RAPPORT TECHNIQUE

ISO/TR 18128

Première édition
2014-03-15

Information et documentation — Evaluation du risque pour les processus et systèmes d'enregistrement

Information and documentation — Risk assessment for records processes and systems

Numéro de référence
ISO/TR 18128:2014(F)

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

Publié en Suisse

Sommaire

Page

Avant-propos

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

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

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou sur la liste ISO des déclarations de brevets reçues (voir www.iso.org/patents).

Les éventuelles appellations commerciales utilisées dans le présent document sont données pour information à l'attention des utilisateurs et ne constituent pas une approbation ou une recommandation.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité et pour toute information au sujet de l'adhésion de l'ISO aux principes de l'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires Foreword - Supplementary information

Le Comité responsable du présent document est le Comité technique ISO/TC 46, *Information et documentation*, Sous-comité SC 11, A*rchives/Gestion des documents d'activité.*

Introduction

Tous les organismes identifient et gèrent les risques pouvant avoir une incidence sur leur bon fonctionnement. L'identification et le management des risques liés aux processus et aux systèmes documentaires relèvent de la responsabilité du professionnel de la gestion documentaire.

Le présent Rapport technique est destiné à aider les professionnels de la gestion documentaire et les personnes responsables, au sein de leur organisme, des documents d'activité à apprécier les risques liés aux processus et aux systèmes documentaires.

NOTE «Système» désigne toute application professionnelle qui crée et stocke des documents d'activité.

Il s'agit d'une activité distincte de la tâche consistant à identifier et apprécier les risques professionnels de l'organisme, pour lequel la création et la tenue des documents d'activité appropriés constituent une réponse stratégique. Les décisions relatives à la création ou non des documents d'activité pour répondre au risque général de l'activité sont des décisions de gestion qu'il convient d'éclairer par l'analyse des exigences de l'organisme en matière de documents d'activité; cette analyse est assurée par des professionnels de la gestion documentaire conjointement avec les dirigeants. Le présent Rapport technique repose sur le principe que l'organisme a créé des documents d'activité concernant ses activités professionnelles pour répondre à des objectifs opérationnels ou autres, et qu'il a mis en place au moins les mécanismes minimaux de gestion et de contrôle systématiques de ces documents d'activité.

Pour les processus et les systèmes documentaires, les conséquences des événements porteurs de risques se traduisent par la perte ou l'altération des documents d'activité qui, par conséquent, ne sont plus exploitables, fiables, authentiques, complets ou inaltérés et qui, donc, peuvent ne plus répondre aux objectifs de l'organisme.

Le présent Rapport technique prodigue des conseils et fournit des exemples en se basant sur le processus général de management du risque défini dans l'ISO 31000 (voir Figure 1) à appliquer aux risques liés aux processus et aux systèmes documentaires. Il traite de

a) l'identification des risques,

b) l'analyse des risques et

c) l'évaluation des risques.

Il convient d'intégrer au cadre organisationnel général de management du risque de l'organisme les résultats de l'analyse des risques liés aux processus et aux systèmes documentaires. En procédant ainsi, l'organisme aura un meilleur contrôle de ses documents d'activité et de leur qualité pour répondre aux besoins de son activité.

L'Article 5 présente une liste exhaustive des zones d'incertitude liées aux processus et aux systèmes documentaires, servant de guide d'identification des risques.

L'Article 6 dispense des conseils permettant de déterminer les conséquences et les probabilités des événements porteurs de risques qui ont été identifiés, en tenant compte de la présence (ou de l'absence) et de l'efficacité des contrôles existants.

L'Article 7 dispense des conseils permettant de déterminer l'importance du niveau de risque et du type de risque identifiés.

Le présent rapport n'aborde pas le traitement des risques. Une fois l'appréciation des risques liés aux processus et aux systèmes documentaires achevée, les risques objets de l'appréciation sont documentés et communiqués au service chargé du management du risque au sein de l'organisme. La réponse à apporter aux risques objet de l'appréciation entre dans le cadre du programme global de management du risque de l'organisme. Le professionnel de la gestion documentaire attribue une priorité aux risques objet de l'appréciation pour étayer les décisions de l'organisme relatives au management de ces risques.

