NORME INTERNATIONALE

ISO/IEC 27006

Troisième édition
2015-10

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

Numéro de référence
ISO/IEC 27006:2015(F)

© ISO/IEC 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, 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, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée 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 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b6b6/sist-iso-iec-27006-2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

 © ISO/IEC 2015 – Tous droits réservés

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 document. 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.

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 : Avant-propos — Informations supplémentaires.

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df86f5a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

Le comité chargé de l'élaboration du présent document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

L'ISO/IEC 27006 a été élaborée par le comité technique mixte ISO/IEC TC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

La présente troisième édition annule et remplace la deuxième édition (ISO/IEC 27006:2011) qui a fait l'objet d'une révision technique.

© ISO/IEC 2015 – Tous droits réservés

Introduction

L'ISO/IEC 17021-1 énonce les critères applicables aux organismes procédant à l'audit et à la certification des systèmes de management. Si lesdits organismes sont à accréditer comme étant conformes à l'ISO/IEC 17021-1 dans le but de procéder à l'audit et de certifier les systèmes de management de la sécurité de l'information (SMSI) conformément à l'ISO/IEC 27001:2013, certaines exigences et recommandations complémentaires de l'ISO/IEC 17021-1 sont nécessaires. Celles-ci sont fournies par la présente Norme internationale.

Le texte de la présente Norme internationale suit la structure de l'ISO/IEC 17021-1, et les exigences et recommandations spécifiques aux SMSI relatives à l'application de l'ISO/IEC 17021-1 pour la certification de SMSI sont identifiées par les lettres « SI ».

Le terme « shall » (doit) est utilisé dans la version en langue anglaise de la présente Norme internationale pour indiquer les dispositions qui, conformément aux exigences de l'ISO/IEC 17021-1 et de l'ISO/IEC 27001, revêtent un caractère obligatoire. Le terme « should » (il convient de/que) est utilisé pour indiquer une recommandation.

L'objectif principal de la présente Norme internationale est de permettre aux organismes d'accréditation d'harmoniser plus efficacement l'application des normes sur la base desquelles ils sont tenus d'évaluer les organismes de certification.

Dans l'ensemble de la présente Norme internationale, les termes « système de management » et « système » sont utilisés de façon interchangeable. La définition d'un système de management est disponible dans l'ISO 9000:2005. Le système de management utilisé dans la présente Norme internationale n'est pas à confondre avec d'autres types de systèmes, tels que les systèmes d'information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

 © ISO/IEC 2015 – Tous droits réservés

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

1 Domaine d'application

La présente Norme internationale spécifie les exigences et fournit des recommandations pour les organismes procédant à l'audit et à la certification d'un système de management de la sécurité de l'information (SMSI), en plus des exigences contenues dans l'ISO/IEC 17021-1 et l'ISO/IEC 27001. Elle a pour principal objet de soutenir l'accréditation des organismes de certification qui procèdent à la certification de SMSI.

Il est nécessaire que tout organisme qui procède à la certification de SMSI démontre qu'il respecte les exigences stipulées dans la présente Norme internationale en termes de compétences et de fiabilité, et les recommandations contenues dans la présente Norme internationale fournissent une interprétation supplémentaire de ces exigences pour tout organisme procédant à la certification de SMSI.

NOTE La présente Norme internationale peut être utilisée comme référentiel pour l'accréditation, l'évaluation par des pairs ou d'autres processus d'audit.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 Références normatives

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-af93-ba3b38a1b0d6/sist-iso-iec-27006-2018

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 17021-1:2015, *Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management — Partie 1: Exigences*

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

ISO/IEC 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 17021-1, l'ISO/IEC 27000 et les suivants s'appliquent.

3.1
documents de certification
documents indiquant que le SMSI d'un client est conforme à des normes de SMSI spécifiées et à toute documentation supplémentaire requise en vertu du système

4 Principes

Les principes de l'ISO/IEC 17021-1, 4 s'appliquent.

