Dispositif particulier

Certification «Lead Implementer ISO/IEC 27001»

Table des matières

1. Description de la certification « Lead Implementer ISO/IEC 27001»

1.1 Intitulé et durée de la certification

Lead Implementer ISO/IEC 27001 est délivré par Bestcertifs en application des exigences de la norme NF EN 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 d'élaborer et mettre en œuvre 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 » qui tienne compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation.

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(fr) 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.

L'ISO/IEC 27001 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 NF EN ISO/IEC 27001:2017.

Dans ce cadre, la mission des managers qui élaborent et mettent en œuvre les système sde management de la sécurité de l'information devient déterminante pour anticiper et réduire les

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

risques. Cette mission 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 de la Sécurité de l'Information souhaitant attester qu'ils sont capables de préparer ou réaliser des projets d'implémentation de systèmes de gestion de la sécurité de l'information 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 ».

• Chefs de projets souhaitant acquérir une certification reconnue dans le domaine de l'implantation d'un système de gestion de la sécurité de l'information 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 désirant certifier qu'ils maîtrisent le processus d'implémentation 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 de mise en œuvre d'un système de 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 ».

1. 5 Candidature à la certification et à 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 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 son 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’usages 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 : cliquez ici

1.7 Candidature au 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 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 de la mise en place d’un système de management du système d’information de l’entreprise.

Activités, tâches compétences

Activités	Tâches	Compétences
Réaliser un diagnostic de la situation en termes de sécurité de l'information de l'entreprise, afin de définir les objectifs du projet de mise en œuvre d'un SMSI	Recueillir et analyser les informations sur l'existant (identifier les parties prenantes et les exigences).	C1. Collecter et analyser les données existantes en s'appuyant sur la documentation et les personnes ressources afin de mesurer la maturité de l'entreprise concernant la sécurité de l'information
	Identifier le périmètre du projet	C2. Définir les objectifs du système de management de la sécurité de l'information en s'appuyant sur la norme ISO 27001 afin de préciser le périmètre du projet de mise en oeuvre
	Définir les objectifs et l'approche de mise en œuvre en alignement avec la stratégie de l'organisation.	C3. Formaliser le domaine d'application, l'approche et le business case en vue de permettre la décision du lancement du projet en cohérence avec la stratégie de l'organisation
	Identifier le domaine d'application et formaliser le périmètre du projet.	
	Créer un cas d'affaire	
Définir et planifier l'ensemble des activités nécessaires à l'implémentation du SMSI afin obtenir l'approbation de la direction de l'entreprise	Création de l'équipe projet en définissant tous les rôles et responsabilités.	C4. Constituer une équipe projet en définissant les rôles et responsabilités afin d'optimiser la mise en œuvre du projet de SMSI
	Création du plan de projet pour l'implémentation du SMSI incluant les plans pour le traitement de toutes les vulnérabilités.	C5. Concevoir un plan de projet d'implémentation du SMSI en s'appuyant sur les parties prenantes du projet afin de garantir le succès de sa mise en œuvre
	Création de la politique de Sécurité de l'information et formalisation de la déclaration d'applicabilité pour valider le démarrage de la réalisation de la mise en œuvre	C6. Elaborer la politique de sécurité de l'information et la déclaration d'applicabilité en prenant en compte les contraintes de l'organisation afin d'obtenir l'approbation de la direction
Implémenter le SMSI en Coordonnant l'ensemble des parties prenantes afin d'atteindre les objectifs ciblés	Mise en œuvre de la nouvelle organisation humaine (rôles) pour répondre aux besoins du SMSI.	C7. Mettre en œuvre le plan de projet en créant, documentant et implémentant les dispositifs et mesures de sécurité spécifiques pour augmenter la maturité de l'entreprise concernant la sécurité de l'information
	Création, documentation et mise en œuvre des politiques d'utilisation spécifiques du SMSI	
	Conception et création et implémentation des procédures spécifiques et des mesures pour répondre aux vulnérabilités du système d'information	
	Communication et accompagnement de l'organisation pour la sensibilisation et la formation de toutes les parties prenantes au SMSI	C8. Informer, sensibiliser et former toutes les parties prenantes du SMSI en s'appuyant sur des actions de communication et de formation afin d'atteindre les objectifs ciblés
Mettre en œuvre une démarche d'amélioration continue afin de garantir le niveau de performance du SMSI	Identifier, créer et mettre en œuvre les indicateurs pour suivre et maintenir les performances du SMSI	C9. Mettre en œuvre une démarche de contrôle et d'amélioration continu du SMSI afin de garantir le niveau de performance du SMSI requis pour l'obtention de la certification ISO 27001.
	Mise en place et support des Revues de Direction pour maintenir les performances du SMSI	
	Identifier et définir les plans d'actions pour traiter les non-conformités	
	Suivi et contrôle de la gestion des changement vis-à-vis du SMSI.	
	Réaliser des audits internes pour préparer garantir un haut niveau de performance du SMSI et préparer la certification.	