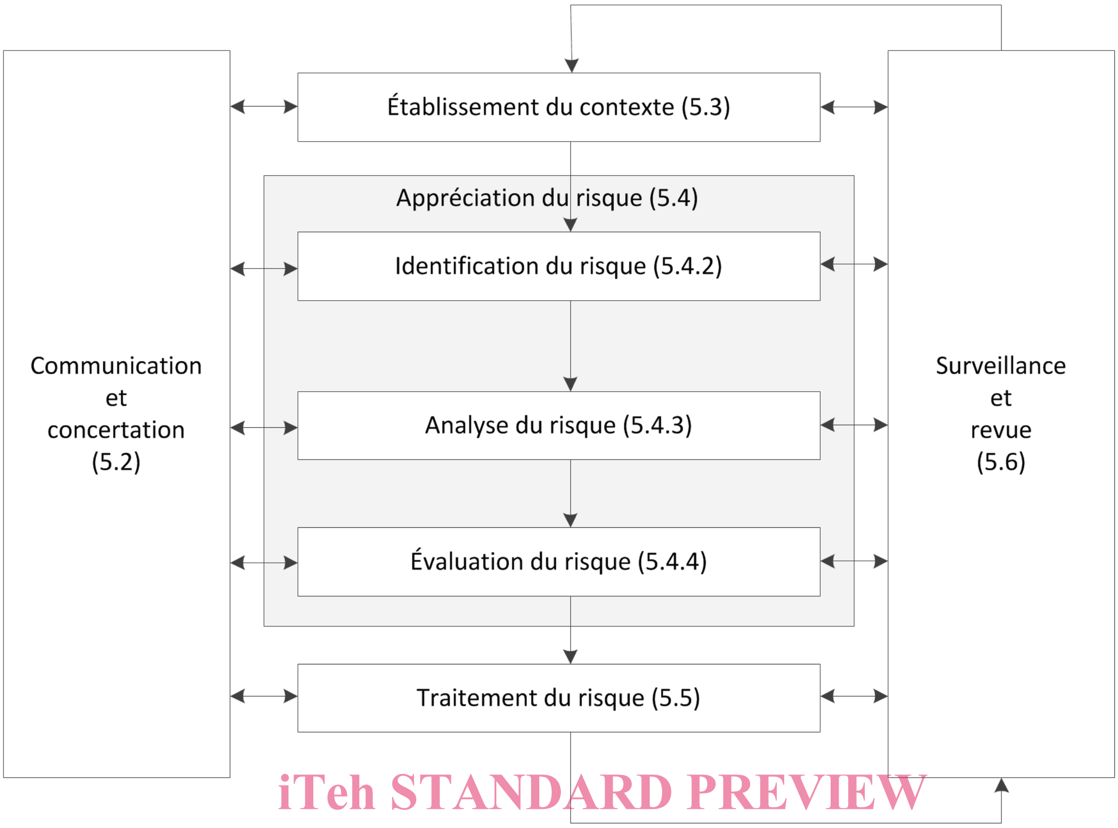

Figure 1 — Processus de management du risque

NOTE Figure 1 tirée de l'ISO 31000:2009. La numérotation renvoie au texte de l'ISO 31000.

Information et documentation — Evaluation du risque pour les processus et systèmes d'enregistrement

1 Domaine d'application

Le présent Rapport technique a pour objet d'aider les organismes à apprécier les risques liés aux processus et aux systèmes documentaires de manière qu'ils puissent s'assurer que les documents d'activité répondent aux besoins de gestion identifiés aussi longtemps que nécessaire.

Ce rapport

a) établit une méthode d'analyse pour l'identification des risques liés aux processus et aux systèmes documentaires,

b) fournit une méthode d'analyse des effets potentiels des événements indésirables sur les processus et les systèmes documentaires,

c) fournit des lignes directrices pour mener une appréciation des risques liés aux processus et aux systèmes documentaires, et

d) fournit des lignes directrices pour la documentation des risques identifiés et appréciés pour préparer des mesures d'atténuation.

