

CYBERSECURITY GOVERNANCE, RISK AND COMPLIANCE



GENTEX[®]

TRAINING CENTER



Introduction

Cybersecurity Governance, Risk and Compliance Training Course prepares professionals to govern cyber risk and demonstrate compliance with confidence. Participants work through cybersecurity governance structures and accountability, the ISO/IEC 27001 information security management system, cyber risk assessment and quantification, the NIST Cybersecurity Framework, regulatory and legal compliance obligations, and control monitoring, incident governance, and assurance reporting as one connected discipline. The programme links the cyber exposure an organisation carries with the governance, risk, and compliance discipline that manages it. As a result, learners gain a practical command of cyber GRC. Furthermore, the course strengthens risk judgement, control design, and compliance literacy.

Cybersecurity Governance, Risk and Compliance Course Objectives

- Explain cybersecurity governance principles and accountability models.
- Apply the ISO/IEC 27001 information security management system.
- Apply cyber risk assessment, treatment, and risk register practice.
- Apply the NIST Cybersecurity Framework functions and tiers.
- Apply ISO/IEC 27005 and cyber risk quantification concepts.
- Apply legal, regulatory, and contractual cybersecurity obligations.
- Apply data protection, privacy, and breach notification duties.
- Apply control design, access management, and security control testing.
- Apply third-party, cloud, and supply chain cyber risk governance.
- Apply incident governance, assurance, and cyber reporting practice.

Course Methodology



LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Interactive sessions built on cyber governance, risk, and compliance cases.
- Workshops on ISO 27001 clauses, cyber risk registers, and control mapping.
- Group exercises on NIST CSF mapping, breach scenarios, and reporting.
- Hands-on practice with risk registers, control matrices, and compliance logs.
- Simulation of a cyber governance review and an incident escalation.
- Facilitator coaching and peer review on personal cyber GRC plans.

Who Should Take This Course

- Cybersecurity and information security professionals.
- IT governance, risk, and compliance officers.
- Data protection and privacy officers.
- Technology risk managers and internal auditors.
- IT, cloud, and infrastructure managers.
- Consultants advising on cyber GRC frameworks and readiness.

Cybersecurity Governance, Risk and Compliance Course Outlines

Day 1: Cybersecurity Governance Foundations

- Cybersecurity governance principles and business drivers.
- Board and executive accountability for cyber risk.
- The three lines model applied to cybersecurity.
- Cybersecurity policy architecture and delegation.
- Roles: CISO, risk owner, control owner, and security operations.
- Common cyber governance failures and warning signs.





- Case discussion: an organisation breached with full policy coverage.

Day 2: ISO/IEC 27001 and the Information Security Management System

- ISO/IEC 27001 structure and management system clauses.
- Context, leadership, planning, and support requirements.
- Risk assessment and risk treatment in ISO 27001.
- Annex A controls and the Statement of Applicability.
- Internal audit, management review, and continual improvement.
- Certification readiness and audit evidence.
- Workshop: mapping ISO 27001 clauses to organisational practice.

Day 3: Cyber Risk Assessment and Treatment

- Cyber risk identification across assets, threats, and vulnerabilities.
- Risk analysis: likelihood, impact, and control effectiveness.
- Cyber risk registers and risk ownership assignment.
- Risk treatment options: mitigate, transfer, avoid, accept.
- Cyber risk quantification and financial impact modelling.
- Key risk indicators and cyber risk appetite setting.
- Exercise: building a cyber risk register with treatment plans.

Day 4: Frameworks, Legal Compliance, and Third-Party Risk

- NIST Cybersecurity Framework functions: identify, protect, detect, respond, recover.

LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- NIST CSF implementation tiers and profiles.
- Legal and regulatory obligations: data protection and sector rules.
- Breach notification duties and regulator interaction.
- Contractual security requirements and customer commitments.
- Third-party, cloud, and supply chain cyber risk governance.
- Simulation: assessing a cloud provider's security posture.

