

Évaluer et traiter les risques de sécurité de l'information en s'appuyant sur la norme NF ISO 27005 (ISO/CEI 27005 - Security Risk Manager)

RS6399 · RS · Publiée

L'essentiel

Code(s) NSF	326p
Formacode(s)	31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	20/09/2023
Date d'échéance	20/09/2026

Certificateur(s)

SKILLS4ALL · SIRET : 82815451800025

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

Toutes les informations détenues par une entreprise sont exposées à des menaces d'attaques, d'erreur, d'événements naturels et sont exposées à des vulnérabilités inhérentes à leur utilisation.

Afin d'apporter une réponse adaptée, les organisations ont la possibilité développer des démarches de préservation de leur système d'information telle que l'analyse des risques portée par la norme NF ISO 27005. Pour cela, elles doivent pouvoir disposer de personnel formé et certifié capable d'analyser les risques potentiels susceptibles d'affecter leur dispositif de sécurité de l'information.

La certification s'adresse à tout professionnel en lien avec le management de la sécurité de l'information de l'entreprise souhaitant attester qu'il possède de manière complémentaire les connaissances et les compétences nécessaires pour identifier, évaluer et traiter les risques auxquels est soumis le Système d'Information de façon à préserver les activités essentielles de l'entreprise en s'appuyant sur l'ISO 27005.

Les activités en lien avec cette certification sont :

- Définir le périmètre de l'analyse des risques
- Apprécier les risques
- Traiter les risques
- Garantir que la gestion des risques est une des activités essentielles de l'entreprise

COMPÉTENCES ATTESTÉES

C1. Identifier les processus métiers sensibles et stratégiques et leur système d'information associé en s'appuyant sur une analyse SWOT de l'environnement et de l'entreprise afin de garantir la cohérence des décisions de traitements des risques avec la stratégie de l'entreprise

C2.

Délimiter le domaine d'application (périmètre d'action) sur lequel s'exerce l'analyse de risque en synthétisant toutes les informations collectées issus de groupes de travail collaboratifs et de la documentation de l'entreprise afin de définir la stratégie d'évaluation et de traitement des risques

C3. Construire et hiérarchiser par criticité des scénarii de dysfonctionnement ou d'agression en s'appuyant sur les personnes ressources compétentes afin de retenir les scénarii les plus critiques en fonction de leur probabilité et de leurs impacts

C4. Elaborer les plans de traitement des risques (intégrant l'impact, la probabilité et les risques résiduels) en s'appuyant sur l'analyse des scénarii afin de permettre à la direction de l'entreprise de choisir les plus pertinents au regard de la stratégie de l'entreprise

C5. Accompagner l'entreprise dans la mise en œuvre du plan de traitement en s'appuyant sur des indicateurs de suivi des dysfonctionnements et en collectant de retours d'expérience afin de s'assurer de son efficacité dans le temps

C6. Favoriser une culture de la gestion du risque lié au système d'information dans l'organisation en facilitant les remontées d'incidents de sécurité de l'information et leur analyse afin de pérenniser les bénéfices obtenus de la démarche

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, Candidature individuelle

PRÉREQUIS À L'ENTRÉE EN FORMATION

Une bonne connaissance des systèmes d'information des organisations est nécessaire.

Le candidat devra produire 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 une démarche d'analyse des risques et cela dans les 5 dernières années

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	20/09/2023
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	20/09/2026
Date de dernière délivrance possible	20/03/2027

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.skills4all.com/certification/iso-27005-risk-manager-formation/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/6399/>

Entrées et sorties de formation

Entrées en formation	188
Parcours menés à terme	171
Taux d'achèvement	91 %

Demande CPF — formations engagées

Dossiers CPF engagés	212
Montant total engagé	494 355 €
Coût moyen par dossier	2 332 €
Durée moyenne	32 h
Période	10/2023 – 09/2026
France compétences	87 %
Reste à charge titulaire	7 %
France Travail	4 %
Entreprise	2 %
Régions	0 %
OPCO	0 %
Compte d'engagement citoyen	0 %

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