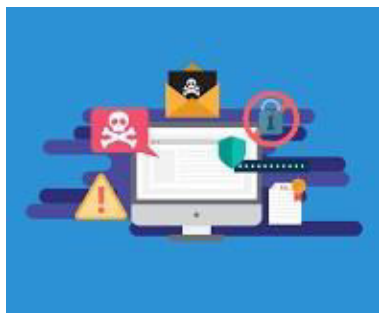


# ISO/IEC 27032 Lead Cybersecurity Manager (formation & examen de certification)

Module 820 – ISO 27032 Lead  
Cybersecurity Manager



## Objectifs

La formation ISO/IEC 27032 Lead Cybersecurity Manager vous permet d'acquérir l'expertise et les compétences nécessaires pour soutenir un organisme dans la mise en œuvre et le management d'un programme de cybersécurité basé sur la norme ISO/IEC 27032 et le cadre de cybersécurité du NIST. Au cours de cette formation, vous acquerez des connaissances approfondies sur la cybersécurité, la relation entre la cybersécurité et d'autres types de sécurité informatique, et du rôle des parties prenantes dans la cybersécurité. La formation se conclut par un examen donnant lieu à une certification ISO/IEC 27032 Lead Cybersecurity Manager.

## A qui s'adresse ce cours

Ce stage s'adresse aux professionnels de la cybersécurité, aux experts en sécurité de l'information, aux professionnels cherchant à gérer un programme de cybersécurité, aux personnes responsables de concevoir un programme de cybersécurité, aux spécialistes de la TI, aux conseillers-experts en technologie de l'information.

## Cours de 5 jours – 2 950 € HT

| Paris        | Lyon         |
|--------------|--------------|
| 18 mars 2024 | 18 mars 2024 |
| 13 mai       | 13 mai       |
| 01 juillet   | 01 juillet   |
| 16 sept      | 16 sept      |
| 18 nov       | 18 nov       |
| 20 janv 2025 | 20 janv 2025 |
| 10 mars      | 10 mars      |

Intra entreprise  
Sur demande

## Contenu du module 820

### Jour 1 Introduction à la cybersécurité et aux notions connexes, selon la recommandation de la norme ISO/IEC 27032

- Objectifs et structure du cours
- Normes et cadres réglementaires
- Notions fondamentales de la cybersécurité
- Programme de cybersécurité
- Lancer un programme de cybersécurité
- Analyser l'organisme
- Leadership

### Jour 2 Politiques de cybersécurité, management du risque et mécanismes d'attaque

- Politiques de cybersécurité
- Gestion du risque de la cybersécurité
- Mécanismes d'attaque

### Jour 3 Mesures de contrôle de cybersécurité, partage et coordination de l'information

- Mesures de contrôle de cybersécurité
- Partage et coordination de l'information
- Programme de formation et de sensibilisation

### Jour 4 Gestion des incidents, suivi et amélioration continue

- Continuité d'activité
- Management des incidents de cybersécurité
- Intervention et récupération en cas d'incident de cybersécurité
- Conclusion de la formation
- Tests en cybersécurité
- Mesure de la performance
- Amélioration continue

### Jour 5 Examen de certification



## Pour vous inscrire

Téléphone : 01 40 33 76 88  
E-mail : [contact@beresilientgroup.com](mailto: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

**brg**  
be resilient group

Module 820

Mise à jour du 01/01/2024

# ISO/IEC 27032 Lead Cybersecurity Manager (formation & examen de certification)

## Prérequis

Connaître les principes de bases liés à l'ISO 27032  
Formation initiale second cycle ou 5 ans minimum d'expérience professionnelle

## 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 3 heures - 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 cyberspace.
- 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 cyberspace, 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 27001 Lead Implementer

## 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

