Comprendre vos obligations et responsabilités en matière de risques cyber

Objectifs Généraux

Cette formation vise à renforcer la gouvernance en matière de cybersécurité au sein des organisations. Son objectif principal est d'aider les participants à saisir les obligations techniques découlant des réglementations et des normes en vigueur, sans se plonger dans les détails de leur exécution.

La formation met l'accent sur l'autonomisation des apprenants pour qu'ils puissent élaborer une stratégie de conformité efficace, adaptée à leur niveau et à leur département.

Elle fournit des outils et des méthodologies pratiques pour identifier les exigences spécifiques et mettre en œuvre des stratégies de remédiation, telles que la protection des données personnelles et la gestion des incidents de sécurité. De plus, cette formation promeut une approche proactive de la cybersécurité en sensibilisant les participants aux meilleures pratiques et en leur permettant de contribuer activement à l'application de mesures de sécurité adaptées à leur organisation.

Aptitudes clefs visées

1. **Développer des stratégies de gouvernance IT responsables** pour sécuriser efficacement les infrastructures critiques, en intégrant des pratiques alignées sur les standards internationaux (ISO, NIST), dans une optique de gouvernance durable (ESG).
2. **Maîtriser les principes fondamentaux de la gestion des incidents de sécurité** en adoptant une approche proactive pour identifier, répondre et remédier aux menaces cyber, tout en limitant l'impact sur la continuité des opérations.
3. **Garantir la résilience des activités grâce à des plans PCA/PRA** adaptés aux risques identifiés, en assurant la continuité des services essentiels même en cas d'incident majeur, tout en respectant les exigences légales et contractuelles.
4. **Comprendre les obligations légales et les responsabilités des entreprises** dans la gestion des incidents cyber, tant vis-à-vis des clients que des prestataires, en se préparant à répondre aux attentes des autorités de régulation et des assureurs, dans le cadre d'une approche juridique rigoureuse.
5. **Intégrer la conformité réglementaire liée à la protection des données (RGPD, etc.)** et aux exigences européennes dans une stratégie globale de gestion des risques, en assurant une gouvernance qui respecte les principes de transparence, d'éthique et de protection des parties prenantes.

Programme détaillé

JOUR 1 : Enjeux techniques et responsabilité dans la cybersécurité : de quoi parle-t-on?

Introduction à la cyber-responsabilité
- Présentation des objectifs de la formation et de la notion de cyber-éthique
- Comprendre pourquoi une approche responsable est essentielle en matière de Cybersécurité

I. Panorama des menaces cyber et techniques de cyberattaques :
- Présentation des principales cybermenaces (ransomware, phishing, DDoS, etc.)
- Étude de cas sur des exemples d'attaques récentes et leurs conséquences
Démonstration des techniques d'attaques courantes

II. Gouvernance des systèmes d'information
- Définition des rôles et responsabilités des acteurs internes et externes
- Introduction aux processus de gouvernance des systèmes d'information (ISO 27001, NIST)
- Intégration de la responsabilité dans la gouvernance IT

III. Sécurisation des infrastructures et gestion des incidents
- Bonnes pratiques de sécurité (pare-feu, gestion des identités, surveillance)
- Stratégies d'intervention face aux incidents de sécurité et présentation des outils de détection et de réponse

IV. Plan de continuité d'activité (PCA) et reprise après sinistre (PRA)
- Différences entre PCA et PRA
- Élaboration d'une stratégie pour assurer la continuité des opérations en cas d'incident
- Importance des sauvegardes et leur gestion

V. Synthèse des concepts abordés et retour sur les exercices réalisés.

JOUR 2 : Aspects juridiques et gestion des risques cyber

Introduction à la journée et enjeux juridiques en cybersécurité
Présentation du cadre juridique en matière de cybersécurité, incluant les principales lois (RGPD, Cybersecurity Act, etc.) et leur impact sur les entreprises

I. Responsabilité légale des entreprises en cas d'incident cyber :
- Présentation des responsabilités civiles et pénales des entreprises
- Études de cas sur la jurisprudence récente liée aux incidents cyber et aux poursuites Judiciaires