Day 5: Monitoring, Incidents, Assurance, and Reporting

- Control monitoring, testing, and continuous compliance.
- Security metrics, KPIs, and cyber governance reporting.
- Incident governance, escalation, and crisis interface.
- Cyber insurance and risk transfer considerations.
- Internal audit, assurance mapping, and penetration test review.
- Continuous improvement and cyber maturity assessment.
- Capstone: presenting a cybersecurity GRC framework.

Conclusion

By successfully completing Cybersecurity Governance, Risk and Compliance, participants will gain a practical command of cybersecurity governance, the ISO/IEC 27001 management system, cyber risk assessment and treatment, the NIST Cybersecurity Framework, legal and regulatory compliance with third-party risk governance, and monitoring, incident governance, assurance and reporting. They will acquire skills in cyber governance design, cyber risk assessment, control and compliance management, and cyber assurance reporting that strengthen organisational resilience. Gentex Training Center designs the programme to help professionals govern cyber risk with confidence.





FAQs for the Cybersecurity Governance, Risk and Compliance course

Q1 What is the "Cybersecurity Governance, Risk and Compliance" course about?

It prepares professionals to govern cyber risk and demonstrate compliance with confidence. The course spans cybersecurity governance foundations, ISO/IEC 27001 and the information security management system, cyber risk assessment and treatment, frameworks, legal compliance and third-party risk, and monitoring, incidents, assurance and reporting.

Q2 What are the key benefits of the "Cybersecurity Governance, Risk and Compliance" course?

You gain a practical command of cyber GRC that links the cyber exposure an organisation carries with the governance, risk, and compliance discipline that manages it. The course improves governance design and ISO 27001 implementation, strengthens cyber risk assessment and treatment planning, sharpens control monitoring and compliance management, and gives you breach and assurance reporting practice that stands up to boards and regulators.

Q3 What skills will I gain from the "Cybersecurity Governance, Risk and Compliance" course?



You will develop four core skills: cybersecurity governance and accountability structuring, ISO/IEC 27001 information security management system implementation, cyber risk assessment with risk register and treatment practice, and cyber control monitoring, compliance and assurance reporting.

Q4 What tools, methods, or standards are covered in the "Cybersecurity Governance, Risk and Compliance" course?

The course covers cybersecurity governance principles and business drivers, board and executive accountability for cyber risk, the three lines model applied to cybersecurity, cybersecurity policy architecture and delegation, roles across CISO, risk owner, control owner and security operations, ISO/IEC 27001 structure and management system clauses, context, leadership, planning and support requirements, risk assessment and risk treatment in ISO 27001, Annex A controls and the Statement of Applicability, internal audit, management review and continual improvement, certification readiness and audit evidence, cyber risk identification across assets, threats and vulnerabilities, risk analysis across likelihood, impact and control effectiveness, cyber risk registers and risk ownership assignment, risk treatment options of mitigate, transfer, avoid and accept, cyber risk quantification and financial impact modelling, key risk indicators and cyber risk appetite setting, NIST Cybersecurity Framework functions of identify, protect, detect, respond and recover, NIST CSF implementation tiers and profiles, legal and regulatory obligations including data protection and sector rules, breach notification duties and regulator interaction, contractual security requirements and customer commitments, third-party, cloud and supply chain cyber risk governance, control monitoring, testing and continuous compliance, security metrics, KPIs and cyber governance reporting, incident governance, escalation and crisis interface, cyber insurance and risk transfer considerations, internal audit, assurance mapping and penetration test review, and continuous improvement and cyber maturity assessment.



Q5 How is the "Cybersecurity Governance, Risk and Compliance" course applied in real-world practice?

Participants apply it to real work such as mapping ISO 27001 clauses to organisational practice, building a cyber risk register with treatment plans, preparing a Statement of Applicability, mapping controls to the NIST Cybersecurity Framework, assessing a cloud provider's security posture, handling a breach notification, reviewing a penetration test report, and presenting a cyber GRC framework to the board. The same methods support certification readiness and cyber maturity improvement.