

Certification PECB NIS 2 Directive Lead Implementer

Formation certifiante — Partenaire officiel PECB · 4 jours — 28 heures de formation + examen PECB (session différée via voucher)

2026 – V2 | CABEXSI — Cabinet d'expertise en cybersécurité et systèmes d'information

1. Informations générales

INTITULÉ	Certification PECB NIS 2 Directive Lead Implementer
TYPE DE FORMATION	Formation certifiante — Partenaire officiel PECB
DURÉE	4 jours — 28 heures de formation + examen PECB (session différée via voucher)
MODALITÉ	Présentiel (lieu communiqué dans la convocation) — intra ou inter-entreprises
PUBLIC VISÉ	Professionnels de la cybersécurité souhaitant maîtriser les exigences de la directive NIS 2. DSI, RSSI, responsables conformité, responsables cybersécurité, consultants, responsables de la résilience et des systèmes critiques. Responsables gouvernementaux chargés de l'application de la directive.
PRÉREQUIS	Connaissances fondamentales en cybersécurité. Une connaissance des principes de la directive NIS 2 est un atout.
RÉFÉRENT HANDICAP	Laurent Rousee — contact@cabexsi.com 06 22 56 29 17
TARIF	Sur devis — nous contacter : contact@cabexsi.com 06 22 56 29 17
FINANCEMENT	Potentiellement finançable par les OPCO selon les dispositifs en vigueur et les conditions propres à chaque organisme. CABEXSI vous accompagne dans le montage du dossier.

2. Objectifs pédagogiques

- Expliquer les concepts fondamentaux et les exigences de la directive NIS 2
- Acquérir une compréhension approfondie des principes, stratégies, méthodologies et outils pour mettre en œuvre un programme de cybersécurité conforme à NIS 2
- Initier et planifier la mise en œuvre des exigences de NIS 2 en utilisant la méthodologie PECB
- Soutenir une organisation dans la planification, mise en œuvre, gestion, surveillance et maintien d'un programme de cybersécurité NIS 2
- Préparer et réussir l'examen de certification PECB NIS 2 Directive Lead Implementer

3. Compétences visées

- Capacité à comprendre les objectifs, le périmètre et les exigences de la directive NIS 2
- Capacité à identifier les entités concernées (EE et EI) et leurs obligations
- Capacité à conduire une analyse des risques cyber adaptée aux infrastructures critiques

- Capacité à mettre en œuvre les contrôles de cybersécurité requis par NIS 2
- Capacité à gérer les incidents de cybersécurité et les plans de continuité d'activité
- Capacité à piloter la communication, les tests et la surveillance du programme
- Capacité à articuler NIS 2 avec ISO/IEC 27001, IEC 62443 et DORA

4. Méthodes et moyens pédagogiques

La formation est basée sur des méthodes participatives, explicatives et interrogatives, alternant apports théoriques et échanges d'expérience. La mise en pratique suit chaque séquence théorique. Le formateur ne passe pas à l'enseignement du module suivant tant que le précédent n'a pas été parfaitement compris et assimilé.

- Méthode pédagogique : expositive, participative et interrogative — alternance théorie / pratique
- Modalité : Présentiel (lieu communiqué dans la convocation) — intra ou inter-entreprises
- Matériel : écran, PC, salle de vidéoprojection, support PPTX
- Effectif recommandé : 6 à 12 participants
- Supports de cours PECB officiels : plus de 400 pages — remis via la plateforme PECB dès J1
- Voucher d'examen PECB inclus dans le tarif — valable 12 mois à compter de la formation
- 31 crédits CPD (Continuing Professional Development) attribués à l'issue de la formation

5. Évaluation des acquis

Au début et en fin de chaque module, un contrôle des connaissances vérifie que les principes et méthodes enseignés sont bien acquis avant de passer au module suivant.

