



## PECB Certified NIST Cybersecurity Professional

Acquérez une expertise dans l'application des lignes directrices du NIST, la gestion des contrôles de sécurité, l'utilisation de techniques de gestion des risques et la conception d'un programme de cybersécurité aligné sur les objectifs organisationnels et les besoins en matière de sécurité.

### Pourquoi devriez-vous y participer ?

Dans le monde actuel de plus en plus numérique, les organisations sont confrontées à des défis croissants pour sécuriser leurs systèmes d'information et assurer leur conformité aux normes réglementaires. Les publications du NIST, telles que le NIST SP 800-12, le NIST SP 800-53, le NIST RMF, le NIST SP 800-171 et le NIST Cybersecurity Framework, offrent des lignes directrices complètes et des bonnes pratiques pour établir des mesures de cybersécurité robustes. La mise en œuvre de ces cadres aide les organisations à renforcer leur posture en matière de cybersécurité, à gérer efficacement les risques et à maintenir leur conformité aux exigences fédérales.

Grâce à des directives approfondies sur les publications du NIST, les participants apprennent à relever des défis complexes en matière de sécurité, en appliquant ces cadres pour concevoir des programmes de cybersécurité robustes, alignés sur les objectifs organisationnels. La formation fournit également une expertise pratique pour prévenir, détecter et répondre efficacement aux cybermenaces, en intégrant les bonnes pratiques et les normes afin de créer une approche de sécurité cohérente. À l'issue de la formation, les participants pourront passer l'examen. Les personnes ayant réussi l'examen recevront la certification mondialement reconnue « PECB Certified NIST Cybersecurity Professional ».



## À qui s'adresse la formation ?

Cette formation est destinée aux :

- Dirigeants ou administrateurs responsables de la supervision des initiatives de cybersécurité au sein de leur organisation
- Administrateurs systèmes et ingénieurs réseaux souhaitant approfondir leur compréhension des contrôles de sécurité et des processus de gestion des risques afin de se conformer aux normes de sécurité du NIST
- Professionnels impliqués dans le développement et la mise en œuvre de programmes de cybersécurité
- Professionnels et conseillers qui fournissent des services de cybersécurité et de conformité, en veillant à rester informés des derniers cadres et bonnes pratiques du NIST
- Enquêteurs en criminalistique numérique et en cybercriminalité qui doivent comprendre les aspects techniques et réglementaires des cadres de cybersécurité afin d'enquêter sur les incidents de sécurité et d'y répondre de manière complète
- Personnes travaillant en cybersécurité ou en sécurité de l'information qui visent à approfondir leur compréhension des lignes directrices du NIST et à développer des compétences pratiques en gestion des risques liés à la cybersécurité

## Programme de la formation

Durée : 5 jours

### Jour 1 | Introduction aux normes et principes de cybersécurité du NIST

- Objectifs et structure de la formation
- Cadres et normes en matière de sécurité de l'information et de cybersécurité
- Introduction au NIST et à son rôle dans la cybersécurité
- Introduction à la cybersécurité
- L'organisation et son contexte
- Rôles, responsabilités et autorités
- Politique de cybersécurité

### Jour 2 | Stratégie de gestion des risques et gestion des risques liés à la chaîne d'approvisionnement

- Stratégie de gestion des risques
- Gestion des risques liés à la chaîne d'approvisionnement
- Gestion des actifs
- Évaluation des risques
- Amélioration

### Jour 3 | Sélection des contrôles de sécurité, sensibilisation et formation, et surveillance continue

- Sélection des contrôles de sécurité
- Sensibilisation et formation
- Mesures de sécurité
- Surveillance continue de la sécurité

### Jour 4 | Gestion des incidents de cybersécurité

- Gestion et analyse des incidents
- Réponse aux incidents, atténuation et rapport
- Rétablissement après incident et leçons apprises
- Clôture de la formation

### Jour 5 | Examen de certification



## Objectifs d'apprentissage

Au terme de cette formation, les participants seront en mesure de :

- Discuter des principes et concepts fondamentaux de la cybersécurité
- Soutenir la conformité aux principales publications du NIST, y compris le NIST 800-12, le NIST 800-53, le NIST RMF, le NIST 800-171 et le NIST CSF
- Évaluer les contrôles de sécurité et prodiguer des conseils à cet égard, en conformité avec les lignes directrices du NIST
- Fournir des orientations sur la gestion des risques en cybersécurité et les stratégies de gestion des incidents
- Guider les organisations dans le développement et l'optimisation de leurs programmes de cybersécurité

## Examen

Durée : 3 heures

L'examen « PECB Certified NIST Cybersecurity Professional » répond pleinement aux exigences du Programme d'examen et de certification (PEC) de PECB. Il couvre les domaines de compétences suivants :

**Domaine 1** | Principes et concepts fondamentaux de la cybersécurité

**Domaine 2** | Planification d'une stratégie organisationnelle en cybersécurité

**Domaine 3** | Évaluation et conseil en matière de programmes de cybersécurité et de contrôles de sécurité

**Domaine 4** | Gestion des incidents de cybersécurité

**Domaine 5** | Réponse aux incidents de cybersécurité

Pour des informations spécifiques concernant le type d'examen, les langues disponibles et d'autres détails, veuillez consulter la [Liste des examens de PECB](#) ainsi que les [Règles et politiques relatives aux examens](#).



## Certification

Après avoir réussi l'examen, vous pouvez postuler pour l'une des certifications ci-dessous. Un certificat vous sera délivré si vous remplissez toutes les exigences relatives à la certification sélectionnée.

Certification	Examen	Expérience professionnelle	Expérience en programme de cybersécurité	Autres exigences
<b>PECB Certified Provisional NIST Cybersecurity Professional</b>	Examen PECB Certified NIST Cybersecurity Professional	Aucune	Aucune	Signature du Code de déontologie de PECB
<b>PECB Certified NIST Cybersecurity Professional</b>		<b>5 ans</b> (dont 2 en cybersécurité)	Au moins 300 heures	

## Informations générales

- Les frais d'examen et de certification sont inclus dans le prix de la formation.
- Les participants recevront plus de 450 pages de matériel de formation complet, incluant des exemples pratiques, des exercices et des quiz.
- Une Attestation d'achèvement de formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation.
- Les candidats ayant suivi la formation auprès de l'un de nos partenaires et ayant échoué à leur premier examen peuvent le repasser gratuitement dans un délai de 12 mois à compter de la date de réception du code coupon, car les frais de formation couvrent la première tentative d'examen ainsi que la reprise. Autrement, des frais s'appliquent.