios stratégiques

À partir des informations sur les sources de risque et les événements concernés, des scénarios réalistes de haut niveau (scénarios stratégiques) peuvent être imaginés, indiquant de quelle manière une source de risque peut procéder pour atteindre sa DES. Il peut par exemple traverser l'écosystème ou détourner certains processus métiers. Ces scénarios sont identifiés par déduction, à partir des sources de risque et de leur DES : pour chacun d'eux, les questions suivantes peuvent être posées, du point de vue de la source de risque :

— Quels sont les actifs commerciaux de l'organisation que les sources de risques doivent viser pour atteindre leur DES ?

— Afin de rendre leur attaque possible ou de la faciliter, sont-ils susceptibles de s'attaquer aux parties intéressées critiques de l'écosystème qui ont un accès privilégié aux actifs de l'entreprise ?

Une fois les éléments les plus exposés identifiés, le scénario stratégique peut être dessiné, en décrivant l'enchaînement des événements générés par la source de risque afin d'atteindre son DES. Les atteintes aux actifs de l'entreprise correspondent à des événements ultimes tandis que les événements concernant l'écosystème sont des événements intermédiaires. Le scénario stratégique reflète une évaluation des conséquences directement héritée des événements concernés.

Ces scénarios peuvent être représentés sous forme de graphiques d'attaque ou directement sur la vue écosystème de la cartographie du système d'information en superposant le(s) chemin(s) d'attaque.

Les scénarios stratégiques nécessitent une considération supplémentaire de la probabilité des événements. L'approche basée sur les actifs et les scénarios opérationnels associés peuvent être utilisés pour définir la probabilité des événements. Les exemples de menaces présentés en A.2.5.1 peuvent être utilisés pour obtenir les évaluations nécessaires.

A.2.5 Approche basée sur les actifs

A.2.5.1 Exemples de menaces

Le tableau A.10 donne des exemples de menaces typiques. La liste peut être utilisée pendant le processus d'évaluation des menaces. Les menaces considérées comme sources de risque peuvent être délibérées, accidentelles ou environnementales (naturelles) et peuvent entraîner, par exemple, des dommages ou une perte de services essentiels. La liste indique pour chaque type de menace où D (délibéré), A (accidentel), E (environnemental) est pertinent. D est utilisé pour toutes les actions délibérées visant les informations et les actifs liés à l'information, A est utilisé pour toutes les actions humaines qui peuvent accidentellement endommager les informations et les actifs liés à l'information, et E est utilisé pour tous les incidents qui ne sont pas basés sur des actions humaines. Les groupes de menaces ne sont pas classés par ordre de priorité.

Les contrôles peuvent atténuer les menaces en dissuadant ou en empêchant ces menaces d'agir ou de se produire.
La sélection des contrôles pour réduire les risques nécessite également de prendre en compte des contrôles de détection et réactifs qui identifient, réagissent, contiennent et récupèrent des événements. Les contrôles de détection et réactifs sont associés à des conséquences plutôt qu'à des menaces.

EXEMPLE La journalisation et la surveillance permettent l'identification et la réponse aux événements de sécurité.

Tableau A.10 — Exemples de menaces typiques

Catégorie	Non.	Description de la menace	Type de risque source [un]
Menaces physiques	TP01	Incendie	A, D, E
	TP02	Eau	A, D, E
	TP03	Pollution, rayonnements nocifs	A, D, E
	TP04	Accident majeur	A, D, E
	TP05	Explosion	A, D, E
	TP06	Poussière, corrosion, gel	A, D, E
Menaces naturelles	TN01	Phénomène climatique	ET
	TN02	Phénomène sismique	ET
	TN03	Phénomène volcanique	ET
	TN04	Phénomène météorologique	ET
	TN05	Inondation	ET
	TN06	Phénomène pandémique/épidémique	ET
Pannes d'infrastructure	TI01	Défaillance d'un système d'alimentation	ANNONCE
	TI02	Défaillance du système de refroidissement ou de ventilation	ANNONCE
	TI03	Perte d'alimentation	A, D, E
	TI04	Panne d'un réseau de télécommunications	A, D, E
	TI05	Panne des équipements de télécommunication	ANNONCE
	TI06	Rayonnement électromagnétique	A, D, E
	TI07	Rayonnement thermique	A, D, E
	TI08	Impulsions électromagnétiques TT01	A, D, E
Pannes techniques		Défaillance d'un appareil ou d'un système TT02	UN
		Saturation du système d'information TT03 Violation de la	ANNONCE
		maintenabilité du système d'information TH01 Terreur. attaque, sabotage	ANNONCE
	TH02	Ingénierie sociale TH03 Interception	D
		des radiations d'un appareil	D
			D

a D = délibéré ; A = accidentel ; E = environnemental.

