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 2014



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2014

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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 ..... **iv**

Introduction ..... **v**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes et définitions **2**
3.1 Termes spécifiques au risque 2
3.2 Termes spécifiques aux documents d'activité 2

4 Critère d'appréciation du risque de l'organisme **2**
4.1 Appréciation du risque 2
4.2 Critères de risque 3
4.3 Attribution des priorités 3

5 Identification du risque **4**
5.1 Généralités 4
5.2 Contexte: Facteurs externes 5
5.3 Contexte: Facteurs internes 7
5.4 Systèmes documentaires 9
5.5 Processus documentaires 12

6 Analyse des risques identifiés **14**
6.1 Généralités 14
6.2 Analyse de la vraisemblance et estimation des probabilités 14

7 Évaluation du risque **17**
7.1 Généralités 17
7.2 Évaluation des conséquences des événements indésirables 18
7.3 Évaluation du risque 19

8 Communication des risques identifiés **21**

Annexe A (informative) **Exemple d'une entrée de risque documentée dans un registre des risques** **22**

Annexe B (informative) **Exemple: listes de contrôle visant à identifier les zones d'incertitude** **23**

Annexe C (informative) **Guide d'utilisation des mesures de l'Annexe A de l'ISO/IEC 27001** **31**

Bibliographie **43**

© ISO 2014 – Tous droits réservés

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.*

© ISO 2014 – Tous droits réservés

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.

© ISO 2014 – Tous droits réservés