NORME INTERNATIONALE

ISO/IEC 27007

Troisième édition
2020-01

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

Numéro de référence
ISO/IEC 27007:2020(F)

© ISO/IEC 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2020

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
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **v**

Introduction ..... **vi**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes et définitions **1**

4 Principes de l'audit **1**

5 Management d'un programme d'audit **1**

5.1 Généralités 1
5.2 Détermination des objectifs du programme d'audit 1
5.3 Détermination et évaluation des risques et des opportunités du programme d'audit 2
5.4 Établissement d'un programme d'audit 2
5.4.1 Rôles et responsabilités de la ou des personnes responsables du management du programme d'audit 2
5.4.2 Compétence de la ou des personnes responsables du management du programme d'audit 2
5.4.3 Détermination de l'étendue du programme d'audit 2
5.4.4 Détermination des ressources du programme d'audit 3
5.5 Mise en œuvre du programme d'audit 3
5.5.1 Généralités 3
5.5.2 Définition des objectifs, du domaine d'application et des critères pour chaque audit individuel 3
5.5.3 Choix et détermination des méthodes d'audit 4
5.5.4 Choix des membres de l'équipe d'audit 4
5.5.5 Attribution de la responsabilité d'un audit individuel au responsable de l'équipe d'audit 5
5.5.6 Management des résultats du programme d'audit 5
5.5.7 Management et conservation des enregistrements du programme d'audit 5
5.6 Surveillance du programme d'audit 5
5.7 Revue et amélioration du programme d'audit 5

6 Réalisation d'un audit **5**

6.1 Généralités 5
6.2 Déclenchement de l'audit 5
6.2.1 Généralités 5
6.2.2 Prise de contact avec l'audité 5
6.2.3 Détermination de la faisabilité de l'audit 5
6.3 Préparation des activités d'audit 6
6.3.1 Réalisation d'une revue des informations documentées 6
6.3.2 Planification de l'audit 6
6.3.3 Répartition des tâches au sein de l'équipe d'audit 6
6.3.4 Préparation des informations documentées en vue de l'audit 6
6.4 Réalisation des activités d'audit 6
6.4.1 Généralités 6
6.4.2 Attribution des rôles et responsabilités des guides et des observateurs 6
6.4.3 Conduite de la réunion d'ouverture 6
6.4.4 Communication pendant l'audit 6
6.4.5 Disponibilité et accès aux informations d'audit 6
6.4.6 Réalisation d'une revue des informations documentées au cours de l'audit 7
6.4.7 Recueil et vérification des informations 7
6.4.8 Production de constatations d'audit 7
6.4.9 Détermination des conclusions d'audit 7
6.4.10 Conduite de la réunion de clôture 7
6.5 Préparation et diffusion du rapport d'audit 8

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abadbde-1ec6-48f1-ad3-ed347cfa203f/iso-iec-27007-2020

© ISO/IEC 2020 – Tous droits réservés

6.5.1 Préparation du rapport d'audit 8
6.5.2 Diffusion du rapport d'audit 8
6.6 Clôture de l'audit 8
6.7 Réalisation du suivi d'audit 8
7 Compétence et évaluation des auditeurs 8
7.1 Généralités 8
7.2 Déterminer la compétence d'un auditeur 8
7.2.1 Généralités 8
7.2.2 Comportements personnels 9
7.2.3 Connaissances et aptitudes 9
7.2.4 Acquérir la compétence d'auditeur 9
7.2.5 Acquérir la compétence de responsable d'équipe d'audit 9
7.3 Déterminer les critères d'évaluation des auditeurs 9
7.4 Choisir la méthode d'évaluation des auditeurs appropriée 9
7.5 Réaliser l'évaluation d'un auditeur 10
7.6 Maintenir et améliorer la compétence du ou des auditeurs 10
Annexe A (informative) **Recommandations pour la pratique d'audit de SMSI 11**
Bibliographie 42

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

© ISO/IEC 2020 – 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.