Le présent Rapport technique ne traite pas des risques généraux liés aux opérations d'un organisme pouvant être atténués par la création de documents d'activité.

Le présent Rapport technique peut être utilisé par tous les organismes, quelles que soient leur taille, la nature de leurs activités ou la complexité de leurs fonctions et de leur structure. Ces facteurs, ainsi que le régime réglementaire dans lequel l'organisme évolue et qui prescrit la création et le contrôle de ces documents d'activité, sont pris en compte au moment de l'identification et de l'appréciation des risques liés aux documents d'activité et aux systèmes documentaires.

Il convient que la définition d'un organisme ou l'identification de son périmètre tiennent compte des structures complexes, des partenariats et des dispositions contractuelles concernant les services externalisés et les chaînes logistiques, qui constituent, de nos jours, une caractéristique commune aux entités publiques et privées. L'identification du périmètre de l'organisme est la première étape de la définition du domaine d'application du projet d'appréciation des risques en matière de documents d'activité.

Le présent Rapport technique ne traite pas directement de l'atténuation des risques, les méthodes en la matière différant d'un organisme à l'autre.

Le présent Rapport technique peut être utilisé par des professionnels de la gestion documentaire ou par des personnes responsables des documents d'activité de leur organisme, ainsi que par des auditeurs ou des dirigeants responsables des programmes de management du risque de leur organisme.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 30300:2011, *Information and documentation — Management systems for records — Fundamentals and vocabulary*

Guide ISO 73:2009, *Management du risque — Vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 30300, le Guide ISO 73, ainsi que les suivants s'appliquent.

3.1 Termes spécifiques au risque

3.1.1
risque
effet de l'incertitude

Note 1 à l'article: Un effet est un écart, positif et/ou négatif, par rapport à une attente.

Note 2 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Note 3 à l'article: Un risque est souvent caractérisé en référence à des événements (Guide ISO 73, 3.5.1.3) et des conséquences potentiels (Guide ISO 73, 3.6.1.3) ou à une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa vraisemblance (Guide ISO 73, 3.6.1.1).

[SOURCE: Guide ISO 73:2009, définition 1.1]

3.2 Termes spécifiques aux documents d'activité

3.2.1
système documentaire
système d'information qui intègre, organise, gère et rend accessibles les documents d'activité dans le temps

Note 1 à l'article: Ceci peut inclure les applications métiers ou les systèmes qui créent et préservent les documents d'activité.

[SOURCE: ISO 30300:2011, définition 3.4.4]

3.2.2
processus documentaire
ensemble d'activités permettant à un organisme de créer, maîtriser, utiliser, conserver et éliminer des documents d'activité

4 Critère d'appréciation du risque de l'organisme

4.1 Appréciation du risque

Il convient d'inclure l'appréciation du risque pour les processus et les systèmes documentaires dans le processus général de management du risque de l'organisme, lorsqu'il en existe un. Dans ce cas, il convient que les professionnels de la gestion documentaire tiennent compte du contexte externe et du contexte interne de l'organisme, ainsi que du contexte propre au processus de management du risque, y compris:

a) les rôles et responsabilités: il convient de spécifier le rôle des professionnels de la gestion documentaire dans l'appréciation du risque lié aux processus et aux systèmes documentaires;

b) l'étendue et le domaine d'application des activités d'appréciation du risque: afin d'éviter redondance et conflits et de permettre une approche intégrée de l'appréciation du risque incluant les documents

d'activité, il convient de préciser les relations avec les autres domaines d'appréciation du risque, comme la sécurité de l'information;

c) la méthodologie: il convient d'appliquer une méthodologie d'appréciation du risque normalisée en utilisant les outils d'appréciation du risque existants et en communiquant les rapports au groupe de personnes désignées;

d) les critères de risque: lorsque l'organisme dispose de critères de risques généraux, il convient que les risques liés aux processus et aux systèmes documentaires soient évalués en utilisant ces critères.