Tableau A.10 (suite)

Catégorie	Non.	Description de la menace	Type de risque source [un]
Actions humaines	TH04	Espionnage à distance	D
	TH05	Écoute clandestine	D
	TH06	Vol de supports ou de documents	D
	TH07	Vol de matériel	D
	TH08	Vol d'identité numérique ou d'identifiants	D
	TH09	Récupération des supports recyclés ou mis au rebut	D
	TH10	Divulgation d'informations	ANNONCE
	TH11	Saisie de données provenant de sources non fiables	ANNONCE
	TH12	Falsification du matériel	D
	TH13	Falsification de logiciels	ANNONCE
	TH14	Drive-by-Exploits utilisant la communication basée sur le Web	D
	TH15	Replay attaque, attaque de l'homme du milieu	D
	TH16	Traitement non autorisé des données personnelles	ANNONCE
	TH17	Entrée non autorisée dans les installations	D
	TH18	Utilisation non autorisée des appareils	D
	TH19	Utilisation incorrecte des appareils	ANNONCE
	TH20	Appareils ou supports endommagés	ANNONCE
	TH21	Copie frauduleuse de logiciels	D
	TH22	Utilisation de logiciels contrefaits ou copiés	ANNONCE
	TH23	Corruption des données	D
	TH24	Traitement illégal des données	D
	TH25	Envoi ou distribution de logiciels malveillants	A, D, R
	TH26	Détection de position	D
Compromis de fonctions ou de services	TC01	Erreur d'utilisation	UN
	TC02	Abus de droits ou d'autorisations	ANNONCE
	TC03	Forge de droits ou autorisations	D
	TC04	Refus d'actions	D
Menaces organisationnelles	TO01	Manque de personnel	A, E
	TO02	Manque de ressources	A, E
	TO03	Défaillance des prestataires de services	A, E
	TO04	Violation des lois ou règlements	ANNONCE

a D = délibéré ; A = accidentel ; E = environnemental.

A.2.5.2 Exemples de vulnérabilités

~~Le tableau A.~~11 donne des exemples de vulnérabilités dans divers domaines de sécurité, y compris des exemples de menaces pouvant exploiter ces vulnérabilités. Les listes peuvent fournir une aide lors de l'évaluation des menaces et des vulnérabilités, pour déterminer des scénarios de risques pertinents. Dans certains cas, d'autres menaces peuvent également exploiter ces vulnérabilités.

Tableau A.11 — Exemples de vulnérabilités typiques

Catégorie	Non.	Exemples de vulnérabilités
Matériel	VH01	Maintenance insuffisante/installation défectueuse des supports de stockage
	VH02	Programmes de remplacement périodique insuffisants des équipements
	VH03	Sensibilité à l'humidité, à la poussière, aux salissures
	VH04	Sensibilité aux rayonnements électromagnétiques
	VH05	Contrôle des changements de configuration insuffisant
	VH06	Susceptibilité aux variations de tension
	VH07	Susceptibilité aux variations de température
	VH08	Stockage non protégé
	VH09	Manque de soins à disposition
	VH10	Copie incontrôlée
Logiciel	VS01	Tests logiciels inexistants ou insuffisants
	VS02	Défauts bien connus du logiciel
	VS03	Pas de « déconnexion » en quittant le poste
	VS04	Élimination ou réutilisation de supports de stockage sans effacement approprié
	VS05	Configuration insuffisante des journaux pour les besoins de la piste d'audit
	VS06	Mauvaise attribution des droits d'accès
	VS07	Logiciel largement distribué
	VS08	Application de programmes d'application aux mauvaises données en termes de temps
	VS09	Interface utilisateur compliquée
	VS10	Insuffisant ou manque de documentation
	VS11	Configuration de paramètre incorrecte
	VS12	Dates incorrectes
	VS13	Mécanismes d'identification et d'authentification insuffisants (par exemple pour l'authentification des utilisateurs)
	VS14	Tables de mots de passe non protégés
	VS15	Mauvaise gestion des mots de passe
	VS16	Services inutiles activés
	VS17	Logiciel immature ou nouveau
	VS18	Spécifications peu claires ou incomplètes pour les développeurs
	VS19	Contrôle des modifications inefficace
	VS20	Téléchargement et utilisation incontrôlés de logiciels
	VS21	Absence ou copies de sauvegarde incomplètes
	VS22	Défaut de produire des rapports de gestion
Réseau	VN01	Mécanismes insuffisants pour la preuve d'envoi ou de réception d'un message
	VN02	Lignes de communication non protégées
	VN03	Trafic sensible non protégé
	VN04	Mauvais câblage commun
	VN05	Point de défaillance unique
	VN06	Inefficacité ou absence de mécanismes d'identification et d'authentification de l'expéditeur et destinataire
	VN07	Architecture réseau non sécurisée
	VN08	Transfert de mots de passe en clair
	VN09	Gestion réseau inadéquate (résilience du routage)
	VN10	Connexions au réseau public non protégées

