BLACKBIRD FOR TRAINING

LDR519: SANS Cybersecurity Risk Management and Compliance

LDR519: SANS Cybersecurity Risk Management and Compliance

Introduction

The course LDR519: SANS Cybersecurity Risk Management and Compliance provides a structured and practical framework for managing cybersecurity risks and ensuring organizational compliance.

It focuses on connecting technical risk exposure with executive decision-making and institutional governance.

The course enables participants to move from reactive incident response to proactive, measurable risk management.

This program is designed for executives, department managers, risk managers, cybersecurity professionals, internal audit teams, governance specialists, and project leaders.

It is highly relevant for organizations that depend on data protection, operational continuity, and regulatory adherence.

Participants will learn how to identify critical assets, assess threats and vulnerabilities, evaluate business impact, and design practical risk treatment strategies.

The course strengthens institutional resilience, improves reporting quality to senior leadership, and enhances enterprise-wide risk awareness.

Course Objectives

The course aims to build analytical and practical capabilities in cybersecurity risk management and compliance.

- Understand the core principles of cybersecurity risk management.
- Identify organizational assets and classify information.
- Analyze threat sources and vulnerability exposure.
- Apply qualitative and quantitative risk assessment methods.
- Develop and maintain a structured risk register.
- Prioritize risk treatment based on impact and likelihood.
- Align risk management with governance and internal controls.
- Prepare executive-level risk reports.
- Monitor risk indicators and measure effectiveness.
- Strengthen compliance culture across the organization.

Course Outlines

Day One: Foundations of Cybersecurity Risk Management.

- Define risk in the cybersecurity context.
- Identify critical business assets.
- Classify sensitive information.
- Recognize internal and external threat sources.
- Understand the relationship between risk and organizational strategy.
- Review real-world case studies of risk management failures.
- Conduct a practical exercise on asset and threat identification.

Day Two: Risk Assessment and Analysis.

- Explain qualitative and quantitative assessment approaches.
- Build and interpret a risk matrix.
- Evaluate likelihood and business impact.
- Rank risks based on severity and exposure.
- Perform gap analysis between current and target state.
- Develop a structured risk assessment report.
- Apply concepts to a simulated incident scenario.

Day Three: Compliance and Governance.

- Understand regulatory compliance principles.
- Link risk management to internal policies.
- Identify key control requirements.
- Assess current compliance posture.
- Develop remediation plans for compliance gaps.
- Analyze the reputational impact of non-compliance.
- Draft a concise risk management policy.

Day Four: Building an Integrated Risk Management Program.

- Design a comprehensive risk management framework.
- Define roles and responsibilities.
- Establish structured monitoring mechanisms.
- Develop measurable risk performance indicators.
- Create executive reporting mechanisms.
- Design dashboards for risk visibility.
- Apply practical steps to build a complete program model.

Day Five: Practical Application and Evaluation.

- Review key concepts and frameworks.
- Discuss implementation challenges.
- Present participant practical exercises.
- Evaluate analytical and reporting capabilities.
- Develop an individual organizational action plan.
- Explore continuous improvement approaches.
- Provide structured feedback and a final assessment.

Why Attend This Course? Wins & Losses!

- Improve executive decision-making through structured risk analysis.
- Strengthen regulatory compliance posture.
- Reduce exposure to cybersecurity-related losses.
- Enhance reporting clarity to senior leadership.
- Support business continuity and operational stability.
- Increase institutional risk awareness.
- Improve coordination between technical and management teams.
- Establish a measurable and sustainable risk management approach.

Conclusion.

LDR519: SANS Cybersecurity Risk Management and Compliance provides a comprehensive and structured approach to managing cybersecurity risks and ensuring organizational compliance. The course integrates analytical frameworks, practical exercises, and governance alignment into one coherent methodology. Participants gain the ability to assess risk exposure, measure business impact, and design effective mitigation strategies. Applying the knowledge gained from this course improves governance quality, strengthens executive reporting, and enhances operational stability.

It supports organizations in building a proactive risk culture capable of adapting to evolving digital threats. Cybersecurity risk management is no longer optional. It is a strategic requirement for long-term resilience and sustainable growth.