NORME INTERNATIONALE

ISO/IEC 30121

Première édition
2015-03-15

Technologies de l'information — Gouvernance du cadre de risque forensique numérique

Information technology — Governance of digital forensic risk framework

Numéro de référence
ISO/IEC 30121:2015(F)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, 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/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée 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 et l'IEC ne sauraient être tenues pour responsables 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 dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 40, *Gestion des services IT et gouvernance IT*.

Introduction

Les organismes de n'importe quel type sont confrontés à la fois à des facteurs et influences internes et externes qui peuvent mener à la survenue d'actions en justice et à la formulation d'exigences concernant les technologies de l'information (TI) et les systèmes d'information (SI) associés aux fins de divulguer des preuves numériques. La survenue d'actions en justice peut être le résultat d'un événement incertain, non planifié ou inattendu ou il peut s'agir d'un plan d'action planifié à l'encontre d'employés, de concurrents et de fournisseurs de service. L'importance d'un risque dépend du niveau de risque et de l'attitude face au risque de l'organisme. L'attitude de ce dernier face au risque est reflétée par ses critères de risque. Étant donné qu'il est presque certain que des preuves numériques seront découvertes et qu'elles seront, par conséquent, soumises à une divulgation légale, il convient que les organismes planifient et développent leur capacité à faire face à de telles actions en justice avant qu'elles ne se produisent.

La présente Norme internationale concerne la préparation stratégique avisée d'un organisme pour l'investigation numérique. La préparation à l'approche forensique garantit qu'un organisme a engagé une préparation stratégique appropriée et pertinente pour donner son aval concernant des événements potentiels de nature probatoire. Des actions peuvent se produire suite à d'inévitables violations de sécurité, fraudes et déclarations de réputation. Dans chaque situation, il convient que les technologies de l'information (TI) soient déployées de manière stratégique afin de maximiser la disponibilité des preuves, leur accessibilité et leur efficience économique.

La responsabilité de l'organe de gouvernance est de fournir une direction stratégique pour toutes les questions pertinentes pour l'organisme. L'organe de gouvernance est informé via les principes des pratiques d'excellence qui fournissent des préconisations générales concernant les questions de certitude et de conformité. Ces principes peuvent provenir de mandats légaux, de normes ou d'impératifs sociaux et culturels. Dans la présente Norme internationale, les principes proviennent de l'ISO/IEC 38500 en ce qui concerne les préconisations sur les pratiques d'excellence pour la gouvernance des TI (Article 4).

Ces principes doivent être mis en œuvre. Les tâches de gouvernance doivent évaluer les propositions et les plans, surveiller les performances et la conformité et orienter la stratégie et les politiques. Les parties prenantes d'un organisme peuvent fournir le mandat quant à la gouvernance et l'organe de gouvernance assume la responsabilité finale des risques. Un cadre pour la gouvernance du risque forensique numérique est établi par les responsables du risque en prenant les mesures appropriées pour garantir la direction stratégique de l'organisme. Par conséquent, l'objectif stratégique consiste à mettre en œuvre les principes et à assurer la préparation adéquate de l'investigation numérique (Article 5).

Le cadre requiert des processus stratégiques pour fournir une orientation aux cadres et aux dirigeants. Les processus stratégiques sont sélectionnés pour assurer le domaine d'application adéquat et sont principalement l'archivage, la découverte, la divulgation, la capacité et la conformité aux critères de risque (Article 6).

Les objectifs découlant des principes sont mesurables à travers les indicateurs clés d'objectifs (KGI), les objectifs stratégiques dérivés des stratégies sont mesurables à travers les indicateurs clés des performances (KPI), et la variation entre les mesures KGI et KPI est un indicateur clé des performances de l'activité (KBI) de l'organisme (Article 7).

Il convient d'utiliser la présente Norme internationale conjointement avec le vocabulaire contenu dans le Guide ISO 73:2009; l'ISO/IEC 38502, *Technologies de l'information — Gouvernance des TI — Cadre général et modèle* (disponible uniquement en anglais); et l'ISO/IEC 38500, *Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise* (disponible uniquement en anglais).

Technologies de l'information — Gouvernance du cadre de risque forensique numérique

1 Domaine d'application

La présente Norme internationale fournit un cadre pour les organes de gouvernance des organismes (comprenant les propriétaires, les membres du conseil d'administration, les directeurs, les partenaires, les cadres dirigeants ou des fonctions similaires), sur la meilleure façon de préparer un organisme aux investigations numériques avant leur occurrence. La présente Norme internationale s'applique au développement de processus (et de décisions) stratégiques concernant la conservation, la disponibilité, l'accès et l'efficience économique de la divulgation de preuves numériques. Elle s'applique aux organismes de tous types et de toutes tailles.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences 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/IEC 38500, *Technologies de l'information — Gouvernance des technologies de l'information pour l'entreprise*

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/IEC 38500 et le Guide ISO 73:2009, ainsi que les suivants s'appliquent.

