LDR519: Cybersecurity Risk Management and Compliance

5 Day Program	30 CPEs	Laptop Required

Skills Learned

- Gain practical skills in identifying and managing cybersecurity risks through structured threat modeling and assessment methodologies
- Learn to prioritize and allocate resources effectively by understanding the criticality of various cybersecurity threats and vulnerabilities.
- Develop proficiency in using industry-standard frameworks, such as NIST Risk Management Framework (RMF) and FAIR, to enhance your organization's cybersecurity posture.
- Apply hands-on exercises and real-world case studies to reinforce theoretical knowledge and validate your cybersecurity strategies
- Master the process of conducting comprehensive cybersecurity risk assessments and audits to ensure compliance with regulatory standards
- Enhance your decision-making capabilities with data-driven insights and simulations, preparing you for real-world cybersecurity challenges

Business Takeaways

- Equip employees with advanced skills to identify, assess, and mitigate cybersecurity risks, enhancing organizational security
- Align cybersecurity efforts with business goals through a structured approach to risk management and compliance
- Enhance decision-making capabilities by integrating threat modeling and risk analytics into strategic planning
- Strengthen organizational resilience against evolving cyber threats through proactive risk management strategies
- Ensure compliance with industry standards and regulatory requirements, reducing the risk of legal and financial repercussions
- Implement robust cybersecurity safeguards tailored to your organization's specific risk profile
- Foster a culture of security awareness and critical thinking among team members to improve overall security posture
- Gain insights from expert instructors and practical case studies to apply theoretical knowledge in real-world scenarios
- Improve the effectiveness of cybersecurity governance practices, ensuring comprehensive oversight and alignment with business objectives

Secure Your Organization's Digital Future

Master the essentials of risk management and compliance with SANS Institute's LDR519: Cybersecurity Risk Management and Compliance course. This course is designed to equip cybersecurity professionals with the skills necessary to navigate the complex landscape of cybersecurity risks. Through a systematic approach, students will delve into threat modeling, risk assessments, and safeguard implementation, ensuring their organizations remain resilient against evolving cyber threats.

LDR519 focuses on practical methodologies and industry-best practices, providing participants with a thorough understanding of risk management and compliance frameworks. By exploring real-world case studies and engaging in hands-on simulations, students will learn to develop comprehensive threat inventories, prioritize cybersecurity defenses, and align security measures with business objectives. The curriculum integrates established frameworks such as NIST SP 800-30 and the Cybersecurity Risk Foundation's Governance and Risk Model, offering a structured approach to managing cybersecurity risks and ensuring regulatory adherence.

Enroll in LDR519 to transform your cybersecurity strategy and lead your organization towards robust risk management and compliance. Gain insights from seasoned experts and leverage cutting-edge tools to enhance your decision-making capabilities. With a focus on practical applications and strategic planning, this course empowers you to implement effective cybersecurity safeguards, validate their impact, and communicate risks to stakeholders confidently. Join us at the SANS Institute and elevate your cybersecurity expertise today.

What Is Cybersecurity Risk Management and Compliance?

Cybersecurity risk management is the systematic process of identifying, assessing, and prioritizing risks, followed by the coordinated application of resources to minimize, monitor, and control the probability or impact of unfortunate events. Compliance refers to adhering to laws, regulations, guidelines, and specifications relevant to an organization's operations, ensuring ethical and legal conduct.

Hands-On Cybersecurity Risk Management and Compliance Training

LDR519 uses a combination of case studies and SANS Cyber42 simulations to deepen students' understanding of the concepts covered in the course. Through detailed case studies based on the fictitious company Initech Systems, students can apply theoretical knowledge to real-world scenarios. This approach allows learners to analyze vulnerabilities, develop threat models, and manage risk registers effectively. By pausing to reflect on the concepts learned, students gain practical insights into cybersecurity risk management strategies, enhancing their decision-making skills.

The SANS Cyber42 simulations offer an interactive environment where students confront realistic cybersecurity incidents. These simulations provide hands-on experiences in managing resources, responding to evolving threats, and implementing strategic initiatives. By engaging with these dynamic scenarios, students practice critical thinking, problem-solving, and collaboration techniques essential for effective cybersecurity leadership. The combination of case studies and simulations ensures that students not only understand theoretical principles but also acquire the practical skills needed to navigate complex cybersecurity challenges confidently.

