Future-Oriented Training and Consulting

EXECUTIVE DEVELOPMENT PROGRAM

Cybersecurity Governance, Risk

& Compliance (GRC)

Aligning cybersecurity practices with governance, risk, and regulatory compliance.

Proven GRC Frameworks Structured frameworks for building compliance and risk programs.	**Executive Case Studies** Real-world examples of GRC programs and regulatory response.
Hands-On Tool Exposure Direct exposure to GRC frameworks and compliance tools.	**Practical Compliance Program** Builds a practical compliance and risk management program.

CONTACT & HEADQUARTERS

www.lux-vie.com | Email: contact@lux-vie.com | Tel: +33-614620984

Address: 50 AVENUE DES CHAMPS ELYSEES, 75008 PARIS

Program Overview

This program builds the skills to align cybersecurity practices with governance, risk, and regulatory compliance requirements.

Through case studies, executive discussions, simulations, and hands-on exposure to GRC frameworks and tools, participants will develop a practical compliance and risk management program for their organization.

Program Objectives

- **Understand GRC Fundamentals:** Grasp how governance, risk, and compliance fit together.
- **Assess Organizational Risk Posture:** Identify where cyber risk threatens business objectives.
- **Apply GRC Frameworks and Tools:** Use recognized frameworks to structure a GRC program.
- **Navigate Regulatory Requirements:** Map applicable laws and standards to business operations.
- **Build a Risk Management Program:** Design processes to identify, treat, and monitor risk.
- **Lead GRC Implementation:** Build the roadmap and leadership skills to drive adoption.

Target Audience

This program is designed for professionals responsible for cybersecurity governance, risk, and compliance, including:

- **Chief Information Security Officers** setting security governance and risk strategy.
- **Risk & Compliance Managers** building and running compliance programs.
- **Internal & IT Auditors** assessing control effectiveness and gaps.
- **Legal & Regulatory Affairs Professionals** interpreting regulatory obligations.
- **Security & IT Managers** implementing controls that satisfy auditors.
- **Consultants & GRC Advisors** guiding clients through compliance programs.
- **Business Owners & Executives** accountable for organizational risk exposure.

Program Impact

Participants will complete this program with a practical compliance and risk management program. Graduates will return to their organizations ready to align cybersecurity practices with governance, risk, and regulatory requirements.

Program Outline

MODULE 1: Foundations of Cybersecurity GRC

- How governance, risk, and compliance interconnect
- The business case for a formal GRC program
- Roles and responsibilities across the GRC function
- Overview of major GRC and security frameworks
- Assessing organizational GRC maturity

MODULE 2: Cybersecurity Governance

- Establishing security policy and governance structures
- Aligning security governance with business strategy
- Defining roles, accountability, and reporting lines
- Benchmarking governance against industry standards
- Setting measurable governance targets

MODULE 3: Risk Assessment and Management

- Identifying and classifying cyber risk
- Assessing likelihood, impact, and risk appetite
- Using risk assessment and register tools
- Prioritizing risk treatment and mitigation

MODULE 4: Regulatory and Legal Landscape

- Key data protection and cybersecurity regulations
- Sector-specific compliance requirements
- Cross-border and multi-jurisdictional obligations
- Managing legal exposure from non-compliance
- Hands-on exposure to compliance tracking tools

MODULE 5: Frameworks and Control Implementation

- Applying frameworks such as NIST and ISO 27001
- Mapping controls to regulatory requirements
- Implementing and testing security controls
- Hands-on exposure to GRC platforms

MODULE 6: Third-Party and Vendor Risk Management

- Assessing vendor and supply chain risk
- Contractual and due diligence requirements
- Ongoing monitoring of third-party relationships
- Managing risk from fourth parties and subcontractors
- Building a vendor risk management process

MODULE 7: Auditing, Monitoring, and Reporting

- Key performance and risk indicators for GRC
- Conducting internal audits and control testing
- Tracking remediation and compliance progress
- Reporting GRC status to boards and regulators

MODULE 8: Incident Response and Compliance Readiness

- Aligning incident response with regulatory obligations
- Managing breach notification and disclosure requirements
- Preparing for regulatory audits and examinations

MODULE 9: Leading GRC Implementation

- Leading teams through GRC program adoption
- Overcoming resistance to compliance requirements
- Communicating risk and compliance status effectively
- Building a culture of accountability and compliance

MODULE 10: Sustaining GRC Programs and Future Readiness

- Embedding GRC into long-term business strategy
- Anticipating emerging regulations and risk trends
- Sustaining momentum beyond the program