NORME INTERNATIONALE

ISO/IEC 27041

Première édition
2015-06-15

Technologies de l'information — Techniques de sécurité — Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

Numéro de référence
ISO/IEC 27041:2015(F)

© ISO/IEC 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015, Publié en Suisse

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
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 ..... **iv**
Introduction ..... **v**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Symboles et abréviations **4**
5 Développement de méthode et garantie d'adéquation **4**
5.1 Vue d'ensemble 4
5.2 Principes généraux 4
5.3 Développement général et modèle de déploiement 5
5.4 Phases de garantie d'adéquation 5
5.5 Collecte et analyse des exigences 6
5.5.1 Principes généraux des exigences 6
5.5.2 Exigences fonctionnelles 7
5.5.3 Vérification des exigences 7
5.6 Conception du processus 7
5.6.1 Vue d'ensemble 7
5.6.2 Sélection des outils 7
5.6.3 Incertitude et évaluation du risque 8
5.7 Mise en œuvre du processus 8
5.7.1 Vue d'ensemble 8
5.7.2 Choix final de l'outil — Préconisations concernant le déploiement 9
5.8 Vérification du processus 9
5.8.1 Principes généraux de la vérification 9
5.8.2 Vérification des processus 9
5.8.3 Vérification des outils 9
5.9 Validation du processus 10
5.9.1 Principes généraux de la validation 10
5.9.2 Validation complète 10
5.9.3 Validation standard 10
5.9.4 Processus entièrement validés 10
5.9.5 Validation non conforme 11
5.10 Confirmation 11
5.11 Déploiement 11
5.11.1 Choix final de l'outil 11
5.12 Étude et maintenance 11
6 Modèles de garantie d'adéquation **12**
6.1 Vue d'ensemble 12
6.2 Garantie d'adéquation assurée en interne 12
6.3 Garantie d'adéquation assurée en externe 12
6.4 Garantie d'adéquation mixte 12
7 Production de preuve pour la garantie d'adéquation **12**
7.1 Vue d'ensemble 12
7.2 Préparation antérieure à la validation 13
7.3 Production de la preuve de validation 13
7.4 Maintenance de la validation 13
7.5 Validation des examens 14
7.6 Validation des investigations 14
Annexe A (informative) **Exemples** **15**
Bibliographie **19**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

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 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 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Pour une explication de 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/iso/fr/foreword.html.

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf5e-795909b331f7/iso-iec-27041-2015

Le comité responsable de ce document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité*.

 © ISO/IEC 2015 – Tous droits réservés

Introduction

À propos de la présente Norme internationale

La présente Norme internationale vise à garantir que le processus d'investigation utilisé est approprié à l'incident soumis à investigation et aux résultats exigés. Elle décrit également de manière abstraite le concept de scission de processus en apparence complexes en une série d'éléments atomiques plus petits, dont il convient qu'ils contribuent au développement de méthodes d'investigation simples mais efficaces. Il convient qu'elle soit prise en compte par toute personne autorisant, gérant ou menant une investigation, ou bien donnant des instructions concernant une investigation. Il convient de l'appliquer avant toute investigation, dans le contexte des principes et processus (tels qu'ils sont définis dans l'ISO/IEC 27043:2015) et d'une préparation et d'une planification appropriées (telles qu'elles sont définies dans l'ISO/IEC 27035-2[1)], afin de garantir l'aptitude à l'emploi des méthodes à appliquer dans les processus d'investigation décrits dans l'ISO/IEC 27037:2012 et l'ISO/IEC 27042:2015.

Relation avec d'autres normes

La présente Norme internationale est destinée à compléter d'autres normes et documents donnant des préconisations concernant l'investigation, et la préparation à l'investigation, sur des incidents de sécurité de l'information. Elle ne constitue pas un guide exhaustif, mais édicte certains principes fondamentaux visant à garantir que les outils, les techniques et les méthodes soient choisis de manière appropriée et que leur adéquation avec l'application visée puisse être démontrée, le cas échéant.