Lorsque l'organisme ne dispose pas de processus général de management du risque, il est nécessaire que les professionnels de la gestion documentaire déterminent des critères de risque s'appliquant aux processus et aux systèmes documentaires préalablement au processus d'appréciation.

4.2 Critères de risque

Il convient que les critères s'appuient sur les exigences réglementaires en vigueur dans la juridiction de l'organisme et qu'ils intègrent:

a) la nature et les types de conséquences à inclure, et la façon dont ils vont être mesurés;

b) le mode d'expression des probabilités;

c) la méthode de détermination du niveau de risque;

d) les critères permettant de déterminer le moment où un risque nécessite d'être traité;

e) les critères permettant de déterminer si un risque est acceptable et/ou tolérable;

f) les conditions et la méthode de prise en compte des combinaisons de risques.

En ce qui concerne la nature et les types de conséquences à inclure dans l'appréciation du risque des processus et des systèmes documentaires, il existe un préalable général qui s'applique à tous les organismes. Seuls les documents d'activité qui présentent les caractéristiques d'authenticité, de fiabilité, d'intégrité et qui sont exploitables aussi longtemps que nécessaire répondront aux besoins de l'organisme. L'identification des risques repose sur leur potentiel à compromettre ces caractéristiques générales des documents d'activité, les rendant inaptes à remplir les objectifs ayant présidé à leur création.

En ce qui concerne l'analyse de la probabilité et de la fréquence des événements dans l'appréciation du risque, voir 6.2.

Les critères d'évaluation du risque, y compris les critères permettant de déterminer si un risque est acceptable ou nécessite un traitement, incluent la taille et l'ampleur des systèmes documentaires de l'organisme, le nombre d'utilisateurs et l'utilisation qui est faite du système dans les opérations de l'organisme.

De la même façon, il convient que les critères d'évaluation des risques ayant une incidence sur les processus documentaires incluent la fréquence du processus, le nombre de systèmes dans lesquels il est utilisé, son importance relative dans la création ou la gestion des documents d'activité, la traçabilité des processus et son potentiel à inverser les effets indésirables ou à y remédier.

4.3 Attribution des priorités

De manière générale, l'organisme doit déterminer quels sont les documents d'activité qui constituent des documents essentiels pour son exploitation et le niveau d'importance qui s'y rattache. Il s'agit de décisions de gestion reposant sur les conseils des professionnels de la gestion documentaire et des dirigeants de l'activité.

La priorité attribuée aux documents d'activité pris isolément, leurs agrégations, les processus liés aux documents d'activité ou les systèmes documentaires spécifiques peuvent également faire l'objet d'une appréciation en fonction des réponses à apporter aux catastrophes majeures affectant tout ou partie des

opérations de l'organisme. Par exemple, dans un premier temps, il est nécessaire de disposer de certains documents d'activité immédiatement après une catastrophe naturelle, par exemple les adresses et les numéros de téléphone des contacts sécurité, les enregistrements des entrées dans l'usine/le bâtiment, les coordonnées des équipes d'intervention du plan catastrophe, les contacts des assurances et les détails des polices. Dans un deuxième temps, il convient que la planification de la continuité de l'activité de l'organisme identifie les fonctions qui doivent être restaurées en priorité et les documents d'activité permettant de le faire.

Il convient de porter une attention particulière aux situations dans lesquelles une combinaison de risques concerne des documents d'activité identifiés comme étant essentiels à l'exploitation de l'organisme.

5 Identification du risque

5.1 Généralités

L'identification des risques est structurée selon les catégories suivantes: contexte, systèmes et processus impliqués dans la création et le contrôle des documents d'activité de l'organisme.

Le contexte externe de l'organisme renvoie aux facteurs politiques et sociétaux, macro-économiques et technologiques, physiques et environnementaux échappant à son contrôle, mais qui ont des conséquences sur ses opérations et qui sont pris en compte lors de la détermination de ses exigences en matière de documents d'activité. Le contexte externe inclut les parties prenantes externes qui ont un intérêt particulier dans les opérations de l'organisme.