Référentiels de compétences et d'évaluation

Compétences	**Critères d'évaluation**
C1. Collecter et analyser les données existantes en s'appuyant sur la documentation obligatoire et non obligatoire de l'entreprise et des entretiens de personnes ressources telles que définis dans l'ISO 27001 afin établir un état des lieux concernant la sécurité de l'information	Cr1. Les informations collectées sont pertinentes : elles sont factuelles et documentées ; elles s'appuient sur les recommandations de la norme. L'analyse de l'existant est contextualisée : elle s'appuie sur les données collectées ; elle propose des axes de progrès spécifiques en matière de système de management de la sécurité de l'information
C2. Définir les objectifs du système de management de la sécurité de l'information en s'appuyant sur l'état des lieux réalisés et la norme ISO 27001 afin de préciser le périmètre du projet de mise en oeuvre	Cr2. Les objectifs sont réalistes : ils sont mesurables, évaluables, reliés aux exigences et aux mesures de la norme ISO 27001.
C.3 Formaliser le domaine d'application et le business case en utilisant une approche projet établie en vue de permettre la décision de lancement du projet de mise en œuvre	Cr3. Le domaine d'application est défini : son périmètre est établi, il tient compte des objectifs définis, il a été accepté par les parties prenantes principales Le business case est complet : les risques majeurs sont identifiés, l'évaluation des investissements est réaliste, les liens avec la stratégie de l'organisation sont clairement identifiés, l'approche utilisée est adaptée aux capacités de l'entreprise
C4. Constituer une équipe projet en définissant les rôles et responsabilités en lien avec la norme afin d'optimiser la mise en œuvre du SMSI	Cr4. La composition de l'équipe est cohérente : l'ensemble des rôles et responsabilités nécessaires à la mise en place des exigences du projet SMSI sont définis ; les personnes sélectionnées ont les compétences requises par rapport aux profils définis.
C5. Concevoir un plan de projet d'implémentation du SMSI en s'appuyant sur les parties prenantes du projet afin de garantir le succès de sa mise en œuvre	Cr5. Le plan de projet est réaliste et détaillé : les activités sont décrites au bon niveau de précision ; les moyens et les risques sont évalués ; les coûts, délais et le périmètre sont définis et cohérents
C6. Elaborer la politique de sécurité de l'information et la déclaration d'applicabilité en prenant en compte les contraintes de l'organisation afin d'obtenir l'approbation de la direction	Cr6. La Politique de sécurité est complète : elle tient compte des enjeux de l'organisation et de ses objectifs. La Déclaration d'applicabilité est complète : elle comporte tous les éléments attendus par la norme. L'ensemble des documents sont validés formellement (signature).
C7. Mettre en œuvre le plan de projet en créant, documentant et implémentant les dispositifs, l'organisation et les mesures de sécurité spécifiques pour augmenter la maturité de l'entreprise concernant la sécurité de l'information	Cr7. Les dispositifs, l'organisation et les mesures de sécurité mis en place sont adaptés : ils réduisent les vulnérabilités, ils sont documentés et décrits ; les processus sont créés et validés par les responsables identifiés pour chaque processus conformément au plan de projet.
C8. Faciliter l'appropriation du SMSI en s'appuyant sur une démarche d'accompagnement au changement afin d'obtenir l'engagement des parties prenantes	Cr8. Le plan d'action d'accompagnement au changement est complet et adapté : il comprend des actions de communication ou de sensibilisation ou de formation ; il s'appuie sur une

	documentation du SMSI accessible à toutes les parties prenantes de l'organisation et intégré aux processus de l'entreprise Les actions d'accompagnement sont adaptées aux besoins définis des bénéficiaires. Les objectifs d'accompagnement sont atteints.
C9. Mettre en œuvre une démarche de contrôle et d'amélioration continu du SMSI afin de garantir le niveau de performance du SMSI souhaité	Cr9. La démarche de contrôle et d'amélioration est robuste. Elles s'appuient sur la norme et des outils adaptés constitués de : revue de direction, plan d'action pour traiter les non conformités, suivi des changements, audits internes…

1.9 Modalités de l'examen initial 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 .