La présente Norme internationale vise également à informer les décideurs devant déterminer la fiabilité des preuves numériques qui leur sont soumises. Elle s'applique aux organismes devant protéger, analyser et présenter des preuves numériques éventuelles. Elle est pertinente dans le contexte des organismes en charge de l'établissement de politiques qui créent et évaluent des modes opératoires en rapport avec les preuves numériques, souvent dans le cadre d'un ensemble plus vaste de preuves.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

La présente Norme internationale décrit une partie d'un processus d'investigation complet, portant sans s'y limiter sur les thématiques suivantes:

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

— gestion des incidents, comprenant la préparation et la planification des investigations;

— traitement des preuves numériques;

— utilisation de l'expurgation et problèmes en découlant;

— systèmes de prévention et de détection des intrusions, comprenant les informations pouvant être obtenues à partir de ces systèmes;

— sécurité du stockage, comprenant le nettoyage du stockage;

— vérification de l'adéquation avec l'application visée des méthodes d'investigation;

— analyse et interprétation des preuves numériques;

— connaissance des principes et processus liés à l'investigation des preuves numériques;

— gestion des événements d'incident de sécurité, comprenant l'établissement de preuve à partir de systèmes impliqués dans la gestion des événements d'incident de sécurité;

— relation entre la découverte électronique et les autres méthodes d'investigation, et utilisation des techniques de découverte électronique dans d'autres investigations;

— gouvernance des investigations, comprenant les investigations forensiques.

Ces thématiques sont couvertes partiellement dans les normes ISO/IEC suivantes:

— ISO/IEC 27037:2012;

1) Publication en attente.

© ISO/IEC 2015 – Tous droits réservés

La présente Norme internationale décrit les moyens par lesquels les personnes impliquées dans les premières phases d'une investigation, comprenant la réponse initiale, peuvent s'assurer que des preuves numériques potentielles suffisantes sont recueillies pour permettre de poursuivre l'investigation de manière appropriée.

— ISO/IEC 27038:2014;

Certains documents peuvent contenir des informations dont il ne faut pas qu'elles soient divulguées auprès de certaines communautés. Des documents modifiés peuvent être diffusés auprès de ces communautés, après un traitement approprié du document d'origine. Le processus consistant à supprimer les informations à ne pas divulguer est intitulé l'«expurgation».

L'expurgation numérique des documents est un domaine relativement récent des pratiques de gestion documentaire, qui soulève des problèmes spécifiques et pose des risques potentiels. Lors de l'expurgation de documents numériques, il faut que les informations supprimées ne soient pas récupérables. Dès lors, il est nécessaire de prendre des précautions pour que les informations expurgées soient supprimées définitivement du document numérique (par exemple il ne faut pas qu'elles soient simplement masquées dans des parties non affichables du document).

L'ISO/IEC 27038:2014 spécifie les méthodes d'expurgation numérique de documents numériques. Elle spécifie également les exigences concernant les logiciels utilisables pour l'expurgation.

— ISO/IEC 27040:2015;

La présente Norme internationale donne des préconisations techniques détaillées concernant la manière dont les organismes peuvent définir un niveau approprié d'atténuation du risque grâce à l'emploi d'une approche reconnue et cohérente de la planification, la conception, la documentation et la mise en œuvre de la sécurité de stockage des données. La sécurité du stockage s'applique à la protection (la sécurité) des informations là où elles sont stockées et à la sécurité des informations transférées au moyen des liaisons de communication associées au stockage. La sécurité du stockage comprend la sécurité des dispositifs et des supports, la sécurité des activités de management associées aux dispositifs et aux supports, la sécurité des applications et des services et la sécurité relative aux utilisateurs finaux pendant la durée de vie de leurs dispositifs et supports et après la fin de leur utilisation.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/1f0247490-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

Les mécanismes de sécurité tels que le chiffrement et le nettoyage peuvent affecter la capacité d'investigation d'une personne en mettant en place des mécanismes d'obfuscation. Ils doivent être pris en compte en amont et au cours d'une investigation. Ils peuvent également être importants pour s'assurer que le stockage des matériaux probatoires, au cours et en aval d'une investigation, soit préparé et sécurisé de manière adéquate.

— ISO/IEC 27042:2015;

La présente Norme internationale décrit les modes de conception et de mise en œuvre des méthodes et processus à utiliser au cours d'une investigation, afin de permettre une évaluation correcte des preuves numériques éventuelles, l'interprétation des preuves numériques et la consignation pertinente des découvertes.

