

Mettre en œuvre le système de management de la sécurité de l'information (SMSI) selon la norme ISO/CEI 27001

RS7586 · RS · Publiée

L'essentiel

Code(s) NSF	326m
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	29/05/2026
Date d'échéance	29/05/2029

Certificateur(s)

PECB FRANCE · SIRET : 90871310000018

Partenaires habilités

48 organismes habilités, d'après la liste publiée par France compétences : 43 à former et organiser l'évaluation et 5 à former.

Organisme	SIRET	Habilitation
ACG CYBERSECURITY	85024706500012	Former et organiser l'évaluation
ADENIUM-BRG	44195184500086	Former et organiser l'évaluation
AELION	53410337900028	Former et organiser l'évaluation
ALMOND	84105955300039	Former et organiser l'évaluation
AMBIENT IT	81227101300045	Former et organiser l'évaluation
ATOS DIGITAL SECURITY	81057051500140	Former et organiser l'évaluation
BARDIN CONSULTING	92405071900013	Former et organiser l'évaluation
BCIT FORMATION	91244387600038	Former
BSSI	84370069100010	Former et organiser l'évaluation
CERTYOU	80450946100013	Former et organiser l'évaluation

Liste complète des 48 partenaires habilités : <https://data.aktaconseil.fr/certifications/rs7586-mettre-en-oeuvre-le-systeme-de-management-de-la-securite-de-l-information-smsi-selon-la-norme-iso-cei-27001/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Objectifs de la certification

La certification PECB « Mettre en œuvre le système de management de la sécurité de l'information selon la norme ISO/CEI 27001 » atteste des compétences nécessaires pour planifier, mettre en œuvre, gérer, surveiller et maintenir efficacement un système de management de la sécurité de l'information (SMSI) conforme aux exigences de la norme internationale ISO/CEI 27001. Cette certification s'adresse à des professionnels expérimentés qui souhaitent acquérir

une expertise opérationnelle complémentaire à leur fonction principale, leur permettant de structurer et de piloter des projets de déploiement de SMSI dans des contextes organisationnels variés.

Elle vise spécifiquement les responsables de la mise en œuvre et de la gestion du système de gestion de la sécurité de l'information (SGSI), les responsables ou consultants souhaitant préparer et accompagner une organisation dans la mise en œuvre d'un SGSI, les chefs de projet, consultants ou conseillers experts cherchant à maîtriser la mise en œuvre et la gestion du SGSI, les responsables du maintien de la conformité des exigences du SGSI au sein d'une organisation, ainsi que les professionnels du domaine de la gestion de la sécurité de l'information.

Contexte et finalité professionnelle

Dans un environnement numérique où les menaces cybersécuritaires évoluent rapidement et où la conformité réglementaire devient un enjeu stratégique majeur, les organisations ont besoin de professionnels capables de traduire les exigences normatives en actions concrètes et opérationnelles. Cette certification répond aux besoins du marché en formant des experts capables d'accompagner les entreprises dans la structuration de leur sécurité informationnelle.

Elle s'adresse particulièrement aux professionnels intervenant dans les entreprises de services numériques, les organismes de conseil en IT, les entreprises de conseil en management des risques, ou les services informatiques de tout type d'organisation. La certification constitue une compétence complémentaire stratégique qui permet aux professionnels d'élargir leur périmètre d'intervention et de répondre aux appels d'offres nécessitant une expertise certifiée en mise en œuvre de SMSI, tout en renforçant leur capacité à accompagner les organisations dans leur transformation numérique sécurisée.

Positionnement dans l'environnement professionnel

La certification s'inscrit dans une logique de spécialisation progressive et constitue un levier d'évolution pour des professionnels déjà en poste souhaitant étendre leurs responsabilités dans le domaine de la sécurité de l'information. Elle permet de répondre aux exigences croissantes du marché en matière de mise en œuvre de systèmes de management de la sécurité conformes aux standards internationaux, d'accompagner les organisations dans leurs démarches de certification ISO/CEI 27001, et de structurer des projets de transformation numérique sécurisée. Le périmètre ciblé est celui d'une compétence complémentaire opérationnelle et contextualisée, directement mobilisable sur le marché du travail pour des missions de conseil, de mise en œuvre ou de pilotage de projets SMSI.

