Module 919 – ISO/IEC 27032 Foundation

ISO/IEC 27032 Foundation
Fondamentaux de la cyber sécurité

Objectifs

La formation ISO/IEC 27032 Foundation vous permettra d'appréhender les éléments fondamentaux de la cybersécurité. Durant cette formation, vous comprendrez quels sont les concepts, approches, méthodes et techniques utilisés dans les programmes de cybersécurité.

La formation se conclut par un examen donnant lieu à une certification ISO 27032 Foundation.

A qui s'adresse ce cours

Ce stage s'adresse aux personnes impliquées dans les TI notamment à celles impliquées dans le management de la sécurité de l'information à celles souhaitant acquérir des connaissances relatives aux principaux de la cybersécurité ainsi qu'aux personnes souhaitant poursuivre une carrière dans la cybersécurité.

Cours de 2 jours – 1550 € HT

Paris	Lyon
21 janv. 2021	08 juillet 2021
25 mars	22 sept.
10 juin	08 déc.
18 nov.	

Intra entreprise
Sur demande

Cette offre de formation est éligible à MON COMPTE FORMATION moncompteformation.gouv.fr

Certification enregistrée RS4316
https://www.francecompetences.fr

Pour vous inscrire

Téléphone : 01 40 33 76 88
E-mail : contact@beresilientgroup.com

Courrier

BRG – 10, rue Emile Landrin – 75020 Paris
Centre de formation agréé préfecture : 11754161975
SAS au Capital de 150 000 Euros - Siret Paris B 441 951 845

Contenu du module 919

Jour 1: Introduction aux concepts fondamentaux de la cybersécurité basés sur l'ISO / CEI 27032

- Objectifs et structure du cours
- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Politique de cybersécurité et gestion des risques
- Mécanismes d'attaque

Jour 2 Approches des programmes de cybersécurité et examen de certification.

- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation
- Continuité d'activité
- Management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

Examen

Durée 1 heure
Les frais de certification sont inclus dans le prix de l'examen.
Un manuel de cours contenant les informations et des exemples pratiques est fourni.
À l'issue de la formation, un certificat de participation est délivré.
En cas d'échec à l'examen, vous pouvez le repasser dans les 12 mois qui suivent sans frais supplémentaires.

brg
be resilient group

Mise à jour du 20/01/2021

Module 919

ISO/IEC 27032 Foundation
Fondamentaux de la cyber sécurité

Module 919 – ISO/IEC 27032 Foundation

Prérequis

Pas de prérequis

Modalités et délais d'accès

1. Contacter nous par mail ou téléphone pour qualifier votre besoin de formation
2. Renvoyez le bon de réservation complété (disponible à la fin du catalogue)
2. Validation de votre inscription (éligibilité du stagiaire)
3. Etablissement et signature de la convention de formation
4. Envoi de votre convocation à la session de formation avec les détails (horaires, lieu…)

Durée estimée entre la demande du bénéficiaire et le début de la prestation: de 1 à 3 mois

Méthodes mobilisées

Cours magistral basé sur les meilleures pratiques liées à la cyber sécurité (ISO 27032)
Exercices pratiques panachés de travaux dirigés et guidés par l'apprenant et d'exercices en pleine autonomie, afin d'assurer une assimilation des savoir-faire requis.
Support de cours au format papier et numérique, version française

Modalités d'évaluation – Validation des compétences - Certification

Examen de certification 1 heure - Organisme certificateur PECB
Evaluation de la totalité des cinq compétences constitutives de la certification :
- Analyser le système d'information de l'entreprise, afin de repérer ses points de faiblesse au regard des menaces d'intrusion et de perte de données inhérentes au cyberespace.
- Etablir le cahier des charges de cyber sécurité de son entreprise conformément à la norme ISO 27032, afin de répondre aux impératifs de protection de l'activité dans le cadre du budget disponible.
- Elaborer les parades adaptées aux menaces d'intrusion et de pertes de données inhérentes au cyberespace, conformément au cahier des charges et au budget imparti.
- Etablir le schéma général de cyber sécurité à l'intention des responsables de l'entreprise, en vue de préparer un plan de communication vers l'ensemble du personnel.
- Concevoir un plan de formation des personnels aux bonnes pratiques en matière de cyber sécurité conformes à la norme ISO 27032, afin d'assurer leur implication à tous les niveaux de l'entreprise.

Equivalences, passerelles, suite de parcours et débouchés

Pas de certification partielle – Remise d'un certificat de compétences PECB valable 3 ans
La certification permet aux individus de disposer des compétences nécessaires à la définition et à la mise en œuvre d'un programme de cyber sécurité : elle fournit une solution réaliste aux individus dans la protection de leurs données privées et pour la protection des données des organisations contre les escroqueries de phishing, les cyber attaques, le piratage informatique et autres menaces cybernétiques..
Répondre aux exigences de postes correspondants à ces caractéristiques : RSSI, responsable de la gestion des risques en sécurité de l'information, consultant en cyber sécurité.
Suite de parcours: ISO 27032 Lead Cybersecurity Manager

Accessibilité aux personnes handicapées

Procédure Accueil Handicap: En cas d'accueil d'un stagiaire handicapé, l'office manager de BRG est le référent handicap, qui pourra si besoin mobiliser notre réseau de partenaires du champ du handicap.
Accessibilité aux personnes à mobilité réduite: Nos locaux sont Etablissement Recevant du Public (ERP)
Attestation de vérification de l'accessibilité aux personnes handicapées – Dossier accessibilité

brg
be resilient group

Mise à jour du 20/01/2021