

Audit de systèmes de management de la sécurité de l'information (ISO/CEI 27001 Lead Auditor)

RS6243 · RS · Publiée

L'essentiel

Code(s) NSF	326p
Formacode(s)	31006, 31038
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	25/01/2023
Date d'échéance	25/01/2026

Certificateur(s)

SKILLS4ALL · SIRET : 82815451800025

SKILLS4ALL · SIRET : 82815451800017

Partenaires habilités

2 organismes habilités, d'après la liste publiée par France compétences : 2 à former.

Organisme	SIRET	Habilitation
HS2	84050153000017	Former
OO2	53157067900039	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

Afin de garantir la sécurité des systèmes de l'information, les entreprises sont amenées à mettre en place un système de management de la sécurité de l'information conforme à la norme ISO 27001.

Pour contrôler la bonne mise en œuvre de cette conformité au sein des organisations, la certification "Audit de systèmes de management de la sécurité de l'information (ISO/CEI 27001 Lead Auditor)" permet aux professionnels évoluant dans le domaine de la sécurité de l'information ou ayant déjà réalisé des audits d'attester :

- qu'ils possèdent les connaissances et compétences complémentaires, nécessaires à la pratique de l'audit de systèmes de management de la sécurité de l'information conformes à la norme ISO/CEI 27001 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences », en tant que membre d'équipe d'audit ou seul
- et qu'ils possèdent le savoir-faire et les qualités personnelles nécessaires à la conduite d'un audit, définies dans la norme ISO/CEI 19011 « Lignes directrices pour l'audit des systèmes de management » et dans les guides associés (ISO, IAF, EA).

Les activités en lien avec cette certification sont :

- Concevoir un audit du Système de Management de la Sécurité de l'Information avec une approche holistique, qui permette une analyse ciblée et précise
- Réaliser un audit en mobilisant les parties prenantes et en explorant les preuves disponibles pour identifier des actions correctives
- Élaborer un rapport final qui priorise les actions à réaliser et favorise l'engagement des parties prenantes
- Apprécier la mise en œuvre et le niveau de réalisation des actions pour pérenniser les résultats obtenus

COMPÉTENCES ATTESTÉES

- 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 selon ISO 27001
- C2. Déterminer les risques en analysant la documentation et les processus de l'organisation afin de définir les points de contrôles de l'audit selon ISO 27001
- C3. Composer une équipe d'audit pluridisciplinaire en fonction du périmètre et des points de contrôles définis afin de réaliser un audit conforme à la norme ISO 19011
- C4. Concevoir un plan d'audit en s'appuyant sur les outils et méthodes d'audit pertinents selon ISO 19011, ISO 27007 et 27008 afin de couvrir l'ensemble des activités du périmètre d'audit
- C5. Identifier et apprécier les non conformités en mettant en œuvre le plan d'audit et en utilisant les outils de communication et d'audit pertinents pour proposer des actions correctives en conformité avec la norme ISO 27001
- C6. Formaliser ses recommandations dans un rapport final en priorisant les actions à mener afin de favoriser l'engagement des parties prenantes
- C7. Établir un plan de suivi des actions en s'appuyant sur le rapport final afin de contrôler la mise en œuvre et le niveau de réalisation des actions

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Connaissance générale de la sécurité des systèmes d'information et une expérience des audits sont fortement recommandés.

Le candidat

devra fournir obligatoirement :

- un CV justifiant d'une expérience d'au moins trois ans dans la gestion des systèmes d'information dont au moins 1 an en tant que participant à un projet de mise en place ou de maintien d'un système de management de la sécurité de l'information et cela dans les 5 dernières années.
- ET une attestation de réalisation dans les 2 dernières années de 10 jours d'audit entiers correspondant à deux audits de systèmes de management

COMPOSITION DU JURY — FORMATION CONTINUE, CANDIDATURE INDIVIDUELLE

Le jury est constitué d'au moins trois personnes :

- Le Responsable de la Certification de l'organisme certificateur Skills4All
- Deux professionnels extérieurs à Skills4All dont la qualité est en lien avec la certification visée. Ces deux professionnels ne sont pas en lien ni personnel ni professionnel avec le candidat. Le président du Jury doit être choisi parmi ces deux professionnels extérieurs à Skills4All.

Base légale

Date de décision	25/01/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	25/01/2026
Date de dernière délivrance possible	25/07/2026

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RS7478

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.skills4all.com/certification/iso-27001-lead-auditor-formation/>

Fiche officielle (France Compétences)

Entrées et sorties de formation

Entrées en formation	103
Parcours menés à terme	100
Taux d'achèvement	97 %
Période	05/2023 – 05/2026

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	111
Montant total engagé	259 762 €
Coût moyen par dossier	2 340 €
Durée moyenne	35 h
Période	02/2023 – 12/2025
France compétences	91 %
Reste à charge titulaire	6 %
France Travail	2 %
Entreprise	0 %
OPCO	0 %
Compte d'engagement citoyen	0 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.