— ISO/IEC 27043:2015;

La présente Norme internationale définit les grands principes et processus communs sous-jacents à une investigation sur incident, et fournit un modèle cadre pour toutes les phases des investigations.

Les projets ISO/IEC suivants couvrent également en partie les thématiques identifiées ci-dessus et peuvent conduire à la publication de normes pertinentes, suite à la publication de la présente Norme internationale.

— ISO/IEC 27035 (toutes les parties)[2];

2) Publication en attente.

 © ISO/IEC 2015 – Tous droits réservés

Cette norme en trois parties fournit aux organismes une approche structurée et planifiée de la gestion des incidents de sécurité. Elle se compose des parties suivantes.

— ISO/IEC 27035-1[3];

Cette partie présente les concepts de base et les phases de la gestion des incidents de sécurité de l'information. Elle combine ces concepts à des principes selon une approche structurée de détection, consignation, évaluation, réponse et application des enseignements tirés.

— ISO/IEC 27035-2[4];

Cette partie présente les concepts à planifier et à préparer dans le cadre de la réponse aux incidents. Ces concepts, comprenant la politique et le plan de gestion des incidents, la constitution de l'équipe de réponse aux incidents, et les réunions d'information et la formation de sensibilisation, sont basés sur la phase de planification et de préparation du modèle présenté dans l'ISO/IEC 27035-1[5]. Cette partie couvre également la phase du modèle intitulée «Enseignements tirés».

— ISO/IEC 27035-3[6];

Cette partie couvre les responsabilités du personnel et les activités pratiques de réponse aux incidents pour l'ensemble de l'organisme. Une attention particulière est accordée aux activités de l'équipe de réponse aux incidents, comprenant les activités de surveillance, de détection, d'analyse et de réponse menées sur les données recueillies ou les événements de sécurité.

— ISO/IEC 27050 (toutes les parties)[7];

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ce projet couvre les activités liées à la découverte électronique, comprenant sans s'y limiter l'identification, la préservation, la collecte, le traitement, la revue, l'analyse et la production de stockage électronique d'informations (ESI). Il fournit en outre des préconisations concernant les mesures, allant de la création initiale d'ESI à leur élimination finale, qu'un organisme peut prendre pour atténuer les risques et réduire les dépenses, s'il s'avère que la découverte électronique devient problématique. Il concerne à la fois les membres du personnel associés à des fonctions techniques et non techniques, impliqués dans tout ou partie des activités de découverte électronique. Il est important de noter que ces préconisations ne se destinent pas à contredire ou se substituer aux législations et réglementations locales.

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10647e59-2a76-4aa6-b2b6-7e3d0f8b5214/iso-iec-27041-2015

La découverte électronique constitue souvent un vecteur pour les investigations, ainsi que les activités d'acquisition et de traitement de preuves. En outre, la sensibilité et la criticité des données nécessitent parfois des protections telles que la sécurité du stockage, pour se prémunir contre les violations de données.

— ISO/IEC 30121:2015;

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. Elle concerne la préparation stratégique avisée d'un organisme à l'investigation numérique. La préparation à l'approche forensique garantit qu'un organisme a engagé une préparation stratégique appropriée et pertinente pour supporter des événements potentiels de nature probatoire. Des actions peuvent se produire suite à d'inévitables violations de sécurité, fraudes

3) Publication en attente.

4) Publication en attente.

5) Publication en attente.

6) Publication en attente.

7) Nouveau projet.

