

Your Cyber INSURANCE



Plan de formation : Information Security Management

Jours	Module	Contenu
1 jour	Introduction à la cybersécurité pour les managers Gestion de la cybersécurité	1. Intégrer la sécurité au sein de l'organisation. 2. Intégrer la sécurité dans les projets. 3. Comprendre les difficultés liées à l'intégration de la sécurité dans la responsabilité de chacun. 4. Les métiers liés à la cybersécurité.
3 jours	Gestion des incidents de cybersécurité Réponse aux incidents cyber	1. Principes de la gestion des incidents de cybersécurité. 2. Normes : ISO 27035 & NIST SP800-61. 3. Mise en œuvre du processus de gestion des incidents de cybersécurité. 4. Exemples de réponses à différents scénarios d'incidents. 5. Passer d'une gestion réactive à une gestion proactive des incidents.
3 jours	ISO 22301 Responsable de la mise en œuvre de la continuité d'activité	1. Identifier les défis liés à la continuité d'activité. 2. Préparer un plan de continuité d'activité (PCA). 3. Mettre en œuvre et assurer la maintenance du plan de continuité d'activité.
5 jours	ISO 27032 LCM Responsable du programme de cybersécurité	1. Fondamentaux de la cybersécurité. 2. Programme de cybersécurité. 3. Mise en place d'un programme de cybersécurité. 4. Leadership et politiques organisationnelles. 5. Gestion de la cybersécurité. 6. Gestion des risques cyber. 7. Cyberattaques et contre-mesures. 8. Continuité d'activité et gestion des incidents cyber.
1 jour	ISO 27001:2022 – Les essentiels du management de la sécurité de l'information	1. Principes fondamentaux de la sécurité de l'information. 2. Processus de certification. 3. Système de management de la sécurité de l'information (SMSI).
3 jours	ISO 27005:2018 Responsable de la gestion des risques	1. Cadre réglementaire et normatif. 2. Concepts et définitions de la gestion des risques. 3. Programme de gestion des risques. 4. Processus de gestion des risques. 5. Communication et surveillance des risques.