© ISO/IEC 2015 – Tous droits réservés

5 Exigences générales

5.1 Domaine juridique et contractuel

Les exigences de l'ISO/IEC 17021-1, 5.1 s'appliquent.

5.2 Gestion de l'impartialité

Les exigences de l'ISO/IEC 17021-1, 5.2 s'appliquent. De plus, les exigences et recommandations suivantes s'appliquent.

5.2.1 SI 5.2 Conflits d'intérêts

Les organismes de certification peuvent effectuer les tâches suivantes sans que celles-ci soient considérées comme des activités de conseil ou qu'elles génèrent un potentiel conflit d'intérêts :

a) organiser et participer en tant que formateur à des formations, à condition que, lorsque ces cours se rapportent au management de la sécurité de l'information, aux systèmes de management associés ou à l'audit, les organismes de certification doivent se limiter à la fourniture d'informations et de conseils génériques qui sont publiquement disponibles, c'est-à-dire qu'ils ne doivent pas fournir de conseils spécifiques à une entreprise qui enfreigne les exigences du point b) ci-dessous ;

b) mettre à disposition ou publier sur demande des informations décrivant l'interprétation que fait l'organisme de certification des exigences des normes d'audit de certification (voir 9.1.3.6) ;

c) activités préalables à l'audit uniquement destinées à déterminer l'état de préparation en vue de l'audit de certification ; toutefois, de ces activités ne doit pas résulter la production de recommandations ou de conseils qui contreviendraient au présent paragraphe et l'organisme de certification doit être en mesure de confirmer que ces activités ne contreviennent pas à ces exigences et qu'elles ne sont pas utilisées pour justifier une réduction de la durée finale de l'audit de certification ;

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

d) réaliser des audits seconde partie ou tierce partie conformément à des normes ou règlementations autres que celles relevant du domaine d'application de l'accréditation ;

e) apporter de la plus-value pendant les audits de certification et les visites de surveillance, par exemple en identifiant des opportunités d'amélioration, lorsqu'elles apparaissent pendant l'audit, sans recommander de solutions spécifiques.

L'organisme de certification ne doit pas fournir de revues internes de la sécurité de l'information du SMSI du client soumis à certification. De plus, l'organisme de certification doit être indépendant du ou des organismes (y compris de toutes personnes) qui effectuent l'audit interne du SMSI.

5.3 Responsabilité et situation financière

Les exigences de l'ISO/IEC 17021-1, 5.3 s'appliquent.

6 Exigences structurelles

Les exigences de l'ISO/IEC 17021-1, 6 s'appliquent.

7 Exigences relatives aux ressources

7.1 Compétence du personnel

Les exigences de l'ISO/IEC 17021-1, 7.1 s'appliquent. De plus, les exigences et recommandations suivantes s'appliquent.

© ISO/IEC 2015 – Tous droits réservés

7.1.1 SI 7.1.1 Considérations générales

7.1.1.1 Exigences génériques en matière de compétence

L'organisme de certification doit s'assurer d'avoir la connaissance des développements technologiques, juridiques et règlementaires pertinentes pour le SMSI du client qu'il évalue.

L'organisme de certification doit définir les exigences en matière de compétence pour chaque fonction de certification référencée au Tableau A.1 de l'ISO/IEC 17021-1. L'organisme de certification doit prendre en compte l'ensemble des exigences spécifiées dans l'ISO/IEC 17021-1 et les paragraphes 7.1.2 et 7.2.1 de la présente Norme internationale qui sont pertinentes pour les secteurs techniques du SMSI tel que déterminé par l'organisme de certification.

NOTE L'Annexe A fournit une synthèse des exigences en matière de compétence applicables au personnel impliqué dans certaines fonctions de certification spécifiques.