L'organisme possède également un contexte interne, à savoir les facteurs internes échappant au contrôle du (des) professionnel(s) de la gestion documentaire(s) responsable(s) des processus et des systèmes documentaires. Le contexte interne comprend des facteurs tels que la structure et les finances de l'organisme, la technologie qu'il déploie, ses ressources (humaines et budgétaires), ainsi que la culture de l'organisme, tous ces facteurs influençant les politiques et les pratiques de gestion des documents d'activité.

Les événements potentiels aux effets incertains peuvent être externes ou internes à l'organisme.

Les effets incertains provoqués par un changement dans le contexte externe peuvent diverger en fonction du point de vue des différents niveaux de l'organisme (voir Figure 2). Il est également reconnu que tout changement implique des perspectives pouvant avoir un effet positif.

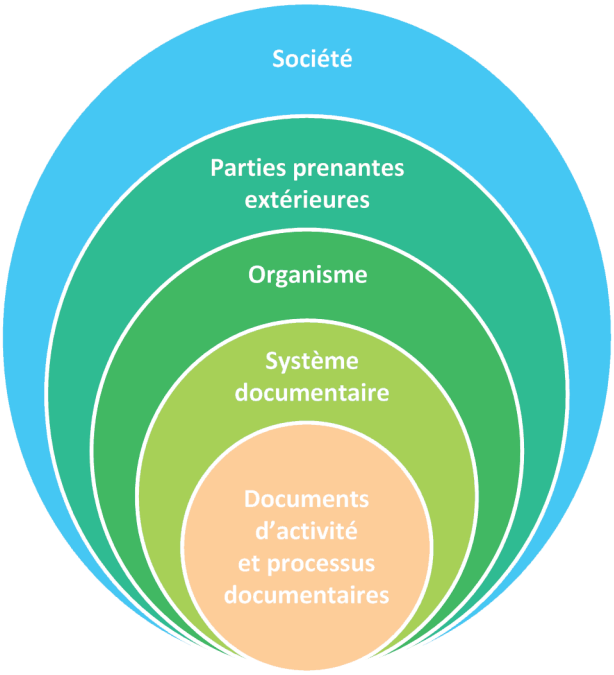

Figure 2 — Multiples éléments de contexte influant sur les documents d'activité et les processus documentaires d'un organisme

L'objectif de l'identification du risque consiste à identifier ce qui peut se produire ou le type de situation pouvant survenir, susceptible d'avoir une incidence sur la capacité des documents d'activité à répondre aux besoins de l'organisme.

Le processus d'identification du risque englobe l'identification des causes et de la source du risque, des évènements, des situations ou des circonstances pouvant avoir des conséquences matérielles sur les objectifs de l'organisme, ainsi que la nature de ces conséquences. Il existe de nombreuses méthodes d'identification du risque. Pour une comparaison des principales méthodes, se reporter à l'IEC 31010:2009, Annexe B.

Il convient de documenter les risques identifiés, soit dans un registre des risques spécifique aux documents d'activité, soit dans le registre des risques de l'organisme. Voir l'exemple fourni en Annexe A.

NOTE L'Annexe B constitue un exemple de liste de contrôle, basée sur la structure de l'Article 5, qu'un organisme peut utiliser pour identifier de façon systématique les risques liés aux processus et aux systèmes documentaires.

5.2 Contexte: Facteurs externes

5.2.1 Zones d'incertitude: Changements dans le contexte politique et social

Des changements intervenant dans le climat politique et social, au niveau national ou international, peuvent avoir une incidence sur l'évolution des mentalités vis-à-vis du gouvernement et sur le comportement de l'entreprise. Ceci peut provoquer des réformes juridiques et réglementaires, qui ont une incidence sur les opérations de l'organisme et, par conséquent, sur ses exigences liées aux documents d'activité.