Tableau A.11 (suite)

Catégorie	Non.	Exemples de vulnérabilités
Personnel	VP01	Absence du personnel
	VP02	Procédures de recrutement inadéquates
	VP03	Formation en sécurité insuffisante
	VP04	Utilisation incorrecte des logiciels et du matériel
	VP05	Mauvaise sensibilisation à la sécurité
	VP06	Insuffisance ou absence de mécanismes de suivi
	VP07	Travaux non surveillés par du personnel extérieur ou de nettoyage
	VP08	Inefficacité ou absence de politiques pour l'utilisation correcte des moyens de télécommunications et Messagerie
Site	VS01	Utilisation inadéquate ou négligente du contrôle d'accès physique aux bâtiments et aux locaux
	VS02	Localisation en zone inondable
	VS03	Réseau électrique instable
	VS04	Protection physique insuffisante du bâtiment, des portes et fenêtres
Organisation	VO01	Procédure formelle d'enregistrement et de désenregistrement des utilisateurs non développée, ou sa mise en œuvre est inefficace
	VO02	Processus formel de révision du droit d'accès (supervision) non développé, ou sa mise en œuvre est inefficace
	VO03	Dispositions insuffisantes (concernant la sécurité) dans les contrats avec les clients et/ou les tiers
	VO04	Procédure de surveillance des moyens de traitement de l'information non développée ou sa mise en œuvre est inefficace
	VO05	Audits (supervision) non effectués de manière régulière
	VO06	Les procédures d'identification et d'évaluation des risques ne sont pas développées ou leur mise en œuvre est inefficace
	VO07	Insuffisance ou absence de rapports de défauts enregistrés dans les journaux de l'administrateur et de l'opérateur
	VO08	Réponse de maintenance du service inadéquate
	VO09	Accord de niveau de service insuffisant ou inexistant
	VO10	Procédure de contrôle des changements non développée ou sa mise en œuvre est inefficace
	VO11	Procédure formelle de contrôle de la documentation du SMSI non développée, ou sa mise en œuvre est inefficace
	VO12	Procédure formelle de supervision des enregistrements du SMSI non développée, ou sa mise en œuvre est inefficace
	VO13	Processus formel d'autorisation des informations accessibles au public non développé, ou sa mise en œuvre est inefficace
	VO14	Mauvaise répartition des responsabilités en matière de sécurité de l'information
	VO15	Les plans de continuité n'existent pas, ou sont incomplets, ou sont obsolètes
	VO16	Politique d'utilisation du courrier électronique non développée ou sa mise en œuvre est inefficace
	VO17	Les procédures d'introduction des logiciels dans les systèmes opérationnels ne sont pas développées ou leur mise en œuvre est inefficace
	VO18	Les procédures de traitement des informations classifiées ne sont pas développées ou leur mise en œuvre est inefficace
	VO19	Les responsabilités en matière de sécurité de l'information ne sont pas présentes dans les descriptions de poste
	VO20	Insuffisance ou absence de dispositions (concernant la sécurité des informations) dans les contrats avec employés
	VO21	Processus disciplinaire en cas d'incident de sécurité de l'information non défini ou non fonctionne correctement
	VO22	Politique formelle sur l'utilisation des ordinateurs mobiles non développée, ou sa mise en œuvre est inefficace

Tableau A.11 (suite)

