SKILLSLAB
Training Provider

COURSE BROCHURE

Cybersecurity Controls and Risk Management – Advanced Security Governance, Risk Assessment and Cyber Defense

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 increasingly depend on interconnected technologies, cloud platforms, digital services, and information systems to deliver essential business operations. This growing digital dependence exposes institutions to cybersecurity threats that can disrupt services, compromise sensitive information, and generate substantial financial and reputational losses. Effective cybersecurity controls and risk management provide a structured approach to identifying vulnerabilities, evaluating threats, and protecting critical organizational assets. This course introduces participants to the essential principles, frameworks, and practical techniques required to establish a risk-based cybersecurity management program. It explores the relationship between information security governance, organizational risk appetite, regulatory requirements, and strategic business objectives. Participants will examine methods for assessing cyber threats, identifying security weaknesses, and selecting appropriate technical, administrative, and physical controls. The program also addresses cybersecurity risk assessment, control implementation, incident management, and security performance monitoring. Practical exercises demonstrate how to develop risk registers, evaluate security controls, prepare risk treatment plans, and communicate cybersecurity exposure to management. Through structured learning and applied case studies, participants will develop the capabilities required to manage cyber risks proactively and improve organizational security maturity.

COURSE OBJECTIVES

Participants will achieve the following objectives by this course:

- Understand cybersecurity risk management principles and their importance in protecting organizational information assets.
- Apply internationally recognized cybersecurity frameworks and security governance practices to organizational environments.

- Identify cyber threats, system vulnerabilities, and potential security risks affecting business operations.
- Conduct structured cybersecurity risk assessments using qualitative and quantitative evaluation techniques.
- Design and implement preventive, detective, and corrective cybersecurity controls based on risk priorities.
- Evaluate information security controls and identify opportunities for improving their effectiveness.
- Develop cybersecurity risk registers, risk treatment plans, and security performance indicators.
- Strengthen identity management, access controls, data protection, and third-party cybersecurity risk management.
- Establish effective incident response, business continuity, and cyber resilience management procedures.
- Communicate cybersecurity risks to stakeholders and support continuous improvement of organizational security capabilities.

TARGET AUDIENCE

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

- Cybersecurity managers responsible for protecting organizational systems, networks, and sensitive information assets.
- Information security officers overseeing security governance, compliance, and enterprise cybersecurity risk management.
- Risk managers and analysts evaluating cyber threats and organizational exposure to security incidents.
- Information technology managers responsible for infrastructure security, cloud environments, and operational resilience.
- Internal auditors assessing cybersecurity controls, risk management practices, and regulatory compliance requirements.
- Governance and compliance professionals developing information security policies and organizational control frameworks.
- Business continuity managers coordinating cyber incident preparedness and organizational recovery capabilities.
- Project managers implementing digital transformation initiatives involving cybersecurity and information protection requirements.

- Senior executives overseeing cybersecurity investments, organizational resilience, and strategic technology risks.
- Security consultants advising organizations on cybersecurity maturity and risk mitigation.

COURSE OUTLINE

Day 1: Cybersecurity Fundamentals, Governance and Risk Management Frameworks

- Understanding cybersecurity principles, objectives, and organizational security responsibilities.
- Examining the evolving cyber threat landscape and emerging security challenges.
- Identifying critical information assets and business processes requiring protection.
- Exploring internationally recognized cybersecurity frameworks and risk management standards.
- Understanding security governance structures, policies, and accountability mechanisms.
- Defining cybersecurity risk appetite, tolerance, and risk acceptance criteria.
- Establishing roles and responsibilities for cybersecurity risk management.
- Integrating cybersecurity governance with enterprise risk management and business objectives.
- Developing cybersecurity policies, procedures, and security management documentation.
- Practical exercise: Establishing a cybersecurity governance and risk management framework.

Day 2: Cyber Risk Identification, Threat Assessment and Vulnerability Management

- Identifying internal and external cybersecurity threats affecting organizational systems.
- Understanding common cyberattack techniques and potential business consequences.
- Assessing vulnerabilities across networks, applications, endpoints, and cloud environments.
- Developing asset inventories and identifying critical security dependencies.
- Applying structured cyber risk identification and assessment methodologies.
- Evaluating threat likelihood, vulnerability severity, and potential business impact.
- Using risk matrices to classify and prioritize cybersecurity risks.
- Developing and maintaining comprehensive cybersecurity risk registers.
- Assessing third-party, supplier, and technology service provider security risks.

