New

ISO/IEC 27035 - Foundation, Gestion des incidents de sécurité de l’information

Assurer la mise en oeuvre d’une gestion efficace des incidents de sécurité

Présentiel ou en classe à distance

2 jours (14 h) | Prix inter : 2.190,00 € HT | Réf.: MG227

La formation **ISO/IEC 27035 Foundation** fournit une compréhension structurée du cycle complet de **gestion des incidents de sécurité**, depuis la **détection** jusqu’au **retour d’expérience**. Elle permet d’intégrer les exigences de la **norme ISO 27035** dans une approche opérationnelle, couvrant la **classification des incidents**, la **collecte d’informations probantes**, la **coordination de l’équipe de réponse** et la mise en oeuvre des actions de confinement et de reprise. Les travaux pratiques renforcent l’appropriation des méthodes et facilitent leur application dans un contexte professionnel.
Au-delà de la maîtrise du référentiel, les participants acquièrent la capacité à construire un **plan de gestion des incidents** adapté à leur organisation, à définir des **indicateurs de sécurité pertinents** et à contribuer à la **gouvernance de la sécurité de l’information**. L’obtention de la certification PECB Foundation, proposée en différé, consolide cette montée en compétence et constitue un atout différenciant pour les professionnels de la cybersécurité.

A qui s'adresse cette formation ?

Pour qui

- Toute personne intéressée par l’approche processus de gestion des incidents de la sécurité de l’information

Prérequis

- Auncun.
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Cadre normatif et concepts fondamentaux

- Présentation de l'ISO et la famille ISO/IEC 27000
- Vue d'ensemble de la série ISO/IEC 27035 (parties 1, 2, 3)
- Autres normes et réglementations connexes
- Sécurité de l'information et triade CIA Vulnérabilités, menaces et risques
- Différence entre événements et incidents de sécurité
- Concepts de gestion des incidents et plan de réponse
- Confidentialité et classification des contrôles

Atelier

Cartographie des normes selon différents secteurs d'activité

Quiz interactif sur les concepts de base

2 - Approche stratégique de la gestion des incidents

- Objectifs et bonnes pratiques de gestion des incidents
- Intégration avec le SMSI (Système de Management de la Sécurité)
- Approche structurée pour la gestion des incidents
- Politiques, plans et processus Rédaction et communication des politiques
- Gestion des risques : contexte, identification, analyse, évaluation
- Traitement des risques et plan d'action
- Communication, surveillance et revue
  Atelier

3 - Planification et organisation des équipes

- Structure et contenu du plan de gestion des incidents
- Révision des processus et procédures documentés Constitution de l'équipe de gestion des incidents
- Rôles et responsabilités détaillés (coordinateur, équipe de réponse)
- Compétences requises et structure organisationnelle
- Relations internes avec l'organisation
- Relations externes et parties prenantes
- Partage d'informations et communication multi-niveaux
  Atelier

  Création de la structure d'un plan de gestion des incidents

  Etablir la matrice de compétences et profils de postes

4 - Préparation opérationnelle

- Programmes de sensibilisation et formation
- Développement et évaluation des compétences
- Systèmes et techniques de test
- Préparation, documentation et activités post-test
- Capacité de surveillance pour la réponse aux incidents
- Surveillance réseau, système et continue (ISCM)
- Évaluation des performances et métriques de sécurité
  Atelier

  Elaboration d'un scénario de test d'incident complet

5 - Détection et classification des incidents

- Mécanismes de détection et signalement
- Mécanismes de détection des incidents de sécurité
- Méthodologie et objectifs des attaquants
- Signes et indicateurs d'incidents
- Processus de classification des incidents
- Niveaux de classification et criticité
- Évaluation des événements de sécurité Activités clés d'évaluation et de décision
- Priorisation des incidents
  Atelier

  Classification d'incidents selon différents critères

  Définition des seuils d'alerte et escalade

6 - Collecte d'informations et reporting

- Sources d'information et méthodes de collecte
- Collecte et préservation des preuves
- Chaîne de custody et aspects légaux
- Signalement d'événements de sécurité
- Informations fondamentales sur les incidents
- Analyse technique et impact business
- Documentation des dommages et préjudices
- Rédaction et soumission de rapports
- Communication vers les parties prenantes
  Atelier