3.1
preuves numériques
informations ou données stockées ou transmises sous forme binaire susceptibles d'être invoquées comme preuves

[SOURCE: ISO/IEC 27037:2012, 3.5]

3.2
organe de gouvernance
personne ou groupe de personnes qui doivent rendre des comptes aux parties prenantes concernant la performance et la conformité de l'organisme

[SOURCE: ISO/IEC/TR 38502:2014, 2.9]

3.3
sciences forensiques numériques
tâches, techniques et pratiques scientifiques utilisées lors de l'investigation des informations ou données binaires stockées ou transmises à des fins légales

3.4
risque stratégique
effet de l'incertitude sur les objectifs

4 Principes

4.1 Responsabilité

Les personnes et groupes de l'organisme comprennent et acceptent leurs responsabilités en ce qui concerne à la fois la fourniture et le besoin de preuves numériques. Les personnes responsables des investigations disposent également du savoir-faire, de l'indépendance et de l'autorité pour réaliser ces actions.

4.2 Stratégie

Le développement de la stratégie de l'organisme prend en compte la conservation actuelle et future, la disponibilité, l'accès à et l'efficience économique des preuves numériques; les plans stratégiques concernant la capacité probatoire satisfont aux besoins actuels et courants de l'organisme.

4.3 Acquisition

Les acquisitions des actifs des technologies de l'information sont réalisées pour soutenir les stratégies de l'organisme, sur la base d'une analyse appropriée et actuelle, avec une prise de décision claire et transparente. Il existe un équilibre approprié entre les avantages, les opportunités, les coûts et les risques, que ce soit à court et à long terme.

4.4 Performance

Les technologies de l'information permettent de soutenir l'organisme, en fournissant les services, les niveaux de service et la qualité de service requise pour satisfaire aux exigences actuelles et futures de l'organisme quant aux preuves numériques.

4.5 Conformité

Les biens des technologies de l'information se conforment à l'ensemble de la législation et des réglementations obligatoires. Les politiques et pratiques sont clairement définies, mises en œuvre et appliquées conformément aux critères de risque de l'organisme.

4.6 Comportement humain

Les politiques, les pratiques et les décisions forensiques numériques respectent le comportement humain, comprenant les besoins actuels et changeants de toutes les personnes impliquées dans les processus de l'organisme.

5 Le cadre

5.1 Mandat des parties prenantes

Il convient de constituer l'organe de gouvernance pour représenter les parties prenantes, il doit disposer de l'autorité requise pour définir l'orientation stratégique de l'organisme et il convient qu'il établisse les capacités permettant son fonctionnement.

5.2 Établissement

Il convient que le cycle de travail de l'organe de gouvernance soit aligné sur les tâches suivantes: Évaluer - Diriger - Surveiller, et qu'il facilite l'adoption de la politique stratégique, de la planification stratégique et de la capacité stratégique.

5.3 Évaluer

Il convient que l'organe de gouvernance examine et formule un jugement concernant les exigences actuelles et futures pour les preuves numériques, comprenant les stratégies, les propositions, les plans et les dispositifs d'approvisionnement (internes, externes ou les deux). Lors de l'évaluation de l'utilisation des technologies de l'information, il convient d'évaluer l'exigence en matière de production de preuves numériques et les exigences concernant les processus forensiques.

5.4 Diriger

Il convient que l'organe de gouvernance oriente la préparation et la mise en œuvre des stratégies, des plans et des politiques, et affecte les responsabilités correspondantes. Il convient que les plans définissent l'orientation stratégique des preuves numériques, les opérations des technologies de l'information et les capacités. Il convient que les organes de gouvernance encouragent une culture de bonne gouvernance des technologies de l'information de leur organisme en demandant aux responsables de fournir des informations dans les délais, de respecter les orientations stratégiques et de se conformer aux critères de risque.

5.5 Surveiller

Il convient que l'organe de gouvernance supervise, via des systèmes de mesure appropriés, la performance et la conformité des systèmes de technologies de l'information pour les preuves numériques. Il convient qu'il s'assure que la performance est conforme aux plans stratégiques et que ses niveaux de risques correspondent aux critères de risque de l'organisme. La responsabilité concernant l'utilisation efficace, efficiente et acceptable des technologies de l'information à des fins probatoires par un organisme, reste celle de l'organe de gouvernance et ne peut être déléguée.

6 Processus

6.1 Stratégie d'archivage

Il convient qu'un organisme établisse un système de conservation complet des archives des propriétés des informations. Il convient que les processus d'archivage soient structurés, complets, efficients, sécurisés et qu'ils préservent l'intégrité des données.

6.2 Stratégie de découverte

Il convient qu'un organisme établisse des capacités de récupération des informations efficaces et efficientes. Un accès précis et opportun aux informations de l'organisme est critique pour la prise de décision et la présentation des preuves.

6.3 Stratégie de divulgation

Il convient qu'un organisme établisse des critères de sécurisation et de divulgation des informations. Pour toute évaluation du risque associé au numérique auquel l'organisme est confronté, il convient qu'il applique ses critères de risque pour déterminer si le niveau de risque est acceptable ou si l'adoption d'un risque stratégique supplémentaire est requise. Il convient que les informations qui sont divulguées soient préservées de sorte à être vérifiables.

6.4 Stratégie de capacité forensique numérique

Il convient qu'un organisme adopte des politiques et des plans afin d'assurer la préservation des preuves numériques et la conservation de et/ou l'accès aux compétences forensiques numériques. Il convient que l'organisme gère les processus qui garantissent l'intégrité des investigations, l'indépendance des experts et la valeur probatoire des informations binaires.