II. RGPD et autres réglementations connexes
- Impacts du RGPD et des autres législations sur la gestion des risques cyber.
- Comment se conformer à ces réglementations et éviter les sanctions ?
- Introduction aux DPIA (analyses d'impact)

III. Gestion des contrats et des sous-traitants en matière de cybersécurité

- Importance des clauses de sécurité dans les contrats
- Responsabilité partagée entre entreprise et sous-traitants
- Étude des obligations juridiques en cas de violation de données par un sous-traitant

IV. Gestion des risques cyber et assurance

- Introduction à la cyberassurance, ses couvertures et exclusions
- Comment évaluer les besoins en cyberassurance et déterminer les critères d'éligibilité

Conclusion générale : synthèse de la formation et perspectives

Récapitulatif des points-clés abordés et discussion sur des actions pratiques pour intégrer une cyberresponsabilité accrue dans son organisation.

Méthodes pédagogiques

- Présentations interactives
- Études de cas pratiques et correction
- Quiz et exercices de mise en situation systématique par notion abordée
- Discussions et échanges collectifs, mise en perspective par rapport au quotidien des apprenants
- Partage de bonnes pratiques

Public concerné

- Responsables juridiques, Compliance officers, Administrateurs de société, Consultant en gouvernance d'entreprise, Consultant en stratégie d'entreprise, Data protection Officers DPO,
- Dirigeants d'organisations et d'entreprises, Directeur financier (CFO), Directeur de la sécurité (CSO), CRO (Directeur des risques)
- Consultants en ESG cherchant à mieux appréhender le G, Consultant en IT, Consultant en risque

Prérequis

Aucun prérequis nécessaire

Mise en œuvre

- Formation en visio-conférence ou présentiel selon dates des sessions – consulter notre planning
- Nombre de journées : 2 jours soit 14 heures
- Nombre minimum de participants : 4
- Nombre maximum de participants : 12
- Adaptations possibles des conditions d'accueil et d'animation selon besoin(s) spécifique(s) du participant, merci de contacter notre référent handicap au moins 2 mois avant la session envisagée via cette adresse : formation@agence-lucie.com

Bien se préparer :

- Bien lire le mail de convocation et répondre au questionnaire concernant vos attentes particulières.

Tarifs et planification

- Sessions collectives : 1200€ H.T. par participant
- Consultez notre planning de sessions,
- Inscription : pour vous inscrire, merci de nous demander une proposition de convention de formation, afin de vous préinscrire, l'inscription finale se faisant à réception de celle-ci et y définir les modalités de règlement. Pré-inscription jusqu'à 10 jours avant la date de début de la formation. Inscription définitive jusqu'à 5 jours avant la date de début de la formation.
- Possibilité d'organiser des sessions propres à votre organisation dans vos locaux
- Possibilité de décliner ce programme en une variante sur-mesure simplifiée pour un public plus large d'initiation à la démarche RSE au sein de votre entreprise.
- Faire votre demande d'inscription : formation@agence-lucie.com

Animateur(s) / Animatrice(s)

Présentation de la formatrice

Sarah ZOUAKI

- **Fondatrice de blueInnovate** spécialisée dans la détection des risques de conformité liés à la données (cybersécurité, conformité RGPD, NIS 2, AI Act)
- **+5 ans d'expérience** en conseil stratégique et juridique pour des entreprises technologiques et financières
- **Expertises** : Réglementations européennes, conformité ESG, protection des données et cybersécurité
- **Intervenante régulière** sur les enjeux de l'IA , de la sécurité et de l'éthique numérique
- Master en Management (**ESSEC**) et en droit (**Sciences Po**)
- **LinkedIn - Sarah Zouaki**

Validation des aptitudes

- ✓ La méthodologie d'évaluation des acquis de cette formation repose sur plusieurs étapes, permettant de vérifier la compréhension et l'application des concepts enseignés.
- ✓ Tout au long de la formation, des évaluations continues telles que **des quiz intermédiaires** et **des études de cas pratiques** seront réalisées pour suivre les progrès des participants.
- ✓ En fin de formation, **un questionnaire à choix multiples (QCM) en ligne** mesurera les connaissances acquises, avec un score minimum requis pour valider la formation.