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) ou dans la liste des déclarations de brevets reçues par l'IEC (voir http://patents.iec.ch).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 www.iso.org/iso/avant-propos.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27007:2017) qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

— le document a été aligné sur l'ISO/IEC 19011:2018;

— l'Introduction a été réécrite et développée;

— en 5.1, le texte a été supprimé dans son intégralité;

— en 5.2.2, le point d) a été supprimé;

— en 5.3, le texte a été supprimé dans son intégralité;

— en 5.5.2.2, le point b) et un alinéa suivant ont été supprimés;

— en 6.5.2.2, le premier alinéa a été supprimé et la NOTE a été reformulée.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

© ISO/IEC 2020 – Tous droits réservés

Introduction

Un audit du management des systèmes de management de la sécurité de l'information (SMSI) peut être réalisé par rapport à une série de critères d'audit, séparément ou en combinaison, comprenant, sans toutefois s'y limiter:

— les exigences définies dans l'ISO/IEC 27001:2013;

— les politiques et les exigences spécifiées par les parties intéressées pertinentes;

— les exigences légales et réglementaires;

— les processus SMSI et les mesures définis par l'organisme ou par d'autres parties;

— le(s) plan(s) de système de management se rapportant à la fourniture d'éléments de sortie spécifiques d'un SMSI (par exemple des plans visant à gérer les risques et les opportunités lors de l'établissement d'un SMSI, des plans visant à atteindre les objectifs en matière de sécurité de l'information, des plans de traitement des risques, et des plans de projet).

Le présent document fournit aux organismes de toutes tailles et de tous types des recommandations pour les audits de SMSI de domaines d'application et d'échelles variables, y compris ceux réalisés par de grandes équipes d'audit, généralement dans de grands organismes, et ceux réalisés par des auditeurs uniques, dans de grands ou petits organismes. Il convient, selon le cas, d'adapter ces recommandations au domaine d'application, à la complexité et à l'échelle du programme d'audit de SMSI.

Le présent document se concentre sur les audits internes de SMSI (de première partie) et les audits de SMSI réalisés par des organismes auprès de leurs prestataires externes et d'autres parties intéressées externes (de seconde partie). Le présent document peut également être utile pour des audits externes de SMSI réalisés à d'autres fins que la certification par tierce partie d'un système de management. L'ISO/IEC 27006 fournit des exigences relatives à l'audit des SMSI en vue d'une certification par tierce partie; toutefois, le présent document peut fournir des recommandations supplémentaires utiles.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

Le présent document doit être utilisé conjointement avec les recommandations de l'ISO 19011:2018.

Le présent document se conforme à la structure de l'ISO 19011:2018.

L'ISO 19011:2018 fournit des recommandations concernant la gestion des programmes d'audit, la conduite d'audits internes ou externes des systèmes de management, ainsi que la compétence et l'évaluation des auditeurs de systèmes de management.

L'Annexe A fournit des recommandations sur les pratiques d'audit des SMSI ainsi que les exigences de l'ISO/IEC 27001:2013, Articles 4 à 10.

© ISO/IEC 2020 – Tous droits réservés

Sécurité de l'information, cybersécurité et protection des données privées — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

1 Domaine d'application

Le présent document fournit des recommandations sur le programme d'audit des systèmes de management de la sécurité de l'information (SMSI), sur la conduite d'audits, et sur la compétence des auditeurs de SMSI, en plus des recommandations de l'ISO 19011.

Le présent document est conçu à l'intention de ceux qui ont besoin de comprendre ou de réaliser des audits internes ou externes d'un SMSI ou de gérer un programme d'audit de SMSI.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 19011:2018, *Lignes directrices pour l'audit des systèmes de management*

ISO/IEC 27000:2018, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 19011 et de l'ISO/IEC 27000 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

4 Principes de l'audit

Les principes de l'audit spécifiés dans l'ISO 19011:2018, Article 4, s'appliquent.

5 Management d'un programme d'audit

5.1 Généralités

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.1, s'appliquent.

5.2 Détermination des objectifs du programme d'audit

5.2.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.2, s'appliquent. En outre, les recommandations données en 5.2.2 s'appliquent.

© ISO/IEC 2020 – Tous droits réservés

5.2.2 Les considérations spécifiques au SMSI pour la détermination des objectifs du programme d'audit[1)] peuvent comprendre:

a) les exigences identifiées liées à la sécurité de l'information;

b) les exigences de l'ISO/IEC 27001;

c) le niveau de performance de l'audité, tel qu'indiqué par la fréquence d'événements et d'incidents liés à la sécurité de l'information, et par l'efficacité du SMSI;

NOTE Des informations complémentaires concernant le suivi des performances, les mesures, l'analyse et l'évaluation se trouvent dans l'ISO/IEC 27004.

d) les risques de sécurité de l'information pour les parties intéressées, à savoir l'audité et le client de l'audit.