- Practical workshop: Conducting a cybersecurity risk assessment for an organizational environment.

Day 3: Cybersecurity Controls Design, Implementation and Effectiveness Assessment

- Understanding preventive, detective, corrective, and compensating cybersecurity controls.
- Designing risk-based technical, administrative, and physical security controls.
- Implementing identity and access management and least privilege principles.
- Strengthening authentication, authorization, and privileged access management practices.
- Applying network security controls and secure system configuration practices.
- Establishing data classification, encryption, and information protection controls.
- Managing vulnerabilities through patch management and security remediation procedures.
- Evaluating cloud security controls and shared responsibility requirements.
- Testing control design, operational effectiveness, and security compliance.
- Practical exercise: Developing a cybersecurity control matrix and effectiveness assessment.

Day 4: Cybersecurity Risk Treatment, Incident Response and Business Resilience

- Developing cybersecurity risk treatment strategies aligned with organizational priorities.
- Applying risk avoidance, mitigation, transfer, and acceptance approaches.
- Evaluating security investments using risk reduction and cost-benefit analysis.
- Establishing incident detection, reporting, escalation, and response procedures.
- Defining cybersecurity incident management roles and communication responsibilities.
- Developing cyber incident response plans and recovery procedures.
- Integrating cybersecurity risk management with business continuity planning.
- Assessing ransomware preparedness, backup protection, and recovery capabilities.
- Managing residual risks and evaluating risk treatment effectiveness.
- Practical workshop: Preparing a cybersecurity risk treatment and incident response plan.

Day 5: Cybersecurity Monitoring, Compliance, Reporting and Continuous Improvement

- Establishing continuous cybersecurity risk monitoring and control review processes.

- Developing key risk indicators and cybersecurity performance metrics.
- Monitoring security events, vulnerabilities, and emerging cyber threats.
- Conducting cybersecurity control assessments and internal security audits.
- Evaluating compliance with applicable cybersecurity regulations and security standards.
- Preparing cybersecurity risk reports for executive management and governance committees.
- Developing dashboards to communicate security posture and risk exposure.
- Assessing organizational cybersecurity maturity and identifying improvement priorities.
- Establishing continuous improvement plans and cybersecurity awareness initiatives.
- Final practical exercise: Presenting an integrated cybersecurity controls and risk management 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, cybersecurity risk assessment exercises, group discussions, and realistic case studies. Participants will work with risk registers, control assessment matrices, security governance frameworks, and incident response planning templates. The course can be delivered through classroom-based training, live virtual sessions, 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, cyber risk assessment, and organizational resilience. The instructor possesses practical expertise in cybersecurity controls, risk treatment strategies, security compliance, incident response planning, and internationally recognized information security frameworks. Training emphasizes professional methodologies, practical case studies, and applied security management exercises to ensure participants can translate cybersecurity knowledge into effective organizational controls and risk management practices.

FREQUENTLY ASKED QUESTIONS

1. What is the main purpose of this course? The course develops practical skills for identifying cybersecurity risks, implementing effective security controls, and strengthening organizational cyber resilience.
2. Is this course suitable for professionals without advanced technical cybersecurity experience? Yes, the program introduces fundamental concepts before progressing to risk assessment, control evaluation, and cybersecurity management applications.
3. Which cybersecurity frameworks are covered during the training? Participants explore internationally recognized approaches, including the NIST Cybersecurity Framework, ISO 27001, and ISO 27005 principles.
4. Does the course include practical cybersecurity risk assessment exercises? Yes, participants develop risk registers, evaluate security controls, prepare risk treatment plans, and examine incident response scenarios.
5. Which organizations can benefit from this training? The program is relevant to government institutions, financial organizations, energy companies, technology providers, and businesses managing sensitive digital information.

CONCLUSION

Effective cybersecurity controls and risk management are essential for protecting organizational information assets and maintaining operational resilience in an increasingly digital environment. This course provides professionals with structured methodologies and practical tools for identifying cyber threats, assessing vulnerabilities, and implementing appropriate security controls. Participants will strengthen their ability to evaluate cybersecurity risks, develop effective treatment strategies, and support organizational compliance and security governance. The program also enhances the monitoring, incident response, communication, and decision-making capabilities required for proactive cybersecurity management. By applying the knowledge and techniques gained, participants can reduce cyber risk exposure, improve security performance, and contribute to sustainable organizational resilience.

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