La sécurité nationale, l'accès aux informations d'un gouvernement ou d'une entreprise, la protection des données personnelles, les droits de propriété intellectuelle et les responsabilités de remontées d'informations d'une entreprise constituent des exemples de zones de changement des mentalités

pouvant avoir une incidence sur les exigences liées aux documents d'activité. De façon plus générale, parmi les exemples de zones d'incertitude figurent:

a) les changements juridiques et réglementaires ayant une incidence sur les exigences liées aux documents d'activité de l'organisme;

b) les changements dans les politiques gouvernementales ayant une incidence sur les documents d'activité, sur les processus et les systèmes documentaires de l'organisme;

c) les nouvelles normes ou les codes de pratique ayant une incidence sur les documents d'activité, les processus et les systèmes documentaires de l'organisme;

d) un changement au niveau de la demande en services documentaires;

e) un changement dans les attentes des parties prenantes;

f) des changements affectant la réputation ou la confiance placée dans l'aptitude d'un organisme à délivrer ses prestations.

5.2.2 Zones d'incertitude: Environnement macro-économique et technologique

Des changements dans l'environnement macro-économique, commercial et industriel, ainsi que dans le secteur de la technologie informatique, ont de grandes conséquences sur la concurrence et l'attente des clients. Les changements peuvent s'opérer de façon progressive et continue ou ponctuellement, en raison de crises, mais ils constituent une zone d'incertitude qui peut présenter des perspectives positives.

Parmi les exemples de zones d'incertitude résultant de changements dans l'environnement macro-économique et commercial, figurent:

a) les changements intervenant dans la propriété et/ou les ressources financières de l'organisme ayant une incidence sur les priorités de gestion, notamment sur la gestion des documents d'activité;

b) les changements intervenant dans les objectifs, les fonctions et les opérations de l'organisme, entraînant des changements au niveau des exigences liées aux documents d'activité;

c) une augmentation de l'activité des organismes de régulation, entraînant une augmentation des demandes extérieures en documents d'activité;

d) une augmentation des litiges, entraînant une augmentation des demandes de documents d'activité;

e) l'introduction et l'adoption de nouvelles technologies au sein de la société;

EXEMPLES L'expansion des médias sociaux à des fins commerciales; l'utilisation de dispositifs informatiques mobiles pour les entreprises.

f) les évolutions du marché ou du portefeuille client de l'organisme.

À ces changements répondront des changements organisationnels examinés ci-après (voir 5.3.1).

5.2.3 Zones d'incertitude: Environnement physique et infrastructure

L'éventualité de catastrophes, naturelles ou d'origine humaine, à grande échelle ayant une incidence sur les opérations générales de l'organisme est une zone d'incertitude majeure exigeant une identification et une appréciation. Parmi les dommages potentiels de tels sinistres, certains ont une incidence directe sur les documents d'activité et leur stockage, ainsi qu'une incidence moins directe en raison de la suspension de services dont l'organisme dépend, par exemple l'eau, l'électricité et autres services essentiels. Parmi les zones d'incertitude figurent:

a) les phénomènes environnementaux régionaux ou locaux, destructeurs ou perturbateurs, tels que les tremblements de terre, les ouragans, les cyclones, les tsunamis, les inondations, les incendies, les grosses tempêtes ou les sécheresses prolongées;

b) l'éventualité que des actes de guerre ou de terrorisme causent des dommages majeurs aux structures ou perturbent les services délivrés aux installations de l'organisme ou dans son voisinage;

c) les autres perturbations subies par les services de transport, informatiques, de gestion des déchets, d'alimentation en eau et en électricité de l'organisme ou par d'autres services essentiels, publics ou non.

5.2.4 Zones d'incertitude: Menaces extérieures contre la sécurité

L'identification du risque doit inclure les menaces extérieures résultant d'une hostilité et ayant une incidence sur la sécurité, qui présentent des conséquences potentielles allant des dommages causés aux installations ou aux réseaux jusqu'à l'accès non autorisé aux systèmes, y compris aux systèmes documentaires. Parmi les exemples de menaces extérieures contre la sécurité figurent:

a) l'intrusion/l'accès extérieur non autorisé aux systèmes documentaires et les modifications non autorisées apportées aux documents d'activité;

b) une compromission de la sécurité non identifiée ou l'exploitation d'une vulnérabilité ne faisant pas l'objet d'une surveillance et entraînant une dégradation de l'information;

EXEMPLE L'utilisation de logiciels espions ou de maliciels; une vulnérabilité découlant de failles ou de faiblesses non corrigées dans la sécurité d'un logiciel.

c) une intrusion physique dans le stockage des documents d'archivage ou dans l'espace informatique;

d) un déni de service ou autre attaque intentionnelle via les services Internet;

e) des actes de vandalisme;

f) la perte de services tiers dont dépendent les systèmes documentaires.

