LES CONSULTANTS
CONSEIL & FORMATION

EN

CYBERSECURITY · LUXEMBOURG

Cyber Risk Management in Luxembourg

Operational approach focused on risk management, resilience, and demonstrable compliance.

▲ Duration: 1 hour ▲ Method: identify – analyse – prioritise – treat – respond

1. TRAINING OBJECTIVES AND APPROACH

▲ Training objectives

1. Understand cyber risk as a business risk.
2. Identify key cyber threats and vulnerabilities.
3. Develop practical prevention, escalation, and incident-management reflexes.
4. Training approach: identify – analyse – prioritise – treat – respond.

10 CHAPTERS · DURATION 1 HOUR

▲ Training programme

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.

KEY METHODOLOGY

Identify – analyse – prioritise – treat – respond.