SKILLSLAB
Training Provider

COURSE BROCHURE

Cybersecurity Governance, Risk and Compliance – Advanced GRC Management and Information Security

Professional Training Course

Skillslab Training Provider
Skills for Tomorrow's World

info@skillslab-training.com | +966 55 965 3447 | www.skillslab-training.com

Course Description

INTRODUCTION

Organizations operate in increasingly interconnected digital environments where cybersecurity threats, regulatory requirements, and stakeholder expectations continue to evolve. Effective cybersecurity governance, risk management, and compliance practices are essential for protecting sensitive information and maintaining business continuity. Institutions must establish clear accountability structures, implement appropriate security controls, and demonstrate compliance with applicable laws and industry standards. This course introduces participants to the principles, frameworks, and practical tools required to build an integrated cybersecurity governance and compliance program. It explores the relationship between corporate governance, information security management, enterprise risk management, and organizational strategy. Participants will examine methods for identifying cybersecurity risks, assessing regulatory obligations, and evaluating the effectiveness of security controls. The program also addresses policy development, compliance monitoring, internal auditing, third-party assurance, and management reporting. Practical exercises demonstrate how to develop cybersecurity governance frameworks, risk registers, compliance matrices, and performance dashboards. Through structured learning and applied case studies, participants will develop the capabilities required to support informed decision-making and continuous improvement in cybersecurity governance.

COURSE OBJECTIVES

Participants will achieve the following objectives by this course:

- Understand cybersecurity governance, risk management, and compliance principles and their organizational importance.
- Align cybersecurity governance strategies with business objectives, regulatory obligations, and enterprise risk management.

- Apply internationally recognized cybersecurity governance and information security management frameworks.
- Establish effective cybersecurity governance structures, policies, responsibilities, and accountability mechanisms.
- Identify, assess, prioritize, and manage cybersecurity risks using structured assessment methodologies.
- Develop cybersecurity compliance programs aligned with applicable laws, regulations, and industry standards.
- Evaluate information security controls and assess their effectiveness in managing organizational risks.
- Strengthen third-party cybersecurity risk management, supplier assurance, and contractual compliance.
- Design cybersecurity governance dashboards, compliance reports, and key performance indicators.
- Implement continuous monitoring, internal auditing, and improvement processes for cybersecurity governance and compliance.

TARGET AUDIENCE

This program targets a professional audience seeking to improve knowledge and skills:

- Cybersecurity managers responsible for developing security governance frameworks and organizational protection strategies.
- Information security officers overseeing cybersecurity policies, compliance requirements, and risk management activities.
- Governance, risk, and compliance professionals managing regulatory obligations and organizational security controls.
- Enterprise risk managers assessing cybersecurity exposure and integrating digital risks into corporate frameworks.
- Internal auditors evaluating cybersecurity governance effectiveness, control implementation, and regulatory compliance.
- Information technology directors responsible for aligning technology security with business and governance objectives.
- Legal and regulatory compliance officers addressing information security laws and contractual obligations.
- Business continuity managers coordinating cybersecurity resilience and operational risk management.

- Senior executives and board representatives overseeing cybersecurity accountability and strategic risk decisions.
- Security consultants advising organizations on governance maturity and compliance improvement.

COURSE OUTLINE

Day 1: Cybersecurity Governance Foundations and Strategic Alignment

- Understanding cybersecurity governance, risk management, and compliance concepts.
- Examining the strategic importance of integrated cybersecurity governance frameworks.
- Exploring internationally recognized cybersecurity governance and information security standards.
- Understanding board oversight, executive accountability, and cybersecurity leadership responsibilities.
- Aligning cybersecurity objectives with organizational strategy and business priorities.
- Defining cybersecurity risk appetite, tolerance, and governance principles.
- Establishing cybersecurity governance committees, reporting structures, and decision-making authorities.
- Developing information security policies, standards, procedures, and governance documentation.
- Integrating cybersecurity governance with enterprise risk management and corporate governance.
- Practical exercise: Designing an organizational cybersecurity governance structure.

Day 2: Cybersecurity Risk Assessment and Enterprise Risk Integration

- Identifying cybersecurity threats, vulnerabilities, and critical information assets.
- Understanding cyber risk assessment methodologies and evaluation criteria.
- Assessing cybersecurity risk likelihood, impact, and organizational exposure.
- Developing risk registers and structured cybersecurity risk classification systems.
- Applying qualitative and quantitative cyber risk assessment techniques.
- Establishing risk ownership, accountability, and escalation procedures.
- Evaluating cybersecurity risk treatment options and control priorities.
- Integrating cybersecurity risks into enterprise risk management processes.
- Assessing emerging technology risks and digital transformation challenges.

- Practical workshop: Conducting a cybersecurity risk assessment and treatment planning exercise.