Les exemples d'objectifs de programme d'audit spécifiques au SMSI comprennent:

— démontrer la conformité avec toutes les exigences juridiques et contractuelles et autres exigences applicables, et leurs implications en termes de sécurité;

— obtenir et maintenir la confiance dans les capacités de management des risques de l'audité;

— évaluer l'efficacité des actions destinées à faire face aux risques et opportunités de sécurité de l'information.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

5.3 Détermination et évaluation des risques et des opportunités du programme d'audit

5.3.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.3, s'appliquent.

5.3.2 Il convient que des mesures destinées à garantir la sécurité et la confidentialité des informations soient déterminées en tenant compte des exigences des audités et des autres parties intéressées. D'autres exigences concernant les parties peuvent inclure les exigences juridiques et contractuelles applicables.

ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5afc4bdc-1ec6-481d-a113-ed947efa203f/iso-iec-27007-2020

5.4 Établissement d'un programme d'audit

5.4.1 Rôles et responsabilités de la ou des personnes responsables du management du programme d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.4.1 s'appliquent. En outre, les recommandations de 5.4.1.2 s'appliquent.

5.4.2 Compétence de la ou des personnes responsables du management du programme d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.4.2 s'appliquent.

5.4.3 Détermination de l'étendue du programme d'audit

5.4.3.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.4.3 s'appliquent. En outre, les recommandations de 5.4.3.2 s'appliquent.

1) Pour les besoins du présent document, le terme « audit » fait référence aux audits de SMSI.

 © ISO/IEC 2020 – Tous droits réservés

5.4.3.2 L'étendue d'un programme d'audit peut englober:

a) la taille du SMSI, y compris:

   1) Le nombre total de personnes effectuant un travail sous le contrôle de l'organisation et les relations avec les parties intéressées et les prestataires pertinentes pour le SMSI;

   2) le nombre de systèmes d'information;

   3) le nombre de sites couverts par le SMSI;

b) la complexité du SMSI (y compris le nombre et la criticité des processus et des activités) en prenant en compte les différences entre les sites dans le cadre du SMSI;

c) l'importance des risques de sécurité de l'information identifiés pour le SMSI par rapport à l'activité;

d) l'importance des risques et des opportunités déterminés lors de la planification du SMSI;

e) l'importance de la préservation de la confidentialité, de l'intégrité et de la disponibilité des informations dans le cadre du SMSI;

f) la complexité des systèmes d'information à auditer, y compris la complexité de la technologie de l'information mise en œuvre;

g) le nombre de sites similaires.

Il convient que le programme d'audit tienne compte de l'établissement de priorités qui nécessitent un examen plus détaillé basé sur l'importance des risques de sécurité de l'information et des exigences métier au vu du domaine d'application du SMSI.

NOTE Des informations complémentaires concernant la durée de l'audit se trouvent dans l'ISO/IEC 27006. Des informations complémentaires relatives à l'échantillonnage multisite se trouvent dans l'ISO/IEC 27006 et le document obligatoire 1 du Forum international de l'accréditation (FIA MD1, voir la Référence [11]). Les informations contenues dans l'ISO/IEC 27006 et le FIA MD 1 ne concernent que les audits de certification.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/3abe40de-4ee0-481d-af15-ed54c4a2057b/iso-iec-27007-2020

5.4.4 Détermination des ressources du programme d'audit

5.4.4.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.4.4 s'appliquent. En outre, les recommandations de 5.4.4.2 s'appliquent.

5.4.4.2 En particulier, pour tous les risques importants applicables à l'audité et relatifs aux objectifs du programme d'audit, il convient que les auditeurs de SMSI disposent de suffisamment de temps pour faire le point sur l'efficacité des actions destinées à faire face aux risques de sécurité de l'information et aux risques et opportunités associés au SMSI.

5.5 Mise en œuvre du programme d'audit

5.5.1 Généralités

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.1 s'appliquent.

5.5.2 Définition des objectifs, du domaine d'application et des critères pour chaque audit individuel

5.5.2.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.2 s'appliquent. En outre, les recommandations de 5.5.2.2 s'appliquent.

© ISO/IEC 2020 – Tous droits réservés

5.5.2.2 Les objectifs de l'audit peuvent comprendre:

a) une évaluation pour déterminer si le SMSI identifie et traite correctement les exigences de sécurité de l'information;

b) la détermination du degré de conformité des mesures de sécurité de l'information aux exigences et procédures du SMSI.

