

DRI CRLE 2000 : orchestrer la cyber-résilience face aux cyberattaques majeures

Date et durée
Code formation : CRLE2000 Durée : 4 jours Nombre d'heures : 32 heures
Description
Face à des cyberincidents majeurs qui paralysent des fonctions essentielles, les organisations recherchent des professionnels capables d'orchestrer la réponse, de la gouvernance jusqu'à la reprise. Dans ces situations dégradées, la cyber-résilience relie cybersécurité, continuité d'activité et gestion de crise, et exige une coordination sans faille entre les acteurs. Cette formation avancée de 4 jours intègre la cyber-résilience dans la gouvernance globale, des 5 éléments de la démarche (préparer, protéger, détecter, répondre, rétablir) à la communication de crise. Vous alternez études de cas, retours d'expérience et exercices, dont une simulation de cyberattaque, pour analyser des scénarios complexes et décider en situation dégradée. À l'issue de ces 4 jours, vous saurez coordonner préparation, réponse et reprise face aux cyberincidents majeurs, et améliorer en continu les dispositifs existants. Vous serez aussi préparé à l'examen de certification DRI, inclus dans notre offre, avant de pouvoir demander la certification ACRP ou CCRP, selon votre expérience (<i>en savoir plus dans l'onglet certification</i>).
Objectifs
À l'issue de cette formation, vous atteindrez les objectifs de compétences suivants : • intégrer la cybersécurité et la continuité d'activité dans un programme de cyber-résilience cohérent ; • analyser les cyberattaques récentes et leurs effets sur la continuité d'activité de l'organisation ; • élaborer les plans de préparation et d'identification, de protection et de détection, puis de réponse et de reprise ; • coordonner la réponse aux cyberincidents et la reprise des opérations entre les équipes concernées ; • défendre la valeur d'un programme de cyber-résilience auprès de la direction pour obtenir les investissements nécessaires ; • concevoir un plan de communication de crise et des actions de sensibilisation qui ancrent la cyber-résilience dans l'organisation ; • se préparer et réussir l'examen de certification DRI, étape requise pour demander la certification ACRP et satisfaire l'exigence de base de la certification CCRP.
Points forts
• Parcours complet : en 4 jours, vous couvrez les cinq éléments de la cyber-résilience, du cadre NIST à la communication de crise, et vous construisez une base solide pour aborder l'examen DRI. • Mises en situation : études de cas, retours d'expérience et simulation de cyberattaque sur table vous entraînent à décider et à coordonner vos équipes en situation dégradée.

- **Examen inclus** : vous passez l'examen de certification en ligne, à votre rythme, ce qui vous ouvre la voie vers les certifications ACRP et CCRP selon votre expérience.
- **Légitimité en entreprise** : vous repartez avec un argumentaire de valeur pour convaincre votre direction d'investir, et la confiance nécessaire pour piloter la réponse à un cyberincident majeur.

Certification

Cette formation prépare à l'examen de certification DRI Cyber Resilience, inclus dans le prix de la formation. Vous le passez en ligne, à votre rythme, une fois les 4 jours de cours terminés.

Modalités de l'examen DRI Cyber Resilience Examination

- **Type d'examen** : questionnaire à choix multiples
- **Lieu** : en ligne
- **Durée** : 02H30
- **Langues** : anglais, japonais, portugais et espagnol
- **Score requis** : 75 % minimum

Une fois l'examen réussi, vous demandez vous-même votre certification sur le site de DRI International (des frais d'émission non compris dans la formation) :

- **ACRP (Associate Cyber Resilience Professional)** : obtenu avec la seule réussite de l'examen, sans condition d'expérience.
- **CCRP (Certified Cyber Resilience Professional)** : accessible avec au moins deux ans d'expérience en cybersécurité, en continuité d'activité ou en reprise informatique, justifiée par des rédactions et des références.

