Dispositif particulier

Certification «Lead Auditor ISO/IEC 27001»

Révision 2022

Table des matières

1. Description de la certification « Lead Auditor ISO/IEC 27001» - Révision 2022

1.1 Intitulé et durée de la certification

Lead Auditor ISO/IEC 27001 – Révision 2022 est délivré par Bestscertifs en application des exigences de la norme ISO/IEC 17024 : 2012 Évaluation de la conformité — Exigences générales pour les organismes de certification procédant à la certification de personnes.

Cette certification est délivrée pour une durée de 3 ans.

1.2 Objectif de la certification

L'objectif principal de cette certification est de valider les compétences des professionnels capables de préparer la démarche d'audit d'un système de management de la sécurité de l'information d'une organisation selon la norme NF EN ISO/IEC 27001 : 2017 « Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences » , de conduire un audit interne et externe en conformité avec cette norme et de mettre en œuvre les principes, procédures et techniques reconnus et documentés par les normes ISO/CEI 19011 et ISO/CEI 27006.

1.3 Périmètre de la certification

Les pirates du Net sont de plus en plus nombreux et s'attaquent à tous types d'entreprises quelque soient leur taille, mais également aux structures publiques, hôpitaux, tribunaux, ministères, …

Entre janvier et septembre 2020, l'industrie, les collectivités territoriales et la santé ont été les secteurs d'activité les plus affectés par les attaques par rançongiciels traités par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)[1].

La norme NF EN ISO/IEC 27001 : 2017 Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences s'adresse à tous les types d'organismes (entreprises commerciales, ONG, administrations…) et définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels de l'organisme. L'objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. Cela apportera la confiance des parties prenantes.

La norme précise que les exigences en matière de mesures de sécurité doivent être adéquates et proportionnées aux risques encourus et donc ne pas être ni trop laxistes ni trop sévères.

1 François Durety – sous-directeur des opérations de l'ANSSI – communiqué de presse du 01/10/2020

La norme NF EN ISO/IEC 27001 : 2017 énumère un ensemble de points de contrôle à respecter pour s'assurer de la pertinence du SMSI, permettre de l'exploiter et de le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002 (anciennement ISO/CEI 17799), classées dans 14 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de faire certifier un organisme ISO/IEC 27001.

Dans ce cadre, la mission d'auditeur devient déterminante pour anticiper et réduire les risques. Cette mission d'auditeur peut être confiée à un collaborateur interne à l'entreprise ou externe (cabinet conseil).

1.4 A qui s'adresse cette certification

Public Visé :

- Professionnels et/ou Auditeurs de la Sécurité de l'Information souhaitant acquérir une certification attestant qu'ils sont capables de préparer ou réaliser des audits internes et/ou externes de conformité avec la norme NF EN ISO/IEC 27001 : 2017 « Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences ».
- Auditeurs et Responsables d'Audit souhaitant acquérir une certification reconnue en tant qu'auditeur en conformité avec la norme NF EN ISO/IEC 27001 : 2017 « Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences ».
- Consultants souhaitant une certification prouvant qu'ils sont capables de maîtriser le processus d'audit du Système de Management de la Sécurité de l'Information (SMSI) en conformité avec la norme NF EN ISO/IEC 27001 : 2017 « Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences ».
- Toute personne, quel que soit son poste dans l'entreprise en relation avec le Système de Management de la Sécurité de l'Information (SMSI), désireuse d'évoluer vers des responsabilités d'auditeur en conformité avec la norme NF EN ISO/IEC 27001 : 2017 « Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences ».

1. 5 Candidature à la certification et l'examen

Pour candidater à la certification il sera demandé :

- De compléter le formulaire de candidature disponible sur la page de description de la certification sur le site www.bestcertifs.com
- De téléverser un CV justifiant d'une expérience d'au moins trois ans dans la gestion des systèmes d'information et métiers rattachés au système d'information

- De fournir une attestation de réalisation dans les 2 dernières années de 10 jours d'audit correspondant à un ou plusieurs audits de systèmes de management dans le domaine IT, ou d'évaluation des risques IT, ou d'audit de système de management de la sécurité de l'information ou tout périmètre approchant
- De téléverser un fichier numérisé d'une pièce d'identité légale en cours de validité comprenant une photo, les nom prénom et date de naissance, rédigée en alphabet latin ; cette pièce sera la pièce demandée pour la vérification de l'identité lors du passage de l'Examen de certification (carte d'identité, passeport, permis de conduire …). A défaut, le numéro de passeport/carte d'identité et le nom et prénom du candidat.
- Le cas échéant, le candidat pourra demander une adaptation de l'Examen en cas de handicap: il en fait la demande dans dossier de candidature. Les demandes seront traitées au cas par cas.

Pour candidater à l'examen, vous pouvez passer par un organisme de formation qualifié qui prépare aux examens de la certification ou réaliser vous même votre inscription sur le site de bestcertifs. Pour passer cet examen, nous vous conseillons néanmoins d'être titulaire d'un diplôme de niveau minimum Bac+2.