Section Descriptions

SECTION 1: Strategies for Cybersecurity Risk Management

Section 1 provides a detailed overview of cybersecurity risk assessments within an organizational context. The course emphasizes the alignment of cybersecurity practices with business objectives, focusing on defining and managing cybersecurity risks through frameworks like the NIST RMF and the CRF-GRM. It covers essential topics such as threat modeling, safeguard selection and prioritization, and the documentation of cybersecurity safeguards to ensure consistency and guidance for implementation. Additionally, the course highlights the significance of cybersecurity governance and risk management, addressing program maturity, stakeholder responsibilities, and effective communication of cybersecurity risks to both executive and technical stakeholders.

TOPICS: What Is the Purpose of This Course?; The Business Context for Cybersecurity Risk Assessment; An Introduction to Cybersecurity Governance and Risk Models; Understanding and Comparing Popular Cybersecurity Risk Management Models; Quantifying Cybersecurity Risk and Business Impact Analysis (BIA)

SECTION 2: Cybersecurity Threat Modeling

Section 2 offers an in-depth exploration of threat modeling, safeguard selection, and risk assessment. The course covers comprehensive theoretical concepts and practical steps for creating a cybersecurity threat inventory, leveraging well-known frameworks like the Open Threat Taxonomy (OTT) and MITRE's ATT&CK. It emphasizes integrating data from industry threat reports and tools such as Monte Carlo simulations to manage and quantify cybersecurity risks effectively. Participants will gain the knowledge needed to develop robust threat models, map threats to safeguards, and prioritize vulnerabilities, ensuring their organizations can proactively address and mitigate cybersecurity threats.

TOPICS: Understanding Risk Management for Safeguard Selection—Creating a Threat Inventory; Understanding Risk Management for Safeguard Selection—Creating a Threat Model; Understanding Risk Management for Safeguard Selection—Quantifying a Threat Model; Understanding Risk Management for Safeguard Selection—Mapping Threats to Safeguards; Understanding Threat Modeling for Vulnerability Management

SECTION 3: Cybersecurity Safeguard Frameworks

Section 3 provides insights into evaluating and selecting cybersecurity safeguards through various frameworks such as NIST, CIS, and ISO. It emphasizes the importance of initiating a cybersecurity governance program, creating a detailed cybersecurity threat inventory, and modeling threats to align safeguards effectively. Participants will gain practical knowledge on implementing cybersecurity policies, conducting risk assessments, and employing tools for risk quantification. The section also discusses leveraging the SANS Cyber42 simulation game to enhance hands-on learning and strategic decision making in cybersecurity risk management.

TOPICS: The Cybersecurity Safeguard Framework Landscape; Understanding the NIST, CIS, and ISO Frameworks; Understanding the CRF-Safeguards; Documenting, Educating, and Implementing Cybersecurity Safeguards

SECTION 4: Validating Safeguards and Third-Party Risk Management

Section 4 covers essential topics such as conducting internal and third-party cybersecurity risk assessments, creating detailed cybersecurity risk assessment plans, and implementing robust threat modeling practices. It emphasizes the importance of evaluating and validating cybersecurity safeguards through practical tools like the CRF-Safeguards Assessment tool. Additionally, it explores the significance of continuous monitoring, business impact analysis, and leveraging frameworks such as NIST and ISO for effective cybersecurity risk management. Participants will gain valuable insights into aligning their cybersecurity strategies with organizational goals, ensuring a systematic and thorough approach to fortifying their digital defenses.

TOPICS: Validating Cybersecurity Safeguards; Understanding How to Evaluate Cybersecurity Policies and Safeguards During a Risk Assessment; Managing Third-Party Cybersecurity Risk; Managing Cybersecurity Risk in the Cloud

SECTION 5: Cybersecurity Risk Analytics and Response

Section 5 emphasizes the integration of governance, risk, and compliance principles with continuous monitoring, asset-centric risk management, and safeguard validation. It covers essential tools and methodologies such as automated cybersecurity risk analytics, penetration testing, and the use of IT Service Management tools for tracking and validating cybersecurity safeguards. Participants will learn to aggregate and present risk data effectively to different stakeholders, including senior leadership and technical teams, ensuring clear communication of cybersecurity risks. Additionally, the course addresses the expectations of senior leadership, the responsibilities of the Board of Directors in cybersecurity governance, and the use of the SANS Cyber42 simulation game for hands-on learning and strategic decision making.

TOPICS: Continuous Monitoring and Asset-Centric Risk Management; Presenting Cybersecurity Risk to Stakeholders; Cybersecurity Risk Remediation and Response; Course Summary

Who Should Attend

- Risk management professionals
- Governance, risk, compliance professionals
- IT Auditors
- Directors of security compliance
- Information assurance management
- System administrators/engineers

NICE Framework Work Roles:

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