

PECB Certified NIS 2 Directive Lead Implementer (formation & examen de certification)



Objectifs

En participant à la formation NIS 2 Directive Lead Implementer, vous acquérez une connaissance approfondie des exigences de la directive, des stratégies de mise en œuvre et des bonnes pratiques qui protègent les infrastructures critiques contre les cybermenaces. Grâce à des sessions interactives et des exercices pratiques, vous apprendrez à évaluer les risques de cybersécurité de l'organisme, à élaborer des plans robustes de réponse aux incidents et à mettre en œuvre des mesures de sécurité efficaces pour répondre aux exigences de la directive NIS 2. Après avoir réussi l'examen, vous pouvez demander la certification « PECB Certified NIS 2 Directive Lead Implementer ».

A qui s'adresse ce cours

Ce stage s'adresse aux professionnels de la cybersécurité cherchant à acquérir une compréhension approfondie des exigences de la directive NIS 2 et à apprendre des stratégies pratiques pour mettre en œuvre des mesures de cybersécurité robustes, e taux responsables réglementaires chargés de faire appliquer la directive NIS 2

Cours de 5 jours – 2 950 € HT

<u>Paris</u>	<u>Lyon</u>
17 février 2025	17 février 2025
14 avril	14 avril
02 juin	02 juin
07 juillet	07 juillet
08 sept	08 sept
17 nov	17 nov
26 janv 2026	26 janv 2026
23 mars	23 mars

Intra entreprise
Sur demande

Contenu du module 830

Jour 1 Introduction à la directive NI2

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Directive NIS 2
- Exigences de la directive NIS 2
- initiation de la mise en œuvre de la directive NIS 2
- L'organisme et son contexte

Jour 2 Analyse du programme de conformité à la directive NIS 2, de la gestion des actifs et de la gestion des risques

- Gouvernance de la cybersécurité
- Rôles et responsabilités de cybersécurité
- Gestion des actifs
- Gestion des risques

Jour 3 Contrôles de cybersécurité, gestion des incidents et gestion des crises

- Contrôles de cybersécurité
- Sécurité de la chaîne d'approvisionnement
- Gestion des incidents
- Gestion des crises

Jour 4 Communication, tests, surveillance et amélioration continue de la cybersécurité

- Continuité d'activité
- Sensibilisation et formation
- Communication
- Tests en cybersécurité
- Audit interne
- Mesurer, surveiller et rendre compte des performances et des indicateurs
- Amélioration continue
- Clôture de la formation

Jour 5 Examen de certification

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

PECB Certified NIS 2 Directive (formation & examen de certification)

Prérequis

Connaître les principes de bases de la sécurité de l'information
Formation initiale second cycle ou 5 ans minimum d'expérience professionnelle

Modalités et délais d'accès

1. Contactez-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 sécurité de l'information(ISO 27001)
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 3 heures - Organisme certificateur PECB

Evaluation de la totalité des cinq compétences constitutives de la certification :

- Décrire les éléments et le fonctionnement d'un système de management de la sécurité de l'information à l'intention des responsables de l'entreprise, en vue de les impliquer dans la mise en œuvre de celui-ci.
- Elaborer un système de management de la sécurité de l'information conforme à la norme ISO/IEC 27001, afin d'optimiser la prévention des menaces d'intrusions dans le système d'information de l'entreprise.
- Coordonner la mise en place d'un système de management de la sécurité de l'information en tenant compte du nécessaire accompagnement des acteurs, en vue d'assurer son efficacité sur le long terme.
- Evaluer et mesurer en continu la performance du système de management de la sécurité de l'information au moyen d'indicateurs pertinents, en vue d'optimiser celui-ci grâce à une exacte identification des points d'amélioration.
- Conseiller une entreprise sur les meilleures pratiques en matière de sécurité de l'information, afin de renforcer l'efficacité du système de management de la sécurité de l'information.

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, à la mise en œuvre, le suivi et l'amélioration de la sécurité de l'information dans l'entreprise. Répondre aux exigences de postes correspondants à ces caractéristiques : RSSI, chefs de projet/consultant en sécurité des systèmes d'information. La certification permet aux entités utilisatrices de faciliter la gestion des compétences et le recrutement en s'appuyant sur une certification reconnue. Favoriser la collaboration inter-organisationnelle en partageant un langage et des processus communs. Garantir aux parties prenantes de l'organisation un certain standard de qualité. Le maintien dans le temps de la certification garantit la transférabilité des compétences d'une entité utilisatrice à une autre.
Suite de parcours: ISO 27001 Lead Auditor

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