7.1.2 SI 7.1.2 Détermination des critères de compétence

7.1.2.1 Exigences de compétence pour l'audit de SMSI

7.1.2.1.1 Exigences générales

L'organisme de certification doit avoir mis en place des critères permettant de vérifier l'expérience professionnelle, la formation spécifique ou l'information des membres de l'équipe d'audit qui garantissent au moins :

iTeh STANDARD PREVIEW
(standards.iteh.ai)

a) la connaissance de la sécurité de l'information ;

b) les connaissances techniques de l'activité à auditer ;

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

c) la connaissance des systèmes de management ;

d) la connaissance des principes de l'audit ;

NOTE Des informations supplémentaires sur les principes de l'audit sont disponibles dans l'ISO 19011.

e) connaissance de la surveillance, de la mesure, de l'analyse et de l'évaluation des SMSI.

Les exigences a) à e) ci-dessus s'appliquent à tous les auditeurs qui font partie de l'équipe d'audit, à l'exception de b), qui peut être partagée entre les auditeurs qui font partie de l'équipe d'audit.

L'équipe d'audit doit avoir les compétences lui permettant d'établir le lien entre les traces d'incidents de sécurité de l'information dans le SMSI du client et les éléments appropriés du SMSI.

L'équipe d'audit doit avoir une expérience professionnelle appropriée sur les sujets ci-dessus et une application pratique de ces sujets (cela ne signifie pas qu'il est nécessaire qu'un auditeur possède un éventail complet d'expériences dans tous les domaines de la sécurité de l'information, mais l'équipe d'audit dans son ensemble doit posséder une compréhension et une expérience suffisantes pour couvrir le domaine d'application du SMSI soumis à l'audit).

7.1.2.1.2 Terminologie, principes, pratiques et techniques du management de la sécurité de l'information

Collectivement, les membres de l'équipe d'audit doivent avoir la connaissance :

a) des structures, de la hiérarchie de la documentation spécifique aux SMSI et des relations entre les documents ;

b) des outils, des méthodes et des techniques de management de la sécurité de l'information, et leur application ;

© ISO/IEC 2015 – Tous droits réservés

c) de l'appréciation du risque et management du risque de la sécurité de l'information ;

d) des processus applicables aux SMSI ;

e) de la technologie existante quand la sécurité de l'information présente un intérêt ou pose un problème

Chaque auditeur doit satisfaire aux points a), c) et d).

7.1.2.1.3 Normes et documents normatifs relatifs aux systèmes de management de la sécurité de l'information

Les auditeurs procédant à l'audit de SMSI doivent avoir connaissance :

a) de toutes les exigences contenues dans l'ISO/IEC 27001.

Collectivement, les membres de l'équipe d'audit doivent avoir connaissance :

b) de toutes les mesures contenues dans l'ISO/IEC 27002 (si cela est aussi identifié comme nécessaire par les normes spécifiques au secteur) et leur mise en œuvre, réparties dans les catégories suivantes :

1) politiques de sécurité de l'information ;
2) organisation de la sécurité de l'information ;
3) sécurité des ressources humaines ;
4) gestion des actifs ;
5) contrôle d'accès, y compris l'autorisation ;
6) cryptographie ;
7) sécurité physique et environnementale ;
8) sécurité liée à l'exploitation, y compris les services d'information ;
9) sécurité des communications, y compris la gestion de la sécurité des réseaux et le transfert de l'information ;
10) acquisition, développement et maintenance des systèmes d'information ;
11) relations avec les fournisseurs, y compris les services externalisés ;
12) gestion des incidents liés à la sécurité de l'information ;
13) aspects de la sécurité de l'information dans la gestion de la continuité de l'activité, y compris les redondances ;
14) conformité, y compris les revues de la sécurité de l'information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

7.1.2.1.4 Pratiques managériales des entreprises

Les auditeurs procédant à l'audit de SMSI doivent avoir la connaissance :

a) des bonnes pratiques de sécurité de l'information de l'industrie et les procédures de sécurité de l'information ;

b) des politiques et exigences métier en matière de sécurité de l'information ;

c) des pratiques et concepts généraux en matière de gestion d'activité, et de la relation entre politique, objectifs et résultats ;

 © ISO/IEC 2015 – Tous droits réservés

d) des processus de gestion et de la terminologie associée.