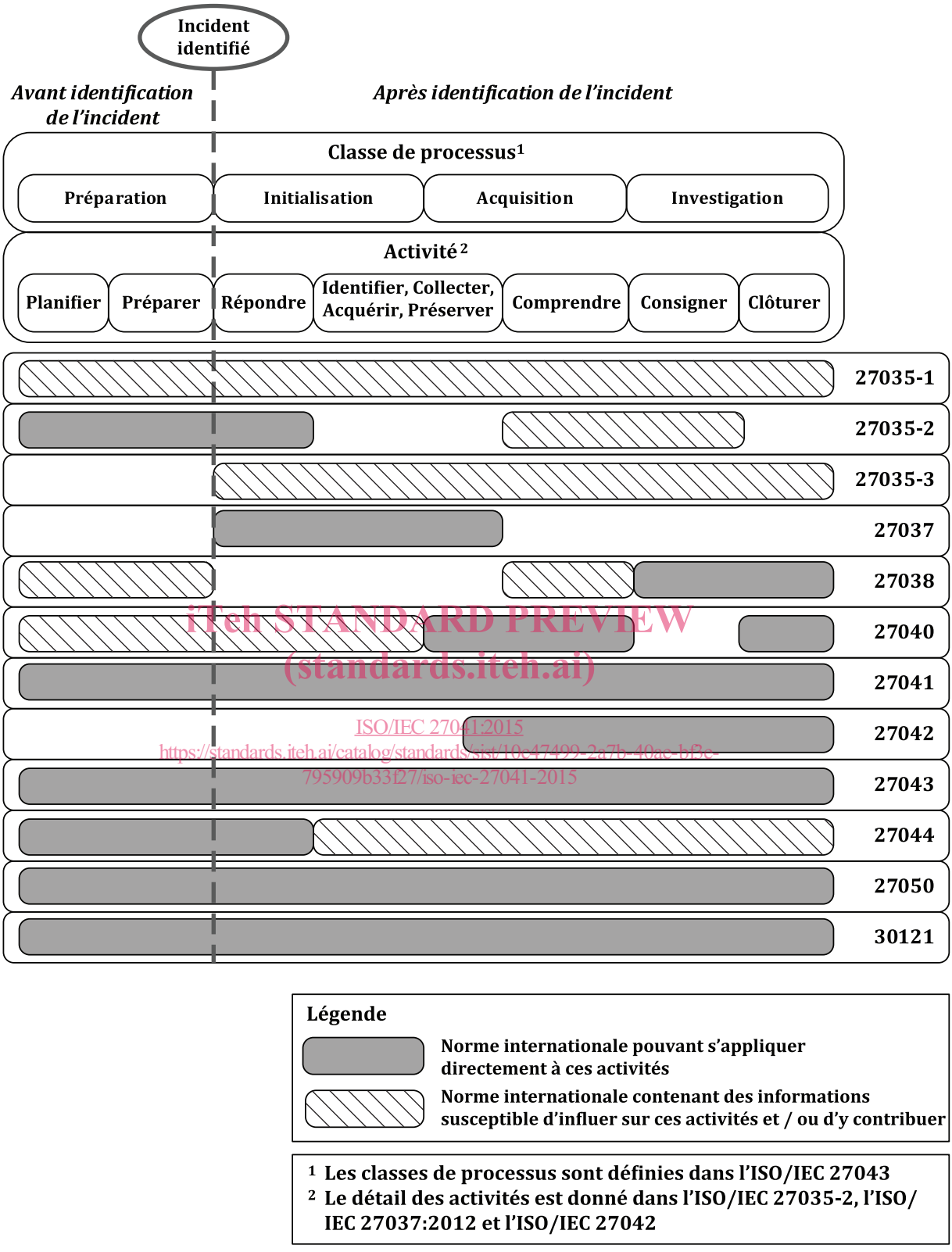
© ISO/IEC 2015 – Tous droits réservés

et déclarations de réputation. Dans chaque situation, les technologies de l'information (TI) doivent être déployées de manière stratégique afin d'optimiser la disponibilité des preuves, leur accessibilité et leur efficience économique.

La Figure 1 représente les activités types liées à un incident et à l'investigation s'y rapportant. Les références représentées dans la figure (par exemple 27037) désignent les Normes internationales répertoriées ci-dessus; les barres grisées représentent les classes/activités auxquelles chacune d'elles est la plus susceptible d'être directement applicable ou sur lesquelles chacune d'elles exerce une certaine influence sur le processus d'investigation (par exemple en stipulant une politique ou en instaurant des contraintes). Il convient cependant qu'elles soient toutes consultées en amont et au cours des phases de planification et de préparation. Les classes du processus qui sont représentées font l'objet d'une définition complète dans cette Norme internationale et les activités identifiées correspondent à celles évoquées plus en détail dans l'ISO/IEC 27035-2, l'ISO/IEC 27037:2012 et l'ISO/IEC 27042:2015.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