1.6 Règles d'usage de la certification

Validité – Eléments figurant sur le certificat – Suspension et retrait – Abandon du certificat- Réduction du périmètre de la certification Voir Procédure de certification paragraphe 5.3. : ici

1.7 Candidature pour le renouvellement de la certification

Pour candidater au renouvellement, il faudra produire les éléments suivants :

- De compléter le formulaire de candidature disponible sur la page de description de la certification sur le site de bestcertifs
- De fournir une attestation de réalisation dans les 2 dernières années de 10 jours d'audit correspondant à un ou plusieurs audits de systèmes de management dans le domaine IT, ou d'évaluation des risques IT, ou d'audit de système de management de la sécurité de l'information ou tout périmètre approchant
- De téléverser un fichier numérisé d'une pièce d'identité légale en cours de validité comprenant une photo, les nom prénom et date de naissance, rédigée en alphabet latin ; cette pièce sera la pièce demandée pour la vérification de l'identité lors du passage de l'Examen de certification (carte d'identité, passeport, permis de conduire …). A défaut, le numéro de passeport/carte d'identité et le nom et prénom du candidat.

Le renouvellement se fait pour une période de 3 ans.

1. 8 Missions, tâches, compétences, critères d’évaluation

La réalisation de la certification est le résultat d’un travail d’ingénierie de formation qui part de la description des activités et tâches réalisées par un professionnel en charge de l’audit du système de management de l’information de l’entreprise.

Activités, tâches compétences

Activités	Tâches	Compétences
A1 - Concevoir un audit du Système de Management de la Sécurité de l'Information en ayant une approche holistique, qui permette une analyse ciblée et précise	Ca1.1 – Identifier les parties prenantes qui vont être mobilisées pour vérifier le Système de Management de la Sécurité de l'Information (SMSI).	C.1, C.2, C.3, C.4
	Ca1.2 – Caractériser les menaces qui pèsent sur le système d'information, en prenant en considération les aspects humains, organisationnels et technologiques pour cibler le périmètre d'audit interne et/ou externe.	
	Ca1.3 – Analyser la documentation et les processus de l'entreprise afin d'identifier les faiblesses liées à la sécurité de l'information	
	Ca1.4 – Cartographier les risques pour identifier les points de contrôle à réaliser pendant l'audit	
	Ca1.5 – Concevoir le mode opératoire, les actions à réaliser pour définir le plan d'audit	
	Ca1.6 Composer une équipe d'audit pluridisciplinaire pour optimiser la mobilisation des parties prenantes	
A2 -Réaliser un audit en mobilisant les parties prenantes et en explorant les preuves disponibles pour identifier des actions correctives	Ca2.1 – mettre en œuvre la communication auprès des parties prenantes pour préparer les équipes et gagner en efficacité	C5, C6, C7
	Ca2.2 – Réaliser les entretiens d'audits	
	Ca2.3 – Questionner pour approfondir l'exploration des éléments fournis	
	Ca2.4 – Elaborer un système de mesure pour permettre la collecte et l'analyse des données d'audit	
	Ca2.5 – Examiner les éléments de preuve afin d'identifier les écarts et les risques éventuels	
	Ca2.6 – Identifier des actions correctives pour réduire les écarts et les risques	
A 3 – Elaborer un rapport final qui priorise les actions à réaliser et favorise l'engagement des parties prenantes pour clôturer l'audit	Ca3.1 – Concevoir un rapport final d'audit pour donner une vision synthétique de la situation	C8
	C3.2 – Prioriser les actions correctives pour proposer une chronologie dans la mise en œuvre	
	C3.3 – Discuter de l'analyse et des préconisations avec les parties prenantes pour valider les actions à réaliser	
A 4 – Apprécier la mise en œuvre et le niveau de réalisation des actions pour pérenniser les résultats obtenus	Ca4.1 Contrôler la mise en œuvre et le niveau de réalisation des actions pour pérenniser les résultats obtenus	C9

