DAWAN

Plan de la formation

www.dawan.fr

Formation ISO 27005 – Risk Manager (Certification PECB incluse)

Durée :	3 jours (21 heures)
Tarif inter-entreprises :	2 925,00 CHF HT (Présentiel) 2 340,00 CHF HT (Distanciel)
Public :	Chefs de projet, consultants, architectes techniques - Toute personne en charge de la sécurité de l'information, de la conformité et des risques dans une organisation - Toute personne impliquée dans un programme de gestion des risques ou la mise en œuvre d'ISO/IEC 27001
Pré-requis :	Notions de base en sécurité de l'information et compréhension générale de la gestion des risques
Objectifs :	Comprendre les concepts et principes de la gestion des risques de sécurité de l'information selon ISO/IEC 27005- Mettre en place un programme de management des risques aligné sur un SMSI ISO 27001 - Savoir identifier, analyser, évaluer et traiter les risques de sécurité de l'information - Connaître les principales méthodes de gestion des risques (OCTAVE, MEHARI, EBIOS) et leurs spécificités - Se préparer à l'examen PECB ISO 27005 Risk Manager
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.

Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102761-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Structurer un programme de gestion des risques selon ISO 27005

Découvrir le cadre normatif de la gestion des risques (ISO 27005, ISO 31000, lien avec ISO 27001)
Comprendre les objectifs, le périmètre et les principes d’un programme de management des risques SSI
Définir les responsabilités et la gouvernance de la gestion des risques dans l’organisation
Planifier les étapes du processus de gestion des risques (contexte, appréciation, traitement, communication, surveillance)
Atelier fil rouge : formaliser la charte et la gouvernance d’un programme de gestion des risques SSI pour un périmètre donné

Établir le contexte et identifier les risques

Analyser le contexte externe et interne : enjeux, parties prenantes, contraintes, objectifs
Définir le périmètre et les critères de la gestion des risques (impact, vraisemblance,

appétence au risque)
Identifier les actifs, leurs propriétaires et leurs dépendances critiques
Recenser les menaces, vulnérabilités et scénarios de risques pertinents pour l'organisation
Atelier fil rouge : construire une première cartographie des actifs et des scénarios de risques pour un cas d'école

Analyser, évaluer et apprécier les risques

Différencier les approches qualitatives, quantitatives et semi-quantitatives
Évaluer la vraisemblance et l'impact des risques en fonction de critères définis
Prioriser les risques et identifier les risques intolérables nécessitant un traitement immédiat
Apprécier les risques résiduels et les arbitrages à effectuer (acceptation, transfert, réduction, évitement)
Atelier fil rouge : conduire une analyse de risques sur quelques scénarios et positionner les résultats dans une matrice

Traiter les risques et communiquer avec les parties prenantes

Définir les options de traitement des risques : mesures, plans d'actions, délais, responsables
Relier les actions de traitement aux contrôles ISO 27001 / ISO 27002
Communiquer sur les risques auprès de la direction, des métiers et des équipes techniques
Documenter les décisions, les plans de traitement et les niveaux de risques résiduels acceptés
Atelier fil rouge : élaborer un plan de traitement des risques et préparer une synthèse à destination d'un comité de direction

Découvrir les méthodes OCTAVE, MEHARI et EBIOS

Présenter les grandes lignes de la méthode OCTAVE et ses domaines d'application
Découvrir la méthode MEHARI et ses spécificités (catalogues, scénarios, scoring)
Introduire la méthode EBIOS et ses concepts fondamentaux (événements redoutés, scénarios de menaces)
Comparer les approches et identifier celle qui est la plus adaptée au contexte de son organisation
Atelier fil rouge : choisir la méthode la plus pertinente pour un contexte donné et justifier les raisons de ce choix

Préparer l’examen ISO 27005 Risk Manager

Revoir le processus de gestion des risques tel que défini dans ISO 27005
Synthétiser les notions clés : contexte, appréciation, traitement, communication, surveillance
S’entraîner sur des questions types et une étude de cas représentative
Élaborer un plan de révision personnalisé pour l’examen PECB ISO 27005 Risk Manager
Atelier fil rouge final : quiz de révision et clarification des points techniques avant l’examen