Catégorie	Non.	Exemples de vulnérabilités
	VO23	Contrôle insuffisant des actifs hors site
	VO34	Politique insuffisante ou absence de « bureau et écran clairs »
	Autorisation	des installations de traitement de l'information VO25 non appliquée ou ne fonctionnant pas correctement
	VO26	Les mécanismes de surveillance des failles de sécurité ne sont pas correctement mis en œuvre
	VO27	Les procédures de signalement des faiblesses de sécurité ne sont pas développées ou leur mise en œuvre est inefficace
	VO28	Les procédures de respect des dispositions relatives aux droits intellectuels ne sont pas développées ou leur mise en œuvre est inefficace

A.2.5.3 Méthodes d'évaluation des vulnérabilités techniques

Des méthodes proactives telles que les tests du système d'information peuvent être utilisées pour identifier les vulnérabilités en fonction de la criticité du système de technologies de l'information et des communications (TIC) et des ressources disponibles (par exemple, fonds alloués, technologie disponible, personnes possédant l'expertise nécessaire pour effectuer le test).
Les méthodes de test comprennent :

— outil automatisé d'analyse des vulnérabilités;

— tests et évaluations de sécurité ;

- tests de pénétration;

— révision du code.

Un outil automatisé d'analyse des vulnérabilités est utilisé pour analyser un groupe d'hôtes ou un réseau à la recherche de services vulnérables connus [par exemple, le système autorise le protocole de transfert de fichiers anonyme (FTP), le relais Sendmail]. Cependant, certaines des vulnérabilités potentielles identifiées par l'outil d'analyse automatisée ne représentent pas nécessairement des vulnérabilités réelles dans le contexte de l'environnement du système (par exemple, certains de ces outils d'analyse évaluent les vulnérabilités potentielles sans tenir compte de l'environnement et des exigences du site). Certaines des vulnérabilités signalées par le logiciel d'analyse automatisée peuvent en réalité ne pas être vulnérables pour un site particulier, mais peuvent être configurées de cette façon parce que leur environnement l'exige. Cette méthode de test peut donc produire des faux positifs.

Les tests et évaluations de sécurité (STE) sont une autre technique qui peut être utilisée pour identifier les vulnérabilités des systèmes TIC au cours du processus d'évaluation des risques. Cela comprend le développement et l'exécution d'un plan de test (par exemple, le script de test, les procédures de test et les résultats de test attendus). L'objectif des tests de sécurité du système est de tester l'efficacité des contrôles de sécurité d'un système TIC tels qu'ils ont été appliqués dans un environnement opérationnel. L'objectif est de garantir que les contrôles appliqués répondent aux spécifications de sécurité approuvées pour les logiciels et le matériel et mettent en œuvre la politique de sécurité de l'organisation ou répondent aux normes de l'industrie.

Les tests d'intrusion peuvent être utilisés pour compléter l'examen des contrôles de sécurité et garantir que les différentes facettes du système TIC sont sécurisées. Les tests d'intrusion, lorsqu'ils sont utilisés dans le processus d'évaluation des risques, peuvent être utilisés pour évaluer la capacité d'un système TIC à résister aux tentatives intentionnelles de contourner la sécurité du système. Son objectif est de tester le système TIC du point de vue d'une source de menace et d'identifier les défaillances potentielles des systèmes de protection du système TIC.

La révision du code est la méthode d’évaluation des vulnérabilités la plus approfondie (mais aussi la plus coûteuse).

Les résultats de ces types de tests de sécurité aident à identifier les vulnérabilités d'un système.

Les outils et techniques de pénétration peuvent donner de faux résultats à moins que la vulnérabilité ne soit exploitée avec succès. Pour exploiter des vulnérabilités particulières, il est nécessaire de connaître la configuration exacte du système/de l’application/des correctifs sur le système testé. Si ces données ne sont pas connues au moment des tests, il n'est pas nécessairement possible d'exploiter avec succès une vulnérabilité particulière (par exemple, obtenir un shell inverse à distance). Cependant, il

il est toujours possible de planter ou de redémarrer un processus ou un système testé. Dans un tel cas, l'objet testé doit être également considérée comme vulnérable.

Les méthodes peuvent inclure les activités suivantes :

— interroger des personnes et des utilisateurs ;

— questionnaires;

- inspection physique;

— analyse de documents.

A.2.5.4 Scénarios opérationnels

Dans une approche basée sur les actifs, des scénarios opérationnels peuvent être construits en analysant les différents chemins, au sein des actifs de support, que les sources de risque peuvent emprunter pour atteindre les actifs de l'entreprise et leur DES.