 © ISO/IEC 2015 – Tous droits réservés



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

Figure 1 — Applicabilité des normes aux activités et classes des processus d'investigation

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

Technologies de l'information — Techniques de sécurité — Préconisations concernant la garantie d'aptitude à l'emploi et d'adéquation des méthodes d'investigation sur incident

1 Domaine d'application

La présente Norme internationale fournit des préconisations concernant les mécanismes visant à garantir que les méthodes et processus utilisés dans l'investigation des incidents de sécurité de l'information sont «en adéquation avec l'application visée». Elle englobe les pratiques d'excellence sur la définition des exigences, la description des méthodes et l'attestation que les mises en œuvre des méthodes satisfont aux exigences. Elle prend en compte les modalités d'utilisation des essais menés par le fournisseur et les tierces parties pour contribuer à ce processus de garantie d'adéquation.

Le présent document vise à:

— fournir des préconisations concernant la collecte et l'analyse des exigences fonctionnelles et non fonctionnelles liées à une investigation sur un incident de sécurité de l'information (IS);

— fournir des préconisations concernant l'usage de la validation comme une garantie d'aptitude à l'emploi des processus sollicités par l'investigation;

iTeh STANDARD PREVIEW
(standards.iteh.ai)

— fournir des préconisations concernant l'évaluation des niveaux de validation requis et les preuves exigées sur un exercice de validation;

— fournir des préconisations concernant l'intégration des essais et documentations externes au processus de validation.

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

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/IEC 27000:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 27000:2013 ainsi que les suivants s'appliquent.

3.1
atomique
qui assure une seule fonction uniquement

Note 1 à l'article: Une *méthode* (3.11) de récupération de tous les fichiers actifs à partir d'un périphérique peut être atomique si elle s'appuie uniquement sur les métadonnées du système de fichiers. Une méthode de récupération de tous les fichiers supprimés a peu de chances d'être atomique, car elle nécessite des sous-méthodes pour identifier et extraire des structures de fichier spécifiques à partir des données figurant sur le périphérique de stockage, en se basant sur l'identification du contenu des fichiers (par exemple .jpg, .png, .odt, XML, etc.).

© ISO 2015 – Tous droits réservés

3.2
essai à la boîte noire
étude d'un processus consistant à l'utiliser pour traiter des intrants connus, et à comparer les résultats aux extrants attendus, qui reflètent les exigences du processus

3.3
client
personne ou organisme pour le compte duquel l'investigation doit être menée

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.2]

3.4
confirmation
évaluation formelle selon des preuves objectives existantes qu'un processus est adapté (ou reste adapté) à une application spécifique

3.5
notes simultanées
consignation simultanée
consignation par écrit des actions et décisions prises, intervenant en même temps que ces actions et décisions ou suivant leur occurrence, dès lors que cela est possible dans la pratique

Note 1 à l'article: De nombreuses juridictions exigent que les notes simultanées soient écrites à la main, à l'encre non effaçable et dans un carnet doté d'un système de scellé, afin de mieux lutter contre les problèmes d'authenticité et d'admissibilité.

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.4]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.6
examen
application d'un ensemble de processus visant à identifier et à extraire des preuves numériques éventuelles pertinentes à partir d'une ou de plusieurs sources

ISO/IEC 27041:2015
https://standards.iteh.ai/catalog/standards/sist/10c47499-2a7b-40ae-bf3e-795909b33f27/iso-iec-27041-2015

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.7]

3.7
investigation
application d'*examens* (3.6), suivis d'analyses et d'interprétations visant à mieux comprendre un incident

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.10]

3.8
chargé d'investigation
personne dirigeant l'investigation au niveau stratégique

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.11]

3.9
équipe d'investigation
toutes les personnes directement impliquées dans l'organisation de l'investigation

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.12]

3.10
investigateur
membre de l'*équipe d'investigation* (3.9), comprenant le *chargé d'investigation* (3.8)

[SOURCE: ISO/IEC 27042:2015, paragraphe 3.13]

 © ISO/IEC 2015 – Tous droits réservés