Plan de formation FRANÇAIS (English below)

Gestion du risque cyber au Luxembourg

Durée : 1 heure – Approche opérationnelle, orientée risques, résilience et conformité démontrable

---

1. **Objectifs et approche de la formation**

• Comprendre le risque cyber comme un risque métier

• Identifier les principales menaces et vulnérabilités

• Développer des réflexes de prévention, d'escalade et de gestion des incidents

• Approche pédagogique : identifier – analyser – prioriser – traiter – réagir

2. **Compréhension du risque cyber**

• Principales cybermenaces : phishing, rançongiciels, BEC, DDoS

• Risques liés aux fournisseurs et aux tiers

• Fuites de données et fraudes assistées par l'IA

• Impacts opérationnels, financiers et réputationnels

3. **Cadre réglementaire et contexte luxembourgeois**

• Principes de résilience opérationnelle numérique

• Protection des données personnelles

• Attentes réglementaires au Luxembourg

• Références à DORA, CSSF, GDPR et CNPD

4. **Approche fondée sur les risques (Risk-Based Approach)**

- Identification et évaluation des risques cyber
- Actifs critiques, vulnérabilités et menaces
- Risque inhérent, risque résiduel et appétence au risque
- Priorisation selon l'impact et la vraisemblance

5. **Identification des situations à risque**

- Signaux d'alerte et comportements suspects
- Risques liés aux accès et aux fournisseurs
- Scénarios d'incidents plausibles
- Distinction entre incident mineur et incident majeur

6. **Surveillance et détection**

- Contrôles de sécurité et mécanismes d'alerte
- Authentification multifacteur et sauvegardes
- Détection précoce des incidents

7. **Réponse aux incidents et gestion de crise**

- Analyse et qualification des incidents
- Processus d'escalade et de communication
- Premières mesures de confinement
- Retour d'expérience et amélioration continue

8. **Mesures de protection et de résilience**

- Prévention et réduction de l'exposition
- Plans de continuité et de reprise d'activité
- Sensibilisation des utilisateurs
- Gestion du risque fournisseur

9. **Gouvernance et organisation interne**

- Rôles et responsabilités des parties prenantes
- Coordination entre métiers, IT, sécurité et conformité
- Reporting et suivi des risques
- Gestion du risque tiers

10. **Synthèse opérationnelle et évaluation**

- Méthode clé : identifier – analyser – prioriser – traiter – réagir
- Réflexes essentiels à adopter au quotidien
- Feuille de route d'amélioration continue
- Évaluation finale des connaissances

ENGLISH VERSION

Cyber Risk Management in Luxembourg

Duration: 1 hour – Operational approach focused on risk management, resilience, and demonstrable compliance

1. **Training Objectives and Approach**

• Understand cyber risk as a business risk

• Identify key cyber threats and vulnerabilities

• Develop practical prevention, escalation, and incident-management reflexes

• Training approach: identify – analyse – prioritise – treat – respond

2. **Understanding Cyber Risk**

• Key cyber threats: phishing, ransomware, BEC, and DDoS attacks

• Supplier and third-party risks

• Data breaches and AI-enhanced fraud

• Operational, financial, and reputational impacts

3. **Regulatory Framework and Luxembourg Context**

• Principles of digital operational resilience

• Personal data protection requirements

• Regulatory expectations in Luxembourg

• References to DORA, CSSF, GDPR, and CNPD

4. **Risk-Based Approach**

- Identification and assessment of cyber risks
- Critical assets, vulnerabilities, and threats
- Inherent risk, residual risk, and risk appetite
- Prioritisation based on impact and likelihood

5. **Identifying High-Risk Situations**

- Warning signs and suspicious activities
- Access-related and supplier-related risks
- Plausible incident scenarios
- Distinction between minor and major incidents

6. **Monitoring and Detection**

- Security controls and alert mechanisms
- Multi-factor authentication and backups
- Early detection of incidents

7. **Incident Response and Crisis Management**

- Incident analysis and classification
- Escalation and communication processes
- Initial containment measures
- Lessons learned and continuous improvement

8. Protection and Resilience Measures

- Prevention and exposure reduction
- Business continuity and disaster recovery planning
- User awareness and training
- Third-party risk management

9. Governance and Internal Organisation

- Roles and responsibilities of key stakeholders
- Coordination between business, IT, security, and compliance functions
- Risk reporting and monitoring
- Third-party risk oversight

10. Operational Summary and Assessment

- Key methodology: identify – analyse – prioritise – treat – respond
- Essential day-to-day reflexes and best practices
- Continuous improvement roadmap
- Final knowledge assessment