LDR519: **Cybersecurity Governance, Risk, and Compliance (GRC)™**

5 Day Program	30 CPEs	Laptop Required

You Will Be Able To

- Establish governance structures for cybersecurity decisions
- Build threat and safeguard inventories
- Select and prioritize safeguards using frameworks and threat modeling
- Operationalize GRC through policy and program management
- Design and execute risk assessments
- Use AI and continuous monitoring to measure controls
- Communicate risk to executive and technical stakeholders

Business Takeaways

- Apply a repeatable, end-to-end GRC lifecycle
- Improve visibility into cybersecurity risk
- Align security efforts with business goals
- Make defensible, evidence-based decisions
- Increase efficiency with AI and automation
- Strengthen consistency across teams and environments
- Enhance resilience and audit readiness

Strategic Risk Governance: Enterprise Security Beyond Compliance

Take command of the full GRC lifecycle with SANS LDR519: Cybersecurity Governance, Risk, and Compliance. Built for assessors, auditors, and GRC practitioners, this course develops the hands-on skills needed to build, operationalize, and lead a resilient, business-aligned cybersecurity program. Through a structured, lifecycle-based approach, students learn to establish governance structures, inventory assets, select and prioritize safeguards, validate controls, and report risk outcomes to business stakeholders.

LDR519 goes beyond frameworks and checklists. Using the CRF Governance and Risk Model and the NIST Risk Management Framework as its backbone, the course teaches students to make defensible, evidence-based cybersecurity decisions at every stage of the program. AI-assisted tools and continuous monitoring are integrated throughout, reflecting how modern GRC programs actually operate. Students also navigate multi-framework environments spanning NIST, CIS Controls, and ISO standards, learning to align cybersecurity investments directly with business priorities.

What Is Cybersecurity GRC?

Cybersecurity GRC is how organizations move beyond reactive security. It combines governance structures, risk management processes, and compliance validation into a repeatable program that ties cybersecurity directly to business priorities and accountability.

Hands-On Cybersecurity GRC Training

LDR519 brings course concepts to life through Cyber42 leadership simulations, where case studies place students in the role of decision-maker to work through the real program challenges GRC practitioners face. In each case study, students select risk models under resource constraints, scope assessments with competing priorities, govern third-party and AI-related risk, and communicate findings to business stakeholders. Grounded in real-world situations, these simulations build judgment and critical thinking by challenging students to weigh tradeoffs, defend their decisions, and adapt as conditions change. By the end of the course, students have practiced the full GRC lifecycle through scenarios that mirror the complexity and ambiguity of real organizational environments.

"I really particularly enjoyed this class because not only is it relevant to my career, it is broken down into understandable content by an instructor who actually does this for a living and can recall a lot of his personal experience as he is teaching the course."

—Madeline K., **REH**

Section Descriptions

SECTION 1: Foundations of Cybersecurity Governance and Risk

This section builds the foundation for a cybersecurity GRC program. Students learn how governance and risk decisions align with business goals, explore risk models, tooling, and Artificial Intelligence (AI), and apply these concepts through the Initiate and Inventory phases to define program structure, ownership, and scope.

TOPICS: Governance and Business Context; GRC Foundations; Risk Management Models; Choosing and Adopting a Risk Model; GRC Tooling and Program Enablement; AI in Cybersecurity GRC; GRC Roadmap Step #1: Initiate and Step #2: Inventory

SECTION 2: Selecting and Prioritizing Cybersecurity Safeguards

This section focuses on selecting and prioritizing cybersecurity safeguards to address risk and support business goals. Students evaluate frameworks, navigate multi-framework environments, and apply threat modeling to map threats to safeguards. The result is a structured, defensible approach to safeguard selection based on likelihood, impact, and business need.

TOPICS: Safeguard Framework Landscape; Comparing Frameworks (NIST, CIS, ISO, etc.); Selecting and Adopting Frameworks; Aggregate Frameworks and Safeguards; Operating in a Multi-Framework Environment; Threat Modeling Concepts; Threat Inventory Development and Classification; Prioritizing Threats by Severity and Likelihood; Mapping Threats to Safeguards

SECTION 3: Cybersecurity GRC Program Management

This section focuses on operationalizing cybersecurity decisions by translating safeguards into governance, documentation, education, and implementation. Students learn to formalize policy, assign ownership, enable the workforce, and manage execution. The focus is on consistent, organization-wide execution that turns decisions into measurable outcomes.

TOPICS: Using AI for Safeguard Selection; Governing Safeguard Decisions Through Policy; AI as a Documentation Accelerator: Capabilities and Constraints; GRC Roadmap Step #4: Educate and Step #5: Implement; Extending Governance to Third Parties; Case Study: Governing Cybersecurity Risk in Cloud Environments; Case Study: AI Governance

SECTION 4: Validating Cybersecurity Safeguards

This section focuses on validating whether cybersecurity safeguards are implemented and operating as intended. Students learn to design and execute risk assessments, including scoping, reviewing documentation, evaluating technical controls, and analyzing evidence. The focus is on making defensible decisions based on multiple forms of evidence.

TOPICS: GRC Roadmap Step 6: Validate: Step #1: Scope the Subject of the Risk Assessment; Step #2: Scope Who Will Perform the Risk Assessment; Step #3: Scope the Quality Level of the Risk Assessment; Step #4: Scope the Safeguards for the Risk Assessment; Step #5: Evaluate Documentation; Step #6: Evaluating Safeguards; Step #7: Analyzing and Interpreting Evidence; AI for Safeguard Validation

SECTION 5: AI-Enabled Continuous Monitoring and Risk Reporting

This section focuses on transitioning cybersecurity risk management from periodic assessments to continuous, data-driven monitoring and reporting. Students learn to use business intelligence, automation, and AI to measure safeguards, reduce uncertainty, and support decisions. The focus is on continuous measurement, analysis, communication, and response.

TOPICS: AI and Continuous Monitoring; Continuous Monitoring and Asset-Centric Risk Management; Penetration Testing and Safeguard Validation; Present Cybersecurity Risk to Stakeholders; Managing a Cybersecurity Risk Register; Cybersecurity Risk Remediation and Response; Course Summary

Who Should Attend

- Risk management professionals
- Governance, risk, compliance professionals
- Second-line GRC teams
- IT Auditors
- Directors of security compliance
- Information assurance management

NICE Framework Work Roles:

- Risk Management (SP-RSK-001)
- Risk Management (SP-RSK-002)
- Test and Evaluation (SP-TST-001)