skillsoft global knowledge™

CYBERSECURITY SPECIALIZATION: GOVERNANCE RISK AND COMPLIANCE

Course Code: 6974

Acquire the skills to design a system of governance to enforce compliance with laws, regulations, and company policies.

In an ever-changing political and criminal landscape, there is an increasing need for people with specialized and up-to-date knowledge of current cybersecurity laws, regulations, and best practices. The skills gap this need creates in an organization exposes the organization to liability.

Cybersecurity Specialization: Governance, Risk, and Compliance will give you an understanding of the current laws and regulations that drive the creation of a governance system of rules, practices, and processes by which a company is directed and controlled. Understanding the fundamentals of the implementation of a risk management strategy will help your organization achieve compliance through policy management, control creation, and assessment of the effectiveness of controls. In this course, you will learn to set up processes to enforce compliant behaviors in your organization, including the enforcement of a systemic culture of documentation, verification, audits, remediation, follow-through, responsibility, and authority.

The course uses a challenge-based design focusing on what a learner should be able to do at the end of the course and back on the job. The practice opportunities and challenge activities resemble—as much as possible—tasks the learner would be asked to perform in a real-life situation.

What You'll Learn

- Develop a strategy to mitigate compliance risk based on laws governing Information Technology and reporting requirements to various regulatory bodies
- Contribute to a risk management strategy that will frame an organization’s risk tolerance along with defining and enabling managers to understand the levels of risk they are allowed to take
- Create policies supported by controls that utilize frameworks and standards to minimize risk to an acceptable level
- Determine the mechanisms to raise the organization’s risk maturity level
- Support both top-down and bottom-up approaches to enterprise security by

acquiring management buy-in and improving employee attitudes to security
- Contribute to a business continuity plan that prioritizes business processes
- Select an eGRC tool to help manage risk based on requirements and capabilities

Who Needs to Attend

- Mid-career professionals who are interested in a career in risk analysis and management of cybersecurity processes, tools, and people.
- Students should have at least two years of experience in cybersecurity but can come to this course from a variety of backgrounds, including but not limited to auditing, project management, DevOps, and engineering.

skillsoft global knowledge™

CYBERSECURITY SPECIALIZATION: GOVERNANCE RISK AND COMPLIANCE

Course Code: 6974

VIRTUAL CLASSROOM LIVE	$2,550 USD	3 Day

Virtual Classroom Live Outline

Why Does GRC Matter?

- Terms and definitions
- Assets, value
- Increasing importance of Governance, Risk, and Compliance

Industry Compliance

- Essence of compliance
- Industry Standards: Payment Card Industry (PCI)
- Industry Standards: Sarbanes-Oxley (SOX) Act
- Industry Standards: Financial Industry Regulatory Authority (FINRA)
- Industry Standards: General Data Protection Regulation (GDPR)
- Compliance and company policy

Privacy Compliance

- Impact of privacy
- Personally identifiable information (PII), protected health information (PHI)
- Data architecture
- Data handling
- Encryption
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Gramm-Leach-Bliley Act (GLBA)
- Privacy best practices

Risk Assessment

- CIA triad
- Threat modeling
- Risk assessment

- Quantitative vs. qualitative risk assessment
- Risk assessment models
- Risk likelihood and impact
- Risk tolerance
- Risk appetite
- Business impact analysis (BIA)
- Risk mitigation strategies

Risk Management

- Risk management strategies: Mitigation, avoidance, transference, acceptance
- Risk Management Framework (RMF)
- RMF vs. CAP
- Risk maturity level
- Residual risk
- Continuous monitoring and incident response
- Patch management and the Common Vulnerability Scoring System (CVSS)

Corporate Culture

- Enterprise-wide attitudes to security and risk
- FUD: Fear, uncertainty, and doubt
- Governance failures in the real world
- Buy-in
- NICE, best practices, role-based training
- Aligning risk management with business goals
- Authorized use policies
- Tools: Training, rewards and consequences, hiring practices
- Ongoing monitoring and tracking

Governance and Policy

- Business continuity plan (BCP)
- Disaster recovery plan (DRP)
- Business impact analysis (BIA)
- Single point of failure
- Redundancy
- BCP dependency chain
- Rapid information sharing
- RACI chart
- Discussion: Fast vs. good vs. cheap

Course Look Around

- eGRC: Archer and OpenPages
- Real-time access to information
- Reporting
- Relevance
- Interoperability
- Savings through reduced complexity

Virtual Classroom Live Labs

- Challenge: Why does GRC matter?
- Challenge: Collaborate on compliance solutions
- Challenge: Identify and classify PII
- Challenge: Calculate risk
- Challenge: Choose a risk management strategy
- Challenge: Adjust corporate culture
- Challenge: Develop a DRP and integrate it with the BCP
- Challenge: Explore eGRC tools

May 12 - 14, 2025 | 8:30 AM - 4:30 PM EDT

Jul 28 - 30, 2025 | 8:30 AM - 4:30 PM EDT

Sep 22 - 24, 2025 | 8:30 AM - 4:30 PM EDT

Nov 10 - 12, 2025 | 8:30 AM - 4:30 PM EST

CYBERSECURITY SPECIALIZATION: GOVERNANCE RISK AND COMPLIANCE

Course Code: 6974

PRIVATE GROUP TRAINING	3 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/17/2025 10:08:29 AM