NOTE Ces processus incluent également la gestion des ressources humaines, la communication interne et externe et les autres processus de support pertinents.

7.1.2.1.5 Secteur professionnel du client

Les auditeurs procédant à l'audit de SMSI doivent avoir connaissance :

a) des exigences légales et réglementaires dans le domaine correspondant de la sécurité de l'information, et dans la zone géographique et la(les) juridictions concernées ;

NOTE La connaissance des exigences juridiques et réglementaires n'implique pas d'avoir une formation juridique approfondie.

b) les risques de la sécurité de l'information du secteur professionnel ;

c) la terminologie générique, les processus et les technologies du secteur professionnel du client ;

d) les pratiques pertinentes du secteur professionnel.

Le critère a) peut être partagé entre les membres de l'équipe d'audit.

7.1.2.1.6 Produits, processus et organisation du client

De façon collective, les auditeurs procédant à l'audit de SMSI doivent avoir connaissance :

iTeh STANDARD PREVIEW
(standards.iteh.ai)

a) de l'incidence du type de l'organisation, de sa taille, sa gouvernance, sa structure, ses fonctions et ses relations sur le développement et la mise en œuvre du SMSI et des activités de certification, y compris l'externalisation ;

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

b) des opérations complexes au sens large ;

c) des exigences légales et réglementaires applicables au produit ou au service.

7.1.2.2 Exigences de compétence pour diriger l'équipe d'audit de SMSI

Outre les exigences définies au paragraphe 7.1.2.1, les responsables d'équipe d'audit doivent satisfaire aux exigences suivantes, qui doivent être démontrées dans le cadre d'audits sous direction et supervision :

a) connaissances et savoir-faire nécessaires à la gestion du processus d'audit de certification et de l'équipe d'audit ;

b) démonstration de la capacité à communiquer de façon efficace, tant à l'oral qu'à l'écrit.

7.1.2.3 Exigences de compétence pour la réalisation de la revue de la demande

7.1.2.3.1 Normes et documents normatifs relatifs aux systèmes de management de la sécurité de l'information

Le personnel qui réalise la revue de la demande afin de déterminer les compétences requises de l'équipe d'audit, de choisir les membres de l'équipe d'audit et de déterminer le temps d'audit doit avoir connaissance :

a) des normes de SMSI et autres documents normatifs pertinents utilisés dans le processus de certification.

7.1.2.3.2 Secteur professionnel du client

Le personnel qui réalise la revue de la demande afin de déterminer les compétences requises de l'équipe d'audit, de choisir les membres de l'équipe d'audit et de déterminer le temps d'audit doit avoir la connaissance :

a) de la terminologie générique, les processus, les technologies et les risques liés au secteur professionnel du client.

7.1.2.3.3 Produits, processus et organisation du client

Le personnel qui réalise la revue de la demande afin de déterminer les compétences requises de l'équipe d'audit, de choisir les membres de l'équipe d'audit et de déterminer le temps d'audit doit avoir la connaissance :

a) des produits du client, de ses processus, de ses types d'organisation, de sa taille, de sa gouvernance, de sa structure, de ses fonctions et de ses relations sur le développement et la mise en œuvre du SMSI et des activités de certification, y compris de l'externalisation de fonctions.

7.1.2.4 Exigences de compétence pour la revue des rapports d'audit et la prise de décisions en matière de certification

7.1.2.4.1 Généralités

Le personnel qui effectue la revue des rapports d'audit et prend les décisions de certification doit posséder des connaissances qui lui permettent de vérifier la pertinence du domaine d'application de la certification ainsi que les modifications du domaine d'application et leur incidence sur l'efficacité de l'audit, en particulier le maintien de la validité de l'identification des interfaces et des dépendances et les risques associés.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/df8615a4-b5ba-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

De plus, le personnel qui effectue la revue des rapports d'audit et prend les décisions de certification doit avoir la connaissance :

a) des systèmes de management de façon générale ;

b) des processus et procédures d'audit ;

c) des principes, pratiques et techniques d'audit.