Compétences	**Critères d'évaluation**
C1. Caractériser les menaces et vulnérabilités qui pèsent sur le système d'information de l'organisation, en prenant en considération les aspects humains, organisationnels et technologiques pour cibler le périmètre d'audit interne ou externe selon NF EN ISO/IEC 27001 : 2017	Cr1. Différencie vulnérabilité et menace (annexe D de la 27005) Identifie les vulnérabilités et les menaces en lien avec le secteur d'activité du client (annexe D de la 27005)
C2. Identifier les risques pertinents en analysant la documentation et les processus de l'entreprise afin de définir les points de contrôles de l'audit selon NF EN ISO/IEC 27001 : 2017	Cr2. Identifie les risques liés au système de sécurité de l'information du client, en lien avec les vulnérabilités et les menaces préalablement identifiés Identifie les risques liés à la mise en place de l'audit chez le client Le schéma de synthèse des risques matérialise les points critiques comme les non conformités majeures et mineures potentielles Les documents analysés sont en conformité avec la norme ISO/CEI 27001
C3. Composer une équipe d'audit pluridisciplinaire en fonction du périmètre et des points de contrôles définis afin de réaliser un audit selon la norme ISO 19011	Cr3. Identifie les compétences nécessaires à la création d'audit (compétences d'un auditeur – ISO 19011) Détecte les conflits d'intérêt au sein d'une équipe (ISO 19011) Définit les rôles de chaque membre de l'équipe (liste de rôles ISO 19011)
C4. Concevoir un plan et un programme d'audit en s'appuyant sur les outils et méthodes d'audit pertinents selon ISO 19001 afin d'optimiser la mobilisation des parties prenantes	Cr4. Les parties prenantes sont choisies de façon pertinente, clairement associées aux points de contrôles à effectuer, en cohérence avec leur rôle dans l'entreprise Le plan est formalisé, chaque participant connaît son rôle et les attentes Définit l'approche pour réaliser l'audit Sélectionne les techniques et outils à intégrer dans l'audit (ISO/CEI19011) Créé un plan d'audit (ISO 19011 – 27007 -27008)
C5. Mettre en œuvre le plan d'audit en contrôlant systématiquement les preuves disponibles pour identifier les écarts et les risques liés au système d'information	Cr5. Crée un plan de test d'audit Élabore les méthodes d'audit à utiliser pour chaque situation. Détermine la technique d'échantillonnage adaptée à la situation (19011)
C6. Mettre en œuvre des outils de communication et d'audit pertinents en s'appuyant sur la norme ISO 19011 avant, pendant et après l'audit afin de garantir la qualité de la	Cr6. Sélectionne le canal d'information adapté aux différentes cibles (canaux écrits oraux, formels informels) Adapte l'information aux différentes cibles (liste de parties

prestation d'audit	prenantes / types d'info) Identifie les éléments clés à mettre dans le compte rendu de réunion (point attendus 3 réunion d'audit 19011) Définit les étapes nécessaires à la réalisation de l'entretien d'audit (ISO 19011) Reformule et synthétise l'entretien Applique les techniques de questionnement Alterne les types de question Utiliser les 7 types de preuves disponibles lors d'un audit de conformité pour corroborer les informations. Évalue les résultats des tests par échantillons (donner trois analyses par échantillon) Analyse la cohérence des résultats des tests par échantillon par rapport aux référentiels
C7. Identifier et apprécier les non conformités pour proposer des actions correctives en conformité avec la norme NF EN ISO/IEC 27001 : 2017	Cr7. Apprécie le degré de la non-conformité (majeure – mineure) Formalise un rapport de non-conformité Propose des actions correctives pertinentes parmi les 114 mesures liées à la sécurité de l'information en conformité avec la norme NF EN ISO/IEC 27001 : 2017
C8. Formaliser ses recommandations dans un rapport final en priorisant les actions à mener afin de favoriser l'engagement des parties prenantes	Cr8. Définit l'ordre des actions à mettre en œuvre en fonction de l'importance de la non-conformité Le rapport d'audit de surveillance est structuré en lien avec la norme 19011
C9. Contrôler la mise en œuvre et le niveau de réalisation des actions pour pérenniser les résultats obtenus	Cr9. Le plan de suivi des actions et de relance est focalisé sur la confirmation des bénéfices, leur mesure et leur contrôle permanent

1.9 Modalités de l'examen initiale et de renouvellement

L'examen initial est réalisé par le passage de 2 questionnaires à choix multiples relatives à la mise en place d'un audit des Systèmes de Management de la Sécurité de l'Information sur une plateforme LMS BESTCERTIF (https://exam.bestcertifs.com/) en mode supervisé par un surveillant :

1. Un questionnaire de 30 questions se rapportant aux connaissances

2. Un questionnaire de 50 questions se rapportant à une étude de cas complexe qui portera sur une entreprise et présentera le contexte spécifique, les particularités de l'entreprise, les enjeux et tous les éléments détaillés de l'entreprise

L'évaluation se fait à distance selon les modalités décrites dans la Procédure de Certification au paragraphe 4.3. 1 Méthode d'évaluation

Durée : 2h00

Score minimum : obtenir 56 points sur 80

L'examen de renouvellement est réalisé par le passage d'un questionnaire à choix multiples relatif à la mise en place d'un audit des Systèmes de Management de la Sécurité de l'Information sur une plateforme LMS BESTCERTIF (https://exam.bestcertifs.com/)

L'évaluation se fait à distance selon les modalités décrites dans la Procédure de Certification au paragraphe 4.3. 1 Méthode d'évaluation

Durée : 1h00

Score minimum : obtenir 35 points sur 50

Le processus de re-certification peut prendre jusqu'à un mois.

1.10 Coût de la certification et du renouvellement

Le prix de la certification s'élève à 399 euros et son renouvellement à 175 euros

2. Procédure de certification

Voir la procédure de certification sur le site https://www.bestcertifs.com/ et en cliquant ici