NOTE L'appréciation du risque fait partie intégrante de la mise en œuvre de la série de normes internationales sur la sécurité de l'information ISO/IEC 27000. Elles s'appliquent à un vaste éventail de zones d'incertitude liées à la sécurité de l'information.

5.3 Contexte: Facteurs internes

5.3.1 Zones d'incertitude: Changements organisationnels

Les décisions de management ayant une incidence sur l'organisme, telles que les fusions, les absorptions et autres acquisitions, restructurations, rationalisations, externalisations ou, à l'inverse, délocalisations des services, constituent une zone d'incertitude liée au contexte interne de l'organisme. Ces décisions auront une incidence sur les processus et les systèmes documentaires, par exemple:

a) un changement de propriété des documents d'activité et des systèmes documentaires, et le transfert des documents qui en résulte, vers et à partir de l'organisme;

b) un changement de propriété des documents d'activité et des systèmes documentaires entraînant la migration forcée des documents d'activité ou la fusion des systèmes;

c) des dispositions en matière d'accès aux systèmes documentaires pour perpétuer le droit d'accès aux documents d'activité, suite aux transferts et aux migrations;

d) une transmission de la responsabilité des documents d'activité et des systèmes documentaires sans documentation adaptée;

e) le départ du personnel ou la perte de la mémoire de l'entreprise ayant une incidence sur la connaissance des documents d'activité et des systèmes utilisés, notamment la connaissance des procédures permettant de les récupérer et de les utiliser, et des documents d'activité plus anciens transmis dans le cadre du changement organisationnel;

f) un abandon des documents d'activité et des systèmes documentaires, en particulier des anciens systèmes, pour lesquels aucune responsabilité n'a été attribuée;

g) des changements dans les termes des contrats de service conclus avec des tiers;

h) de nouvelles politiques internes ou la modification des politiques existantes de l'organisme ayant une incidence sur les systèmes et les processus documentaires;

i) des politiques et des procédures n'ayant pas fait l'objet de revues et d'actualisations et qui ne sont plus applicables ou qui sont devenues incohérentes ou contradictoires suite au changement organisationnel;

j) des changements dans les ressources humaines de l'organisme qui peuvent avoir une incidence sur la responsabilité des documents d'activité;

k) des changements dans la politique de ressources humaines, dans les budgets de formation et dans les opportunités professionnelles ayant une incidence sur la capacité des employés responsables des documents d'activité; et

l) le plan de reprise d'activité après un sinistre qui n'est pas actualisé, ce qui peut avoir une incidence sur les documents d'activité en cas de sinistre.

5.3.2 Zones d'incertitude: Changements technologiques

L'introduction de nouvelles technologies et de nouveaux systèmes présente des perspectives d'amélioration, mais provoque également des zones d'incertitude pouvant entraîner des effets indésirables. Parmi les zones d'incertitude figurent:

a) les changements technologiques ayant une incidence sur l'interopérabilité entre les systèmes qui créent ou contrôlent des documents d'activité;

b) la compatibilité avec les plateformes et les systèmes existants;

c) la planification et la mise en œuvre de la migration des documents d'activité;

d) la reconfiguration des responsabilités et des contrôles liés aux processus documentaires;

e) l'efficacité de la mise en œuvre du changement;

EXEMPLE La pertinence de la planification et du management de projet pour mettre en œuvre une nouvelle plateforme ou un nouveau logiciel.

f) la mesure dans laquelle les politiques existantes s'appliquent aux nouvelles technologies que l'organisme a adoptées;

