DAWAN

Plan de la formation

www.dawan.fr

Formation ISO 27035 – Lead Incident Manager (Certification PECB incluse)

Durée :	5 jours (35 heures)
Tarif inter-entreprises :	4 525,00 € HT (Présentiel) 3 620,00 € HT (Distanciel)
Public :	Gestionnaires d'incidents de sécurité de l'information, responsables TIC, auditeurs IT - Responsables souhaitant mettre en place ou structurer une équipe de réponse aux incidents (CSIRT, CERT, SOC) - Membres d'équipes de réponse aux incidents, responsables des risques de sécurité de l'information - Administrateurs systèmes et réseaux impliqués dans la gestion des incidents
Pré-requis :	Bonnes connaissances en sécurité des systèmes d'information et en fonctionnement d'un SI d'entreprise
Objectifs :	Maîtriser les concepts, méthodes et outils de gestion des incidents de sécurité de l'information selon ISO/IEC 27035 - Comprendre la corrélation entre ISO/IEC 27035 et les autres normes et cadres (ISO 27001, ISO 27002, etc.) - Être capable de concevoir, mettre en œuvre et maintenir un plan de gestion des incidents - Savoir organiser et piloter une équipe de réponse aux incidents de sécurité de l'information - Se préparer à l'examen PECB ISO 27035 Lead Incident 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 :	CYB102766-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

Comprendre le cadre de la gestion des incidents selon ISO 27035

Découvrir la norme ISO/IEC 27035 et ses parties
Situer ISO 27035 dans la famille ISO 27000 et les référentiels de sécurité (ISO 27001, 27002, 27005, etc.)
Définir un incident de sécurité de l’information et distinguer événements, incidents et crises
Identifier les enjeux organisationnels, techniques, juridiques et d’image liés à la gestion des incidents
Atelier fil rouge : analyser quelques incidents médiatisés et en dégager les enjeux de gestion et de communication

Concevoir un plan de gestion des incidents de sécurité de l’information

Définir les objectifs, le périmètre et la gouvernance de la gestion des incidents
Structurer le plan de gestion des incidents : rôles, responsabilités, processus, procédures, outils
Établir les canaux de communication internes et externes en cas d’incident

Prévoir l’articulation avec la gestion de crise et la continuité d’activité
Atelier fil rouge : élaborer un canevas de plan de gestion des incidents pour une organisation type

Mettre en œuvre le processus de gestion des incidents

Organiser la détection, la qualification et la priorisation des incidents
Collecter les informations, les journaux et les éléments de preuve nécessaires aux investigations
Coordonner la réponse technique, métier et communicationnelle
Assurer la traçabilité des actions et la documentation de l’incident
Atelier fil rouge : construire un workflow détaillé de gestion d’incidents et l’appliquer à un scénario d’attaque simulée

Piloter l’équipe de réponse aux incidents et améliorer le dispositif

Définir la composition, les rôles et les compétences d’une équipe de réponse aux incidents (CSIRT, CERT, équipe SOC)
Mettre en place des procédures et politiques structurées pour la gestion des incidents
Organiser la formation, les exercices et la montée en compétence de l’équipe
Mettre en œuvre l’amélioration continue du plan de gestion des incidents (RETEX, indicateurs, audits)
Atelier fil rouge : définir les profils et responsabilités d’une équipe de réponse aux incidents pour son organisation

Préparer l’examen ISO 27035 Lead Incident Manager

Revoir les concepts, processus et bonnes pratiques de gestion d’incidents définis par ISO 27035
Synthétiser les liens entre ISO 27035 et les autres normes (ISO 27001, 27002, 27005, 22301, etc.)
S’entraîner sur des études de cas couvrant détection, réponse, communication et amélioration continue
Préparer son plan de révision et comprendre les modalités de l’examen PECB Lead Incident Manager
Atelier fil rouge final : quiz global et étude de cas intégrant toutes les étapes de la gestion d’un incident majeur