Day 3: Cybersecurity Compliance Frameworks and Regulatory Requirements

- Understanding cybersecurity regulatory environments and organizational compliance obligations.
- Exploring information security management standards and compliance frameworks.
- Identifying applicable legal, contractual, and industry-specific security requirements.
- Developing cybersecurity compliance policies and regulatory obligation registers.
- Establishing compliance monitoring procedures and control verification processes.
- Evaluating data protection, privacy, and information handling requirements.
- Managing third-party compliance obligations and supplier security assurance.
- Preparing regulatory compliance assessments and supporting documentation.
- Identifying compliance gaps and developing corrective action plans.
- Practical exercise: Building a cybersecurity compliance matrix and remediation plan.

Day 4: Security Controls, Internal Auditing and Third-Party Assurance

- Understanding cybersecurity control objectives and risk-based control selection.
- Designing administrative, technical, and physical security control frameworks.
- Evaluating security control design and operational effectiveness.
- Establishing internal cybersecurity audit plans and assessment criteria.
- Conducting control testing, evidence collection, and audit documentation.
- Identifying control deficiencies and assessing associated business risks.
- Developing audit findings, recommendations, and management action plans.
- Assessing supplier cybersecurity risks and third-party control effectiveness.
- Monitoring remediation activities and validating corrective action implementation.
- Practical workshop: Performing a cybersecurity control assessment and audit review.

Day 5: Cybersecurity Reporting, Performance Monitoring and Governance Improvement

- Establishing cybersecurity governance monitoring and compliance reporting processes.

- Developing key risk indicators and cybersecurity governance performance metrics.
- Designing executive dashboards for cybersecurity risk and compliance oversight.
- Preparing board-level cybersecurity reports and management recommendations.
- Monitoring regulatory changes and emerging cybersecurity governance requirements.
- Evaluating cybersecurity governance maturity and organizational control effectiveness.
- Strengthening incident oversight, accountability, and regulatory notification procedures.
- Developing continuous improvement strategies for governance and compliance programs.
- Creating cybersecurity governance roadmaps and implementation priorities.
- Final practical exercise: Presenting an integrated cybersecurity governance, risk, and compliance strategy.

COURSE DURATION

This training program is delivered over five consecutive days, with approximately five hours of structured learning per day, totaling 25 instructional hours. The program combines instructor-led presentations, practical workshops, group discussions, cybersecurity risk assessment exercises, compliance case studies, and governance simulations. Participants will develop practical documents, including governance structures, cybersecurity risk registers, compliance matrices, internal audit checklists, and executive reporting dashboards. The course can be delivered through classroom-based sessions, live virtual training, or customized in-house programs according to organizational requirements and participant experience levels.

INSTRUCTOR INFORMATION

The program is delivered by an internationally certified expert with extensive practical and consulting experience in cybersecurity governance, information security management, enterprise risk management, and regulatory compliance. The instructor possesses practical expertise in cybersecurity governance frameworks, information security standards, internal auditing, risk assessment, compliance monitoring, and organizational security improvement. Training emphasizes internationally recognized professional practices, realistic case studies, and practical governance exercises to ensure participants can apply the acquired knowledge effectively within their organizations.

FREQUENTLY ASKED QUESTIONS

1. What is the main purpose of this course? The course develops practical capabilities for establishing cybersecurity governance frameworks, managing digital risks, and maintaining regulatory compliance.
2. Is this course suitable for professionals without advanced technical cybersecurity experience? Yes, the program focuses on governance, risk management, compliance, and security oversight rather than advanced technical operations.
3. Which cybersecurity standards and frameworks are addressed? The course examines recognized approaches, including ISO 27001, ISO 27005, the NIST Cybersecurity Framework, and COBIT governance principles.
4. Does the course include practical governance and compliance exercises? Yes, participants develop cybersecurity risk registers, compliance matrices, governance structures, audit checklists, and reporting frameworks.
5. Which organizations can benefit from this training? The program is suitable for government institutions, financial organizations, energy companies, technology providers, and regulated businesses.

CONCLUSION

Effective cybersecurity governance, risk management, and compliance are essential for protecting organizational information assets and maintaining accountability in complex digital environments. This course provides professionals with structured methodologies and practical tools for developing governance frameworks, evaluating cyber risks, and strengthening regulatory compliance. Participants will improve their ability to establish security policies, assess control effectiveness, manage third-party risks, and communicate cybersecurity exposure to senior management. The program also strengthens internal auditing, performance monitoring, and continuous improvement capabilities required for sustainable cybersecurity governance. By applying the knowledge and techniques gained, participants can enhance organizational resilience, improve regulatory readiness, and support informed strategic decision-making.

Contact Us

For registration inquiries, upcoming dates, or group pricing, please contact us:

Website	www.skillslab-training.com
Email	info@skillslab-training.com
WhatsApp	+966 559 653 447

Generated by Skillslab Training

info@skillslab-training.com | WhatsApp: +966 559 653 447

www.skillslab-training.com