EXEMPLE L'utilisation de services nuagiques, médias sociaux, RFID, GPS.

g) la capacité des administrateurs et des développeurs de systèmes déployant de nouvelles technologies à comprendre les implications de ces technologies en ce qui concerne les exigences liées aux documents d'activité, à l'étape du projet et lors de sa mise en œuvre;

EXEMPLE L'utilisation de logiciels collaboratifs ou d'environnements wiki pour le développement de nouveaux systèmes qui ne peuvent capturer correctement les documents d'activité liés au projet et la documentation du système.

h) la capacité de l'infrastructure technique existante à répondre aux nouvelles exigences découlant du développement technologique de l'organisme ou des systèmes documentaires.

5.3.3 Zones d'incertitude: Ressources — Personnel et compétences

L'organisme est tributaire de la compétence de son personnel à assurer toutes ses opérations, y compris celles concernant les systèmes et processus documentaires. Le professionnel de la gestion documentaire

ou les employés qui sont responsables de la gestion documentaire évaluent les zones d'incertitude, notamment:

a) le nombre d'employés chargés de créer et de contrôler les documents d'activité, ainsi que de concevoir et d'actualiser les systèmes documentaires;

b) la sensibilisation aux politiques et aux processus documentaires;

c) l'engagement de la direction en faveur de la gestion des documents d'activité;

d) la sensibilisation aux risques liés au processus et aux systèmes documentaires, et l'aptitude de la direction à prendre des décisions concernant les mesures d'atténuation appropriées;

e) la gestion de la relation entre les responsabilités administratives liées aux systèmes documentaires et le point de vue des utilisateurs chargés des opérations;

f) la pertinence des compétences des employés pour créer et contrôler les documents d'activité;

g) le départ d'employés clés possédant des compétences essentielles et une connaissance approfondie de l'organisme et de son historique;

h) la détérioration des niveaux de compétence du personnel;

i) l'adéquation des moyens permettant d'évaluer l'efficacité ou l'aptitude du personnel.

5.3.4 Zones d'incertitude: Ressources — Finances et matériels

Les ressources financières et matérielles mises à disposition pour gérer correctement les processus et les systèmes documentaires sont conditionnées à la fois par l'environnement externe, économique et professionnel et par l'importance du soutien témoigné à la gestion des documents d'activité dans l'organisme. Parmi les zones d'incertitude figurent:

a) la suffisance des ressources financières allouées afin de respecter les engagements et les objectifs de la gestion documentaire;

b) la suffisance des ressources financières allouées afin d'acquérir, d'actualiser ou de préserver des systèmes adéquats.

5.4 Systèmes documentaires

Lors de l'appréciation des conséquences du risque sur les systèmes qui créent ou contrôlent des documents d'activité, il convient de prendre en compte la conception de ces systèmes et les questions de maintenance, de durabilité, de continuité, d'interopérabilité et de sécurité. Les systèmes utilisés par l'organisme évoluent au fil du temps, en fonction des circonstances économiques, des changements intervenant dans ses activités et dans son personnel, ainsi que des changements dans sa taille et sa structure. Il est essentiel que la direction soit correctement informée des risques liés aux systèmes documentaires et qu'elle assume la responsabilité de la réponse que l'organisme doit leur apporter.

NOTE 1 Toutes les références aux systèmes faites dans la présente section peuvent être interprétées comme références aux systèmes documentaires tels que définis en 3.2.1.

NOTE 2 Lors de l'identification des risques liés aux systèmes dans les organismes mettant en œuvre les mesures de l'ISO/IEC 27001, il convient que les professionnels de la gestion documentaire tiennent compte de la façon dont ces mesures peuvent atténuer les risques de certaines zones d'incertitude. Dans les organismes n'ayant pas mis en œuvre l'ISO/IEC 27001, ces mesures peuvent être considérées comme source d'actions d'atténuation. L'Annexe C se compose d'un tableau qui met en relation les exemples de zones d'incertitude relatives aux systèmes documentaires et les mesures de l'ISO/IEC 27001.