L'analyse de ces scénarios peut aider à approfondir l'approche basée sur les événements.

Une attaque réussie est souvent le résultat de l'exploitation de plusieurs failles. Les attaques intentionnelles suivent généralement une approche séquentielle. Cette dernière exploite de manière coordonnée plusieurs vulnérabilités d'ordre informatique, organisationnel ou physique. Une telle approche basée sur l'exploitation simultanée de failles distinctes peut avoir de lourdes conséquences même si les vulnérabilités exploitées peuvent être insignifiantes lorsqu'elles sont considérées individuellement.

Les scénarios analysés peuvent être structurés selon une séquence d'attaque typique. Plusieurs modèles existent et peuvent être utilisés (par exemple le modèle de la cyber kill chain1)). L'approche doit permettre d'identifier les actifs de support critiques qui peuvent être utilisés comme vecteurs d'entrée ou d'exploitation ou comme relais de propagation de l'attaque modélisée.

Ces scénarios peuvent être représentés sous forme de graphiques ou de diagrammes d'attaque, utiles pour représenter les méthodes d'attaque de l'attaquant.

A.2.6 Exemples de scénarios applicables dans les deux approches

Des scénarios de risque peuvent être élaborés en utilisant soit une approche basée sur les événements, soit une approche basée sur les actifs, ou les deux.

La figure A.4 montre l'évaluation des risques basée sur des scénarios de risque.

1) Le modèle de cyber kill chain est le nom commercial d'un produit fourni par Lockheed Martin. Ces informations sont fournies pour la commodité des utilisateurs de ce document et ne constituent pas une approbation par l'ISO du produit nommé. Des produits équivalents peuvent être utilisés s'il peut être démontré qu'ils conduisent aux mêmes résultats.

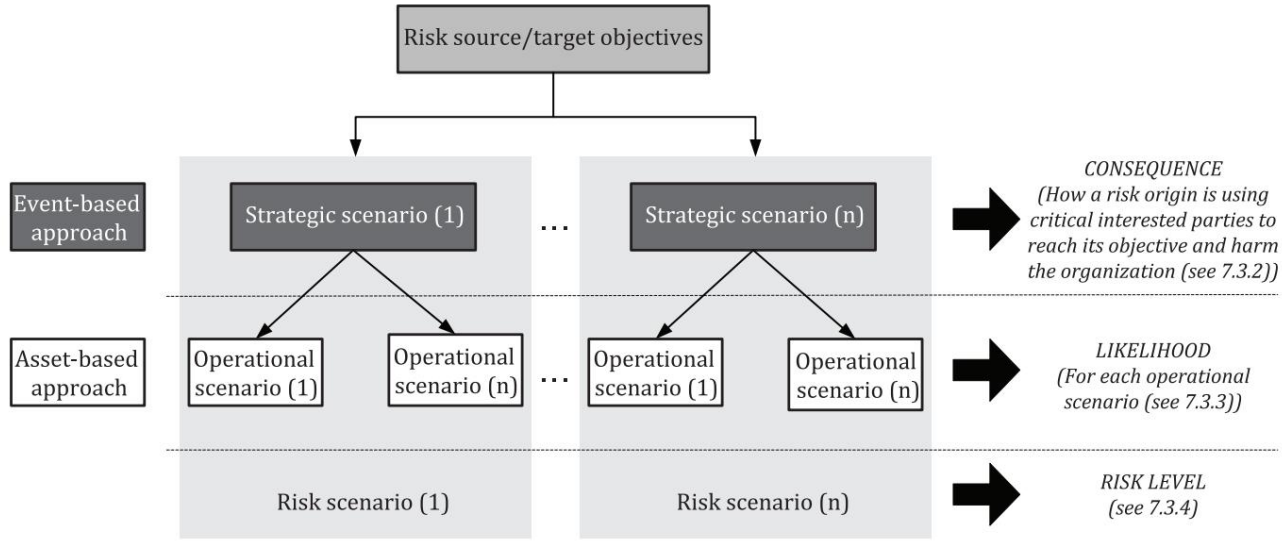


Figure A.4 — Évaluation des risques basée sur des scénarios de risque

Le tableau A.12 présente des exemples de scénarios de risque et les liens avec les approches basées sur les actifs/événements et les sources de risque.