COMPÉTENCES ATTESTÉES

- Identifier les éléments clés d'un système de management de la sécurité de l'information (SMSI), en analysant le contexte organisationnel et en inventoriant les menaces potentielles, les vulnérabilités, les processus opérationnels critiques, les actifs informationnels, la confidentialité, l'intégrité, la disponibilité, les risques associés, les contrôles et les cadres réglementaires applicables, afin de structurer sa mise en œuvre conformément à la norme ISO/IEC 27001.
- Traduire les exigences de la norme ISO/IEC 27001 en actions concrètes en analysant les clauses et contrôles applicables de la norme afin de planifier le déploiement du système de management de la sécurité de l'information (SMSI) en fonction du contexte organisationnel.
- Structurer le projet de mise en œuvre du SMSI en définissant le périmètre, les objectifs, les responsabilités et le contexte organisationnel incluant l'accessibilité pour les personnes en situation de handicap afin d'encadrer le déploiement du système de management de la sécurité de l'information conformément à la norme ISO/CEI 27001.
- Exécuter le plan de mise en œuvre du système de management de la sécurité de l'information en mobilisant les ressources définies, en établissant les responsabilités et en suivant les étapes prévues en optimisant la consommation énergétique des équipements et infrastructures afin d'assurer un déploiement structuré et conforme aux exigences de la norme ISO/CEI 27001 dans une démarche de durabilité environnementale.
- Mettre en œuvre les processus opérationnels du SMSI en élaborant les procédures documentées, en instaurant une politique de gestion des incidents, en constituant une équipe de réponse, et en déployant des programmes de formation et de sensibilisation à la sécurité de l'information adaptés à tous les collaborateurs, y compris les personnes en situation de handicap et des plans de communication afin de renforcer la maturité de l'organisation en matière de sécurité de l'information conforme aux exigences de la norme ISO/CEI 27001.
- Contrôler les performances du SMSI conformément à la norme ISO/CEI 27001 en suivant des indicateurs et en évaluant les résultats afin de vérifier son efficacité et son alignement avec les objectifs de l'organisation.
- Mettre en œuvre un processus d'amélioration continue et analyser les causes profondes des non-conformités en intégrant l'évaluation de l'empreinte carbone des mesures de sécurité afin de garantir que la performance du système de management de la sécurité de l'information s'améliore continuellement et atteigne le niveau requis tout en réduisant son impact environnemental.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue

PRÉREQUIS À L'ENTRÉE EN FORMATION

L'entrée en formation est conditionnée à l'analyse du dossier du candidat, réalisée en amont de l'inscription et fondée sur :

- Un curriculum vitae détaillant son expérience professionnelle dans des fonctions liées à la sécurité de l'information, aux systèmes de management ou au conseil IT ;
- Un questionnaire de positionnement visant à évaluer ses acquis et sa capacité à suivre un parcours de certification sur la mise en œuvre du SMSI ;
- Un projet professionnel cohérent avec les objectifs de la certification.

Le candidat doit justifier :

- Soit d'une expérience professionnelle générale d'au moins 5 ans ;
- Soit d'une expérience spécifique d'au moins 2 ans dans le domaine du management de la sécurité de l'information.
- Et avoir réalisé 300 heures de projet en lien avec la mise en œuvre d'un système de management de la sécurité de l'information ;

PRÉREQUIS À LA VALIDATION

Pour accéder à la certification, le candidat doit avoir suivi l'ensemble de la formation PECB ou d'un partenaire habilité.

COMPOSITION DU JURY — FORMATION CONTINUE

Trois personnes seront désignées pour composer les membres du jury.

- 1 représentant de PECB, n'ayant pas dispensé la formation.
- 2 professionnels extérieurs à l'organisme de formation, sélectionnés en fonction de leur expertise dans le champ de compétence de la certification.

Base légale

Date de décision	29/05/2026
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	29/05/2029
Date de dernière délivrance possible	29/11/2029

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/7586/>

Où se former

Formations référencées	16
Organismes	4
Régions couvertes	8
Prix indicatif	1 140 € – 4 890 €
Durée	35 h

Offre de formation — MonCompteFormation (Caisse des Dépôts), licence ouverte.

Entrées et sorties de formation

Entrées en formation	51
Parcours menés à terme	41
Taux d'achèvement	80 %
Période	06/2026 – 09/2026

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

Demande CPF — formations engagées

Dossiers CPF engagés	76
Montant total engagé	117 646 €
Coût moyen par dossier	1 548 €
Durée moyenne	31 h
Période	06/2026 – 09/2026
France compétences	83 %
Reste à charge titulaire	14 %
Entreprise	2 %

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