- Quiz de positionnement en début de formation
- Exercices pratiques, études de cas et quizz scénarisés PECB après chaque séquence
- Chaque jour : préparation à l'examen — questions d'examen, quizz de révision
- Examen PECB (session différée, open-book, 3h) via voucher dans les 12 mois — seconde tentative offerte en cas d'échec
- Attestation de fin de formation (28h) remise à l'issue de la session
- Certificat PECB délivré après réussite à l'examen et validation des conditions d'expérience

6. Indicateurs de résultats

Les indicateurs de résultats de cette action (taux de satisfaction, taux de réussite le cas échéant, effectifs formés) sont publiés et actualisés annuellement en ligne, et ne sont donc pas figés dans la présente fiche :

- Consultables sur www.cabexsi.com, rubrique Formation, en regard de chaque action
- Transmis sur demande au financeur (OPCO) et communiqués à l'entreprise cliente à l'issue de chaque session

7. Accessibilité handicap

Lors de l'entretien d'évaluation des besoins, préalable à l'entrée en formation, la question de l'accessibilité liée à un handicap est systématiquement abordée. En cas de besoin identifié, le lieu, la durée, le déroulé et les supports pédagogiques peuvent être adaptés. Pour toute demande spécifique : contact@cabexsi.com | 06 22 56 29 17.

8. Modalités et délais d'accès

L'accès à la formation peut être initié par l'employeur, à l'initiative du salarié avec l'accord de ce dernier, ou à l'initiative propre du salarié. Pour chaque demande, une analyse des besoins est réalisée afin d'adapter et personnaliser le parcours, et permettre l'accueil des personnes présentant un handicap.

- Délai d'accès : 1 mois avant le début de l'action, tenant compte des formalités administratives et financières

- Inscription et renseignements : contact@cabexsi.com | 06 22 56 29 17
- Convention de formation transmise et signée avant le démarrage de la session
- À l'issue de la formation, une attestation de fin de formation est remise à chaque participant

9. Programme — 4 jours / 28 heures

Jour 1 — Introduction à la directive NIS 2 et initiation de sa mise en œuvre

- Objectifs, structure et déroulé de la formation
- Contexte réglementaire européen en cybersécurité : NIS 2, DORA, CER, RGPD
- Concepts fondamentaux et définitions de la directive NIS 2
- Champ d'application : entités essentielles (EE) et entités importantes (EI)
- Cadre juridique, responsabilités des dirigeants et régime de sanctions
- Initiation du projet de mise en œuvre NIS 2 : méthodologie PECB
- Analyse du contexte de l'organisation et définition du périmètre

Jour 2 — Analyse du programme de conformité NIS 2, gestion des actifs et des risques

- Gouvernance de la cybersécurité : rôles, responsabilités, politiques
- Gestion des actifs : identification, classification, protection
- Analyse des risques cyber : méthodes, cadre et processus d'appréciation
- Évaluation des risques et définition des plans de traitement
- Sécurité de la chaîne d'approvisionnement : fournisseurs et sous-traitants
- Déclaration de conformité et documentation du programme

Jour 3 — Contrôles de cybersécurité, gestion des incidents et de crise

- Contrôles de sécurité technique et organisationnelle requis par NIS 2
- Sécurité des infrastructures et des applications
- Gestion des incidents de cybersécurité : détection, analyse, réponse
- Obligations de notification aux autorités compétentes (ANSSI) : délais et contenu
- Gestion de crise et continuité d'activité
- Plans de reprise et résilience opérationnelle

Jour 4 (matin) — Communication, surveillance et amélioration continue

- Tests et exercices de cybersécurité : simulations, audits, revues
- Surveillance et mesure de la performance du programme
- Communication interne et externe sur la cybersécurité
- Amélioration continue et retours d'expérience
- Articulation NIS 2 avec ISO/IEC 27001, IEC 62443 et DORA
- Synthèse générale — questions / réponses
- Présentation des 4 domaines de l'examen : Concepts fondamentaux et définitions ; Planification de la mise en œuvre ; Rôles, responsabilités et gestion des risques cyber ; Contrôles de cybersécurité, gestion des incidents et de crise
- Conseils de méthode pour l'examen open-book

10. Niveaux de certification PECB accessibles après l'examen

CREDENTIAL PECB	EXPÉRIENCE PROFESSIONNELLE	EXPÉRIENCE PROJET	AUTRES CONDITIONS
PECB Certified NIS 2 Directive Provisional Implementer	Aucune	Aucune	Signature du Code d'éthique PECB
PECB Certified NIS 2 Directive Implementer	2 ans (dont 1 an en cybersécurité)	200 heures	Signature du Code d'éthique PECB
PECB Certified NIS 2 Directive Lead Implementer	5 ans (dont 2 ans en cybersécurité)	300 heures	Signature du Code d'éthique PECB

En cas d'échec, les participants peuvent repasser l'examen dans les 12 mois, sans frais supplémentaires.