Tableau A.12 — Exemples de scénarios de risque dans les deux approches

Source du risque	Objectif cible DES	Scénario de risque stratégique (Approche événementielle)	Scénario de risque opérationnel (Approche basée sur les actifs)
Autoritaire État	Acquérir une at- persistant	Subversion des infrastructures critiques	Déploiement d' un vecteur d'attaque caché et logiciels malveillants dans la chaîne d'approvisionnement
Crime organisé	Développement des activités illégales activités	Exploitation des infrastructures portuaires	Infiltration du syndicat des dockers
			Prendre la main sur un système informatisé de gestion des flux
		Fraude au carrousel fiscal	Créer des sociétés écrans pour réaliser de faux échanges sur le marché de la taxe carbone
		Extorsion	Distribuer des rançongiciels
Une activité agressive ness	Obtenir un monopole de marché	Influencer le régulateur	Corrompre un décideur
		Supprimer des concurrents	Campagne de diffamation sur les réseaux sociaux

A.2.7 Surveillance des événements liés aux risques

La surveillance des événements liés au risque consiste à identifier les facteurs qui peuvent influencer un scénario de risque pour la sécurité de l'information tel que défini en 10.5.2.

Dans ce contexte, les facteurs sont identifiés comme un ensemble d'éléments permettant de détecter un comportement inattendu envers un actif donné et qui peuvent être intégrés aux capacités et outils de surveillance de l'organisation pour déterminer le déclenchement d'un scénario de risque en matière de sécurité de l'information.

Le suivi des événements liés aux risques peut être défini à l'aide de plusieurs indicateurs issus de scénarios opérationnels ou de scénarios stratégiques, tous deux introduits en 7.2.1. Ils peuvent être de nature différente (techniques, organisationnelles, comportementales, résultats d'audits, etc.). Les événements sont surveillés selon des priorités définies telles que l'ampleur des conséquences et la probabilité de l'événement.

Le Tableau A.13 fournit un exemple de description d'un scénario de risque pour la sécurité de l'information avec les événements liés au risque de surveillance associés.

Tableau A.13 — Exemple de relation entre scénario de risque et événements liés au suivi du risque

Composantes de risque	Exemples		Événements à surveiller
Scénario stratégique (événement basé)	Les documents sensibles sont détruits par un administrateur		
Événements concernés	Perte de documents critiques		
Gravité des conséquences	Mesure descriptive : élevée		
Scénarios opérationnels (basé sur les actifs)	Utilisation des droits d'administrateur pour détruire les documents sensibles en accédant directement à la base de données	->	Détection d'un accès direct à la base de données en dehors des heures normales de travail
	Accès root afin de modifier la date/heure du système		
	Infection par malware du poste administrateur avec propagation sur la base de données	->	Détection d'opérations impactant un volume important de données (Destruction)
Probabilité	Mesure descriptive : moyenne		
Source de risque	Administrateur		
Objectif cible	Compromission de la disponibilité des documents sensibles		
DES	Compromission du système		
Contrôles de sécurité	Mise en œuvre de la stratégie de sauvegarde		
	Solution anti-malware		
	Implémentation du NTP		
	Renforcement du système d'exploitation		
	Restriction des droits d'accès aux données opérationnelles		

Le modèle source-fonction-destination-trigger (SFDT) permet de construire une surveillance des événements liés aux risques, où :

— source : indique d'où vient l'événement/la technique (qui et pourquoi ?) et peut être associé à A.2.3 ressources ;

— fonction : indique le type d'événement/technique réalisé par l'attaquant (quoi ?) ;

— destination : indique sur quoi la technique ou l'événement est réalisé (sur quel primaire de support actifs?);

— déclencheur : indique quelles conditions permettent de détecter et d'identifier le scénario de risque (résultats des attaque).

Un exemple d'application du modèle SFDT est présenté dans la Figure A.5.

