LDR519: SANS CYBERSECURITY RISK MANAGEMENT AND COMPLIANCE



GENTEX®
TRAINING CENTER

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

Introduction

LDR519: SANS Cybersecurity Risk Management and Compliance Training Course equips leaders and practitioners to govern cyber risk and prove compliance to regulators, auditors, and boards. Participants work through cyber risk frameworks, threat and vulnerability assessment, control selection, risk quantification basics, regulatory and contractual obligations, incident response governance, third-party risk, and assurance reporting as one connected system. The programme links the risk an organization carries with the controls and evidence that demonstrate it is managed. As a result, learners gain a repeatable, defensible method for cyber risk and compliance. Furthermore, the course strengthens risk judgement, control design, and audit readiness.

LDR519: SANS Cybersecurity Risk Management and Compliance Course Objectives

- Apply cybersecurity risk management principles and terminology.
- Apply the NIST Cybersecurity Framework and NIST RMF to organizational risk.
- Apply ISO/IEC 27001 and ISO 31000 to control selection and risk treatment.
- Conduct threat, vulnerability, and impact assessments.
- Apply risk quantification basics and risk register maintenance.
- Map regulatory and contractual obligations to security controls.
- Apply CIS Critical Security Controls and control maturity assessment.
- Design third-party and supply chain cyber risk management.
- Apply incident response governance, escalation, and reporting duties.
- Apply cyber assurance, metrics, board reporting, and audit readiness.

Course Methodology

- Interactive sessions built on cybersecurity risk and compliance cases.

GENTEX® TRAINING CENTER

- Workshops on framework mapping, control selection, and obligation mapping.
- Group exercises on risk registers, control maturity, and board reporting.
- Hands-on practice with risk registers, control matrices, and compliance checklists.
- Simulation of a cyber risk committee review and an audit evidence request.
- Facilitator coaching and peer review on personal cyber risk plans.

Who Should Take This Course

- Cybersecurity managers, analysts, and risk officers.
- IT managers, security architects, and compliance professionals.
- Risk, governance, and internal control professionals.
- Internal auditors covering cyber and technology controls.
- Legal, privacy, and regulatory affairs professionals.
- Consultants advising on cyber risk and compliance programmes.

LDR519: SANS Cybersecurity Risk Management and Compliance Course Outlines

Day 1: Cybersecurity Risk Foundations

- Cyber risk concepts: threat, vulnerability, likelihood, and impact.
- Risk management principles and the risk lifecycle.
- Governance structures and accountability for cyber risk.
- Risk appetite, tolerance, and escalation thresholds.
- The NIST Cybersecurity Framework core functions.
- Risk communication and cyber risk language for boards.
- Case discussion: an incident that exposed a governance gap.

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

Day 2: Frameworks, Standards, and Risk Assessment

- The NIST Risk Management Framework (RMF) steps.
- ISO/IEC 27001 and Annex A control structure.
- ISO 31000 risk assessment and treatment process.
- CIS Critical Security Controls and implementation groups.
- Threat modeling and vulnerability assessment basics.
- Risk quantification and risk register maintenance.
- Workshop: completing a cybersecurity risk assessment.

Day 3: Compliance Obligations and Control Mapping

- Regulatory landscape: GDPR, NIS2, DORA, and sector rules.
- Contractual security obligations and customer requirements.
- Mapping obligations to controls and responsible owners.
- Control testing, evidence standards, and documentation.
- Compliance monitoring and continuous control assurance.
- Handling exceptions, compensating controls, and remediation.
- Exercise: mapping obligations to a control matrix.

Day 4: Third-Party Risk, Incidents, and Reporting

- Third-party and supply chain cyber risk management.
- Vendor security assessment and contractual safeguards.
- Incident response governance, roles, and escalation.
- Breach notification duties and regulator communication.
- Cyber metrics, KPIs, and KRIs for management.

- Board reporting on cyber risk and compliance posture.
- Simulation: responding to a third-party breach and reporting it.

Day 5: Assurance, Audit, and Programme Maturity

- Internal audit of cyber risk and compliance.
- Evidence collection, sampling, and audit findings.
- Remediation planning, ownership, and verification.
- Cyber insurance and risk transfer considerations.
- Measuring programme maturity and continuous improvement.
- Building cyber risk capability and succession.
- Capstone: presenting a cyber risk and compliance programme.

Conclusion

By successfully completing LDR519: SANS Cybersecurity Risk Management and Compliance, participants will gain a practical command of cybersecurity risk frameworks, risk assessment, control selection and mapping, regulatory and contractual compliance, third-party risk, incident governance, and assurance reporting. They will acquire skills in risk assessment, control mapping, metrics and board reporting, and audit readiness that strengthen cyber resilience overall. Gentex Training Center designs the programme to help professionals govern cyber risk with confidence.

FAQs

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

Q1 What is the "LDR519: SANS Cybersecurity Risk Management and Compliance" course about?

It equips leaders and practitioners to govern cyber risk and prove compliance to regulators, auditors, and boards. The course spans cybersecurity risk foundations, frameworks, standards and risk assessment, compliance obligations and control mapping, third-party risk, incidents and reporting, and assurance, audit and programme maturity.

Q2 What are the key benefits of the "LDR519: SANS Cybersecurity Risk Management and Compliance" course?

You gain a repeatable, defensible method for cyber risk and compliance that connects the risk an organization carries with the evidence it is managed. The course improves risk assessment and control selection, strengthens obligation mapping and control testing, sharpens third-party and incident governance, and gives you metrics and audit readiness that satisfy boards and regulators.

Q3 What skills will I gain from the "LDR519: SANS Cybersecurity Risk Management and Compliance" course?

You will develop four core skills: cybersecurity risk assessment using NIST CSF and ISO 31000, control selection and mapping with ISO/IEC 27001 and the CIS Controls, regulatory and contractual obligation mapping with control testing, and cyber metrics, board reporting and audit readiness.

GENTEX® TRAINING CENTER

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

Q4 What tools, methods, or standards are covered in the "LDR519: SANS Cybersecurity Risk Management and Compliance" course?

The course covers cybersecurity risk concepts of threat, vulnerability, likelihood and impact, the risk management lifecycle, governance structures and accountability for cyber risk, risk appetite and tolerance and escalation thresholds, the NIST Cybersecurity Framework core functions, the NIST Risk Management Framework (RMF) steps, ISO/IEC 27001 and its Annex A control structure, ISO 31000 risk assessment and treatment, the CIS Critical Security Controls and implementation groups, threat modeling and vulnerability assessment, risk quantification and risk registers, the regulatory landscape across GDPR, NIS2 and DORA, contractual security obligations and customer requirements, obligation-to-control mapping and ownership, control testing and evidence standards, compliance monitoring and continuous control assurance, exceptions and compensating controls and remediation, third-party and supply chain cyber risk management, vendor security assessment and contractual safeguards, incident response governance and escalation, breach notification duties and regulator communication, cyber metrics, KPIs and KRIs, board reporting on cyber risk posture, internal audit of cyber risk and compliance, evidence collection and sampling and audit findings, remediation planning and verification, cyber insurance and risk transfer, and programme maturity measurement.

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

Q5 How is the "LDR519: SANS Cybersecurity Risk Management and Compliance" course applied in real-world practice?

Participants apply it to real work such as completing a cybersecurity risk assessment, mapping GDPR, NIS2, and DORA obligations to controls, maintaining a cyber risk register, assessing a vendor's security posture, preparing a board report on cyber risk posture, and gathering evidence for a technology audit. The same methods support incident reporting and remediation planning.