Il convient que le domaine d'application de l'audit prenne en compte les risques de sécurité de l'information et les risques et opportunités pertinents ayant une incidence sur le SMSI des parties intéressées, à savoir le client de l'audit et l'audité.

Les thèmes suivants peuvent être considérés comme critères d'audit et utilisés comme référence vis-à-vis de laquelle la conformité est déterminée:

a) la politique de sécurité de l'information, les objectifs de sécurité de l'information, les politiques et procédures adoptées par l'audité;

b) les exigences contractuelles et autres exigences concernant l'audité;

c) les critères de risques de sécurité de l'information de l'audité, les processus d'évaluation des risques de sécurité de l'information et le processus de traitement des risques;

d) la Déclaration d'applicabilité, l'identification de toute mesure spécifique au secteur ou autre mesure nécessaire, la justification des inclusions, mises en œuvre ou non, et la justification des exclusions des mesures de l'ISO/IEC 27001:2013, Annexe A;

e) la définition des mesures pour traiter les risques de manière appropriée;

f) les méthodes et les critères de suivi, de mesure, d'analyse et d'évaluation des performances de sécurité de l'information et de l'efficacité du SMSI;

g) les exigences de sécurité de l'information spécifiées par un client;

h) les exigences de sécurité de l'information appliquées par un fournisseur ou un sous-traitant.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

5.5.3 Choix et détermination des méthodes d'audit

5.5.3.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.3 s'appliquent. En outre, les recommandations de 5.5.3.2 s'appliquent.

5.5.3.2 Si un audit conjoint est réalisé, il convient de prêter une attention particulière à la divulgation d'informations entre les parties intéressées. Il convient qu'un accord dans ce sens soit passé entre toutes les parties intéressées avant le commencement de l'audit.

5.5.4 Choix des membres de l'équipe d'audit

5.5.4.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.4 s'appliquent. En outre, les recommandations de 5.5.4.2 s'appliquent.

5.5.4.2 Il convient que la compétence de l'équipe d'audit dans son ensemble comporte une connaissance et une compréhension adéquate des points suivants:

a) un management des risques de sécurité de l'information suffisant pour évaluer les méthodes utilisées par l'audité;

b) une sécurité de l'information et un management de la sécurité de l'information suffisants pour évaluer la détermination des mesures, la planification, la mise en œuvre, la maintenance et l'efficacité du SMSI.

© ISO/IEC 2020 – Tous droits réservés

5.5.5 Attribution de la responsabilité d'un audit individuel au responsable de l'équipe d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.5 s'appliquent.

5.5.6 Management des résultats du programme d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.6 s'appliquent.

5.5.7 Management et conservation des enregistrements du programme d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.5.7 s'appliquent.

5.6 Surveillance du programme d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.6, s'appliquent.

5.7 Revue et amélioration du programme d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 5.7, s'appliquent.

6 Réalisation d'un audit

6.1 Généralités

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Les lignes directrices spécifiées dans l'ISO 19011:2018,6.1, s'appliquent.

6.2 Déclenchement de l'audit

ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

6.2.1 Généralités

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.2.1 s'appliquent.

6.2.2 Prise de contact avec l'audité

6.2.2.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.2.2 s'appliquent. En outre, les recommandations de 6.2.2.2 s'appliquent.

6.2.2.2 Le cas échéant, il convient de veiller à ce que les auditeurs aient obtenu les habilitations de sécurité nécessaires pour avoir accès aux informations documentées ou à d'autres informations requises pour les activités d'audit (comprenant, sans toutefois s'y limiter, les informations confidentielles ou sensibles).

6.2.3 Détermination de la faisabilité de l'audit

6.2.3.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.2.3 s'appliquent. En outre, les recommandations de 6.2.3.2 s'appliquent.

6.2.3.2 Avant le commencement de l'audit, il convient de demander à l'audité si des preuves d'audit SMSI ne sont pas disponibles pour examen par l'équipe d'audit, par exemple parce que ces données contiennent des informations permettant d'identifier des personnes ou d'autres informations confidentielles/sensibles. Il convient que la personne responsable du management du programme d'audit détermine si le SMSI peut être audité de manière satisfaisante en l'absence de preuves d'audit. Si la conclusion est qu'il est impossible d'auditer le SMSI de manière satisfaisante sans examiner les preuves d'audit identifiées, il convient que la personne responsable du management du programme d'audit informe l'audité que l'audit ne peut pas avoir lieu tant que des mesures d'accès appropriées n'ont

© ISO/IEC 2020 – Tous droits réservés

pas été mises en place, ou que d'autres moyens de réaliser l'audit n'ont pas été proposés à ou par l'audité. Si l'audit a lieu, il convient que le plan d'audit prenne en compte les restrictions d'accès.