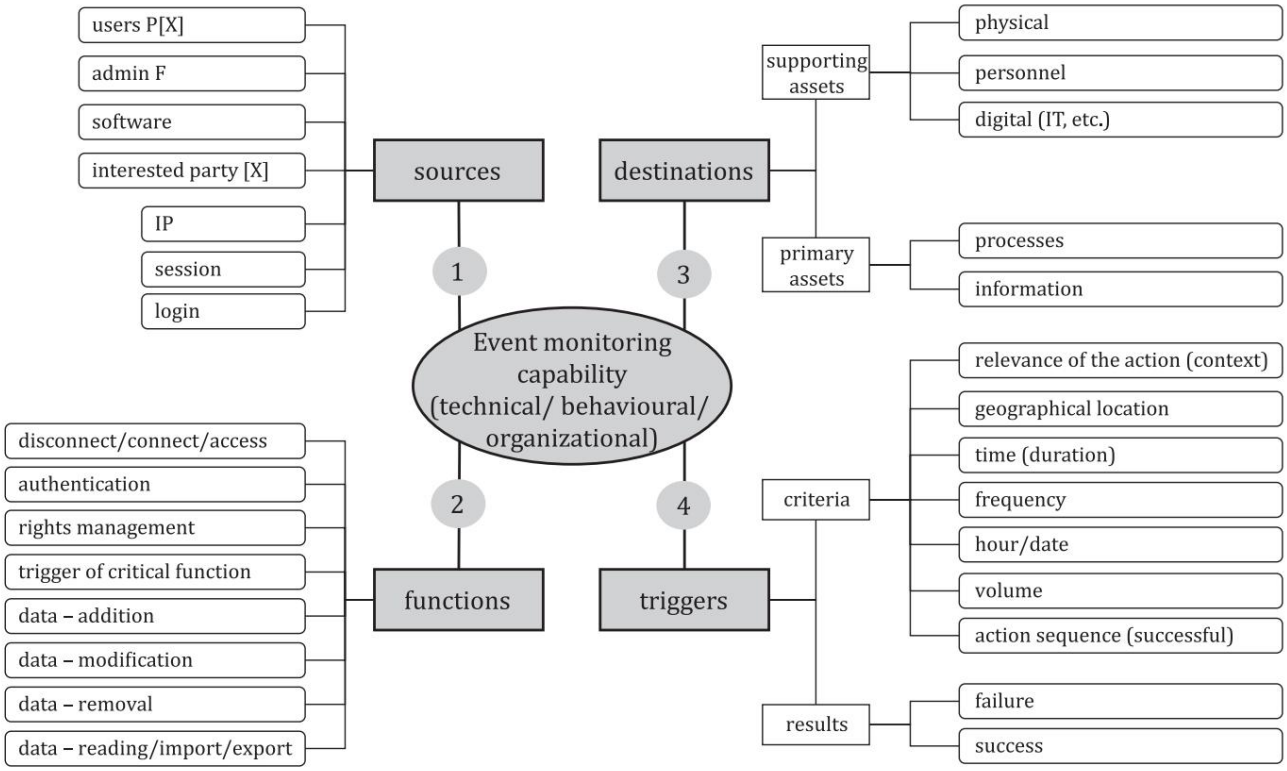


Figure A.5 — Exemple d'application du modèle SFDT

Afin de garantir qu'un événement lié au risque de surveillance est efficace et efficient pour surveiller un scénario de risque de sécurité de l'information, il est nécessaire de déterminer ses indicateurs.

Les indicateurs de suivi des événements liés aux risques sont :

— le niveau de risque du scénario de risque surveillé ;

— efficacité, capacité des événements liés au risque à surveiller un scénario de risque ;

— l'efficacité, le rapport entre l'alerte vraie positive et les faux positifs, ou encore le coût de la caractérisation.

Bibliographie

[1] ISO 17666:2016, Systèmes spatiaux — Gestion des risques

[2] ISO/IEC 27001:2022, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

[3] ISO/IEC 27003, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Lignes directrices

[4] ISO/IEC 27004, Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Suivi, mesure, analyse et évaluation

[5] ISO/IEC 27014, Sécurité de l'information, cybersécurité et protection de la vie privée — Gouvernance de la sécurité de l'information

[6] ISO/IEC/TR 27016, Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Économie des organisations

[7] ISO/IEC 27017, Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information basé sur l'ISO/IEC 27002 pour les services cloud

[8] ISO/IEC 27701, Techniques de sécurité — Extension aux normes ISO/IEC 27001 et ISO/IEC 27002 pour la gestion des informations confidentielles — Exigences et lignes directrices

[9] ISO 31000:2018, Gestion des risques — Lignes directrices

[10] CEI 31010:2019, Gestion des risques — Techniques d'évaluation des risques

[11] Guide ISO 73:2009, Gestion des risques — Vocabulaire

SCI 35.030

Prix basé sur 62 pages