  Construction d'un rapport d'incident

7 - Réponse et résolution d'incidents

- Rôles et responsabilités pendant la phase de réponse
- Stratégies de réponse aux incidents de sécurité Stratégies de confinement et critères de sélection
- Techniques d'isolement et de quarantaine Identification des indicateurs de compromission (IoC)
- Documentation et préservation des preuves
- Processus d'éradication des menaces
- Stratégies et options de récupération Évaluation des sauvegardes et restauration
  Atelier

  Application des techniques de confinement

8 - Post-incident et amélioration continue

- Processus de retour d'expérience (lessons learned) Identification des domaines d'amélioration
- Amélioration du plan de gestion des incidents
- Évaluation des performances de l'équipe
- Amélioration des contrôles de sécurité
- Amélioration de l'évaluation des risques
- Objectifs de mesure et indicateurs de performance
- Méthodes de surveillance et de mesure Fréquence des évaluations et reporting
- Cycle d'amélioration continue
  Atelier

  Analyse post-incident d'un cas pratique

9 - Intégration et gouvernance

- Intégration de la gestion des incidents dans la gouvernance IT Alignement avec les objectifs business Reporting à la direction et au conseil d'administration Conformité réglementaire et obligations légales Gestion des relations avec les régulateurs Assurance et transfert de risques Évolution des menaces et adaptation continue
  Atelier

  Définition d'une roadmap d'amélioration

10 - Examen de certification " PECB Certified ISO/IEC 27035 Foundation" (passage en différé, en ligne après la formation)

- Révision des concepts en vue du passage des certifications
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session
- Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
- Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
- Retrouvez les instructions pour le passage de l'examen en ligne
- L'examen de certification ISO 27035
- Foundation est en anglais
- 40 questions réparties selon différents domaines de compétences
- Un score minimum de 70% est exigé pour réussir l'examen
- L'examen se déroule sur 1 heure
- Les candidats ne sont pas autorisés à utiliser les supports de cours
- Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir les certifications
- En cas d'échec les candidats bénéficient d'une seconde chance pour repasser gratuitement l'examen dans les 12 mois suivant la première tentative
- L'examen "PECB Certified ISO/IEC 27035 Foundation" couvre les domaines de compétences suivants :
- Domaine 1 : Principes et concepts fondamentaux de la gestion des incidents de sécurité de l’information
- Domaine 2 : Gestion des incidents de sécurité de l’information

Après la session

Les objectifs de la formation

- Comprendre les principes fondamentaux de la gestion des incidents de sécurité de l'information

- Connaître la relation entre la norme ISO/IEC 27035 et les autres normes et cadres réglementaires
- Comprendre l'approche basée sur les processus pour gérer les incidents de sécurité de l'information

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- L'apprentissage par la pratique : les phases théoriques sont complétées d'ateliers favorisant un ancrage durable des acquis
- Les nombreux retours d'expérience et conseils des consultants spécialistes du sujet
- Utilisation d'environnements proches du contexte professionnel

Dates et villes 2026 - Référence MG227

Dernières places disponibles Session garantie

A distance

du 26 mars au 27 mars	du 16 juil. au 17 juil.	du 12 nov. au 13 nov.
du 12 mai au 13 mai	du 24 sept. au 25 sept.	

Rennes

du 26 mars au 27 mars	du 16 juil. au 17 juil.	du 12 nov. au 13 nov.

Paris

du 26 mars au 27 mars	du 16 juil. au 17 juil.	du 12 nov. au 13 nov.
du 12 mai au 13 mai	du 24 sept. au 25 sept.	

Lyon

du 26 mars au 27 mars	du 16 juil. au 17 juil.	du 12 nov. au 13 nov.

Nantes

du 26 mars au 27 mars	du 16 juil. au 17 juil.	du 12 nov. au 13 nov.

Toulouse

du 12 mai au 13 mai	du 24 sept. au 25 sept.

Strasbourg

du 12 mai au 13 mai	du 24 sept. au 25 sept.

Sophia Antipolis

du 12 mai au 13 mai	du 24 sept. au 25 sept.

Rouen

du 12 mai au 13 mai	du 24 sept. au 25 sept.

Aix-en-Provence

du 12 mai au 13 mai	du 24 sept. au 25 sept.

Lille

du 12 mai au 13 mai	du 24 sept. au 25 sept.