6.3 Préparation des activités d'audit

6.3.1 Réalisation d'une revue des informations documentées

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.3.1 s'appliquent.

6.3.2 Planification de l'audit

6.3.2.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.3.2 s'appliquent. En outre, les recommandations de 6.3.2.2 s'appliquent.

6.3.2.2 Il convient que le responsable de l'équipe d'audit soit conscient du fait que des risques pour l'audité peuvent résulter de la présence des membres de l'équipe d'audit. La présence de l'équipe d'audit peut affecter la sécurité de l'information et constituer une source de risques supplémentaires pour les informations de l'audité, telles que des enregistrements ou une infrastructure de système confidentiels ou sensibles (par exemple effacement accidentel, divulgation non autorisée d'informations, modification involontaire d'informations).

6.3.3 Répartition des tâches au sein de l'équipe d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.3.3 s'appliquent.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

6.3.4 Préparation des informations documentées en vue de l'audit

6.3.4.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.3.4 s'appliquent. En outre, les recommandations de 6.3.4.2 s'appliquent.

https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

6.3.4.2 Il convient que le responsable de l'équipe d'audit fasse en sorte que tous les documents de travail d'audit soient classés correctement et traités conformément à la classification.

6.4 Réalisation des activités d'audit

6.4.1 Généralités

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.1 s'appliquent.

6.4.2 Attribution des rôles et responsabilités des guides et des observateurs

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.2 s'appliquent.

6.4.3 Conduite de la réunion d'ouverture

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.3 s'appliquent.

6.4.4 Communication pendant l'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.4 s'appliquent.

6.4.5 Disponibilité et accès aux informations d'audit

6.4.5.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.5 s'appliquent. En outre, les recommandations de 6.4.5.2 s'appliquent.

© ISO/IEC 2020 – Tous droits réservés

6.4.5.2 Si des preuves d'audit ne sont pas à la disposition de l'équipe d'audit au cours de l'audit pour des raisons de classification ou de sensibilité, il convient que l'auditeur en chef détermine dans quelle mesure cela affecte la confiance dans les résultats et les conclusions de l'audit, et en fasse mention dans le rapport d'audit, sans compromettre la sensibilité des données non disponibles.

6.4.6 Réalisation d'une revue des informations documentées au cours de l'audit

6.4.6.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.6 s'appliquent. En outre, les recommandations de 6.4.6.2 s'appliquent.

6.4.6.2 Il convient que les auditeurs de SMSI vérifient que les informations documentées requises dans les critères d'audit et applicables dans le cadre de l'audit existent et sont conformes aux exigences de critères d'audit.

Il convient que les auditeurs de SMSI confirment que les mesures déterminées dans le cadre de l'audit sont liées aux résultats de l'appréciation des risques et du processus de traitement des risques, et peuvent ultérieurement être reliées à la politique et aux objectifs de sécurité de l'information.

NOTE L'Annexe A donne des recommandations relatives aux pratiques d'audit de SMSI, y compris à la manière dont le SMSI doit être audité à l'aide des informations documentées applicables.

6.4.7 Recueil et vérification des informations

6.4.7.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.7 s'appliquent. En outre, les recommandations de 6.4.7.2 s'appliquent.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

6.4.7.2 Les méthodes possibles de recueil d'informations pertinentes au cours de l'audit comprennent:

a) l'examen des informations documentées (y compris les journaux d'ordinateur et les données de configuration);

https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020

b) la visite des installations de traitement de l'information;

c) l'observation des processus de SMSI et des mesures associées;

d) l'utilisation d'outils d'audit automatisés.

NOTE 1 L'Annexe A fournit des recommandations sur la manière d'auditer les processus de SMSI.

NOTE 2 L'ISO/IEC TS 27008 fournit des recommandations supplémentaires sur la manière d'évaluer les mesures de sécurité de l'information.

Il convient que les membres de l'équipe d'audit de SMSI s'assurent que toutes les informations reçues des audités conformément à l'accord passé entre le client de l'audit, l'équipe d'audit et l'audité sont traitées correctement.