7.1.2.4.2 Terminologie, principes, pratiques et techniques du management de la sécurité de l'information

Le personnel qui effectue la revue des rapports d'audit et prend les décisions de certification doit avoir connaissance :

a) des éléments indiqués aux points a), c) et d) du paragraphe 7.1.2.1.2 ;

b) des exigences légales et règlementaires pertinentes pour la sécurité de l'information.

7.1.2.4.3 Normes et documents normatifs relatifs aux systèmes de management de la sécurité de l'information

Le personnel qui effectue la revue des rapports d'audit et prend les décisions de certification doit avoir connaissance :

a) des normes de SMSI et autres documents normatifs pertinents utilisés dans le processus de certification.

 © ISO/IEC 2015 – Tous droits réservés

7.1.2.4.4 Secteur professionnel du client

Le personnel qui effectue la revue des rapports d'audit et prend les décisions de certification doit avoir la connaissance :

a) de la terminologie générique et risques liés aux pratiques pertinentes du secteur professionnel du client.

7.1.2.4.5 Produits, processus et organisation du client

Le personnel qui effectue la revue des rapports d'audit et prend les décisions de certification doit avoir connaissance :

a) des produits du client, des processus, des types d'organisation, de la taille, de la gouvernance, de la structure, des fonctions et des relations.

7.2 Personnel intervenant dans les activités de certification

Les exigences de l'ISO/IEC 17021-1, 7.2 s'appliquent. De plus, les exigences et recommandations suivantes s'appliquent.

7.2.1 SI 7.2 Démonstration des connaissances et de l'expérience des auditeurs

L'organisme de certification doit démontrer que les auditeurs ont les connaissances et l'expérience via :

iTeh STANDARD PREVIEW
(standards.iteh.ai)

a) des qualifications spécifiques aux SMSI reconnues ;

b) un enregistrement en tant qu'auditeur le cas échéant ;

c) la participation à des formations aux SMSI et l'obtention d'habilitations personnelles pertinentes ;

SIST ISO/IEC 27006:2018
https://standards.iteh.ai/catalog/standards/sist/4f8615a4-b5bc-4f06-a693-ba5b38a1b606/sist-iso-iec-27006-2018

d) des enregistrements de perfectionnement professionnel à jour ;

e) des audits SMSI observés par un autre auditeur SMSI.

7.2.1.1 Sélection des auditeurs

Outre les exigences du paragraphe 7.1.2.1, les critères de sélection des auditeurs doivent assurer que chaque auditeur :

a) possède un niveau d'éducation ou de formation professionnelle correspondant à un niveau de formation universitaire équivalent ;

b) possède au moins quatre années d'expérience professionnelle pratique à temps plein dans le domaine des technologies de l'information, dont au moins deux années passées à un poste ou une fonction en lien avec la sécurité de l'information ;

c) a suivi avec succès au moins cinq jours de formation, dont le champ d'application couvre les audits de SMSI et le management d'audit ;

d) a acquis une expérience du processus d'évaluation de la sécurité de l'information dans sa totalité avant d'assumer la responsabilité d'exercer en tant qu'auditeur. Il convient que cette expérience ait été acquise en participant à au moins quatre audits de certification de SMSI, incluant des audits de recertification et de surveillance, pour un total d'au moins 20 jours, dont au maximum 5 jours peuvent être liés à des audits de surveillance. Cette participation doit inclure la revue de la documentation et l'appréciation du risque, l'évaluation de la mise en œuvre et l'élaboration de rapports d'audit ;

e) possède une expérience pertinente et à jour ;

© ISO/IEC 2015 – Tous droits réservés