À savoir : des frais annuels s'appliquent pour conserver la certification. La certification CCRP demande 80 crédits de formation continue (CEAP) pour son maintien, alors que l'ACRP n'en exige aucun. Retrouvez toutes les conditions sur le [site officiel de DRI International](#).

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

Aucune expérience préalable n'est nécessaire pour suivre cette formation, cependant les points ci-dessous concernent la langue du cours, l'examen et l'obtention des certifications DRI :

- **Aptitudes linguistiques** : un anglais courant est indispensable, car le cours est dispensé uniquement en anglais et l'examen n'existe pas en français.
- **Expérience professionnelle** : aucune pour la certification ACRP ; pour la certification CCRP, au moins deux ans d'expérience en cybersécurité, en continuité d'activité ou en reprise informatique, à justifier lors de la candidature.

Public

Cette formation s'adresse aux professionnels chargés de piloter, de coordonner ou d'auditer la résilience de leur organisation face aux cyberattaques. Le public inclut notamment :

- les **responsables de la continuité d'activité** qui souhaitent intégrer le risque cyber dans leurs plans ;
- les **responsables de la sécurité de l'information** qui veulent relier cybersécurité et reprise d'activité ;
- les **responsables de la gestion de crise** et de la communication en situation dégradée ;
- les **responsables IT et reprise informatique** impliqués dans la réponse aux cyberincidents ;

- les **consultants, auditeurs et responsables des risques** qui accompagnent la mise en place d'un programme de cyber-résilience.

Programme

Module 1 : passer de la cybersécurité à la cyber-résilience

- Les types de menaces et de cyberattaques récentes.
- La relation de cause à effet entre la cybersécurité et la continuité d'activité.
- Le problème, le défi et l'approche pour franchir le pas vers la cyber-résilience.

Module 2 : s'appuyer sur les cadres de référence

- Le cadre de cybersécurité du NIST et ses grandes fonctions.
- La triade CIA (confidentialité, intégrité, disponibilité) et son lien avec la cyber-résilience.
- Les 5 éléments de la démarche : préparer et identifier, protéger, détecter, répondre, rétablir.

Module 3 : défendre la valeur de la cyber-résilience

- L'argumentaire de valeur à présenter à la direction pour obtenir les investissements nécessaires.
- Le changement de culture indispensable pour atteindre la cyber-résilience.
- Les exigences minimales d'un programme de cyber-résilience.

Module 4 : intégrer cybersécurité et continuité d'activité

- L'analyse d'impact sur l'activité alignée avec la cybersécurité.
- Les points de convergence entre cybersécurité et continuité d'activité.
- La cyber-assurance, les cadres de cybersécurité et les réglementations applicables.

Module 5 : adapter le cadre de cybersécurité pour planifier la cyber-résilience

- La démarche de planification de la cyber-résilience.
- L'adaptation du cadre de cybersécurité aux besoins de l'organisation.

Module 6 : élaborer les plans de préparation, de réponse et de reprise

- Les plans de préparation et d'identification.
- Les plans de protection et de détection.
- Les plans de réponse et de reprise.
- La collaboration entre la réponse aux cyberincidents et la reprise des opérations métiers.

Module 7 : sensibiliser et former pour ancrer la cyber-résilience

- L'importance des formations régulières de sensibilisation aux cybermenaces.
- Les initiatives de formation et de sensibilisation qui préparent le personnel à répondre et à rétablir l'activité.
- Le rôle de la cybersécurité et de la continuité d'activité dans la gestion de la réputation.

Module 8 : maintenir les plans et communiquer en cas de cyberincident

- Le maintien en condition opérationnelle des plans.
- Les plans de communication de crise adaptés aux cyberincidents.

Travaux pratiques

- mener une simulation de cyberattaque sur table et rédiger la synthèse des décisions de réponse et de reprise prises en situation dégradée.

Les noms de marques et logos éventuellement cités dans cette fiche sont la propriété de leurs détenteurs respectifs. Leur mention à des fins pédagogiques ne constitue ni un engagement ni un partenariat.