CYBERSECURITY RISK ANALYSIS & CONTROL IMPLEMENTATION

Istanbul - Turkey
01 - Mar 2026 - 05 - Mar 2026
$5,800

GENTEX®
TRAINING CENTER

Introduction

Cybersecurity has become a core pillar of organizational resilience, business continuity, and digital trust. As global threats grow more advanced, organizations must strengthen their ability to identify risks, analyze vulnerabilities, and implement effective security controls. This course provides a structured, practical, and strategic foundation for professionals who want to enhance their understanding of cybersecurity risk analysis and the steps needed to reduce exposure.

Throughout this program, participants will explore essential frameworks, risk methodologies, control design principles, and practical mitigation strategies. They will also learn how to integrate risk management with organizational objectives, comply with international standards, and support informed decision-making.

The training focuses on building practical skills that help professionals evaluate cyber threats, assess the impact on systems, prioritize risks, and apply controls that improve security posture. Each day blends theory, real-world cases, and interactive exercises, enabling participants to apply concepts directly to workplace scenarios.

Cybersecurity Risk Analysis & Control Implementation Course Objectives

- Understand the core components of cybersecurity risk analysis and why it matters for organizational security.
- Identify threats, vulnerabilities, and potential attack vectors affecting digital environments.
- Apply structured risk assessment methodologies such as qualitative, quantitative, and hybrid approaches.
- Prioritize cybersecurity risks based on likelihood, business impact, and criticality.
- Design, implement, and evaluate effective security controls aligned with international standards such as ISO 27001, NIST CSF, and CIS Controls.

- Strengthen cyber defenses through preventive, detective, and corrective control mechanisms.
- Build risk reports and dashboards that support leadership decisions.
- Develop a practical cybersecurity risk treatment plan and integrate it into organizational processes.
- Support long-term cybersecurity improvement and organizational resilience.

Course Methodology

The course uses a blended learning approach combining expert presentations, interactive discussions, group exercises, practical case studies, and step-by-step demonstrations to ensure deep understanding and long-term retention.

Who Should Take This Course

- Cybersecurity professionals
- IT and system administrators
- Risk, governance, and compliance officers
- Technical managers and team leaders
- Business continuity and operational risk staff
- Anyone involved in managing or supporting cybersecurity programs

Cybersecurity Risk Analysis & Control Implementation Course Outlines

Day 1: Foundations of Cybersecurity Risk Management

- Understanding cybersecurity concepts, terminology, and domains

- Threats, vulnerabilities, assets, and risks
- Types of cyber attacks and common threat actors
- Organizational risk environment and digital exposure
- Introduction to risk management frameworks (ISO 27005, NIST, CIS)
- Building a structured cybersecurity risk program
- Practical exercise: Identifying assets and mapping risks

Day 2: Conducting Effective Cybersecurity Risk Analysis

- Risk identification methods and data-gathering techniques
- Qualitative vs. quantitative risk assessment
- Tools and techniques for analyzing cyber risks
- Using likelihood and impact scales for decision-making
- Vulnerability scanning and threat intelligence
- Hands-on workshop: Building a sample risk register
- Case study: Assessing risks in a cloud-based system

Day 3: Cybersecurity Controls and Countermeasures

- Overview of control categories: preventive, detective, corrective
- Security control frameworks: NIST SP 800-53, ISO 27001 Annex A, CIS v8
- Technical controls: network security, encryption, IAM, endpoint security
- Administrative controls: policies, standards, procedures
- Physical controls: access management and facility protection
- Workshop: Mapping risks to appropriate controls

Day 4: Implementing and Monitoring Cybersecurity Controls

- Planning and designing control implementation
- Integrating controls with business processes
- Security monitoring, SIEM systems, and continuous detection
- Incident response readiness and control testing
- Measuring control effectiveness with KPIs and KRIs
- Group exercise: Designing a real-world control improvement plan

Day 5: Building a Complete Cybersecurity Risk & Control Strategy

- Developing a cybersecurity risk treatment plan
- Prioritizing actions and reducing risk exposure
- Reporting risks to management and stakeholders
- Documenting risk acceptance, transfer, and avoidance decisions
- Developing a cybersecurity improvement roadmap
- Final workshop: Creating a full risk analysis and control implementation plan
- Open discussion and best practices exchange

Conclusion

By successfully completing the Cybersecurity Risk Analysis & Control Implementation training with Gentex Training Center, participants will gain the knowledge and confidence to evaluate risks, design effective controls, and strengthen organizational cybersecurity. They will understand how to identify threats, prioritize risks, and apply practical solutions that improve security posture and support long-term resilience.

GENTEX®
TRAINING CENTER