6.4.8 Production de constatations d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.8 s'appliquent.

6.4.9 Détermination des conclusions d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.9 s'appliquent.

6.4.10 Conduite de la réunion de clôture

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.4.10 s'appliquent.

© ISO/IEC 2020 – Tous droits réservés

6.5 Préparation et diffusion du rapport d'audit

6.5.1 Préparation du rapport d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.5.1 s'appliquent.

6.5.2 Diffusion du rapport d'audit

6.5.2.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.5.2 s'appliquent. En outre, les recommandations de 6.5.2.2 s'appliquent.

6.5.2.2 NOTE

NOTE Si un moyen électronique de diffusion du rapport d'audit est utilisé, un chiffrement approprié est une des mesures possibles à employer pour satisfaire aux exigences de confidentialité.

6.6 Clôture de l'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.6, s'appliquent.

6.7 Réalisation du suivi d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 6.7, s'appliquent.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

7 Compétence et évaluation des auditeurs

7.1 Généralités

ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5a0c46de-7ec0-481d-af13-ed347cfa203f/iso-iec-27007-2020

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.1, s'appliquent.

7.2 Déterminer la compétence d'un auditeur

7.2.1 Généralités

7.2.1.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.1 s'appliquent. En outre, les recommandations de 7.2.1.2 s'appliquent.

7.2.1.2 Il convient de tenir compte des points suivants pour déterminer les connaissances et aptitudes appropriées d'un auditeur de SMSI:

a) la complexité du SMSI (par exemple la criticité des systèmes d'information dans le domaine d'application du SMSI, les résultats d'appréciation des risques du SMSI);

b) le(s) type(s) d'activité(s) exécutée(s) dans le cadre du SMSI;

c) l'étendue et la diversité des technologies utilisées pour l'utilisation des différents composants du SMSI (telles que les mesures mises en œuvre, les informations documentées et/ou les contrôles de procédés, les plates-formes technologiques et les solutions en jeu, etc.);

d) les performances précédemment démontrées du SMSI;

e) l'étendue de l'externalisation et des accords tiers utilisés dans le domaine d'application du SMSI;

f) les normes, exigences juridiques et autres exigences pertinentes pour le programme d'audit.

© ISO/IEC 2020 – Tous droits réservés

7.2.2 Comportements personnels

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.2 s'appliquent.

7.2.3 Connaissances et aptitudes

7.2.3.1 Généralités

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.3.1 s'appliquent.

7.2.3.2 Connaissances et aptitudes générales des auditeurs de systèmes de management

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.3.2 s'appliquent.

7.2.3.3 Compétence des auditeurs spécifique à la discipline et au secteur

7.2.3.3.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.3.3 s'appliquent. En outre, les recommandations du 7.2.3.3.2 s'appliquent.

7.2.3.3.2 Il convient que les auditeurs de SMSI soient également capables de comprendre les exigences métier applicables.

7.2.3.4 Compétence générale du responsable d'une équipe d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.3.4 s'appliquent.

7.2.3.5 Connaissances et aptitudes nécessaires à l'audit de plusieurs disciplines

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.3.5 s'appliquent.

7.2.4 Acquérir la compétence d'auditeur

7.2.4.1 Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.4 s'appliquent. En outre, les recommandations de 7.2.4.2 s'appliquent.

7.2.4.2 Il convient que les auditeurs de SMSI aient des connaissances et des compétences en matière de technologie de l'information et de sécurité de l'information, démontrées par exemple sur la base de certifications applicables (par exemple habilités conformément à l'ISO/IEC 17024). Il convient que l'expérience professionnelle des auditeurs individuels de SMSI contribue également au développement de leurs connaissances et des compétences dans le domaine d'application du SMSI.

NOTE Des informations complémentaires concernant la certification des auditeurs de SMSI se trouvent dans l'ISO/IEC 27006.

7.2.5 Acquérir la compétence de responsable d'équipe d'audit

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.2.5 s'appliquent.

7.3 Déterminer les critères d'évaluation des auditeurs

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.3, s'appliquent.

7.4 Choisir la méthode d'évaluation des auditeurs appropriée

Les lignes directrices spécifiées dans l'ISO 19011:2018, 7.4, s'appliquent.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27007:2020
https://standards.iteh.ai/catalog/standards/sist/5abc4bdc-1ec6-481d-af13-ed347cfa203f/iso-iec-27007-2020