BLACKBIRD FOR TRAINING

LDR521: SANS Security Culture for Leaders

15 – 19 March 2027
London (UK)



LDR521: SANS Security Culture for Leaders

Ref: 3255607_346183 **Date:** 15 – 19 March 2027 **Location:** London (UK) **Fees:** 6100 GBP

Introduction

LDR521: SANS Security Culture for Leaders is a specialized course designed to help organizational leaders build and sustain an effective security culture. The course goes beyond traditional awareness training and focuses on transforming security from a technical responsibility into an organizational behavior embedded across all departments.

This program is relevant for executives, department heads, team leaders, risk managers, human resources professionals, compliance officers, and security specialists. It also supports professionals seeking recognized certifications that strengthen institutional credibility and enhance governance and regulatory alignment.

The practical value of this course lies in enabling participants to design measurable security culture programs, assess organizational maturity, and align security initiatives with strategic objectives. It addresses human risk factors, improves incident resilience, and enhances the overall return on security investments.

Course Objectives

By the end of LDR521: SANS Security Culture for Leaders, participants will be able to:

- Understand the core principles of security culture and its relationship to enterprise risk management.
- Analyze employee behaviors and their impact on security exposure.
- Apply structured frameworks to measure security culture maturity.
- Design data-driven awareness and behavior change initiatives.
- Align security culture strategies with organizational goals.
- Develop performance indicators to measure behavioral security outcomes.
- Implement change management practices to strengthen policy adherence.
- Evaluate real-world security incidents linked to cultural weaknesses.

These objectives ensure that participants gain both strategic insight and operational capability.

Course Outlines

Day 1: Foundations of Security Culture and Human Risk

The first day establishes the conceptual and strategic framework.



- Define security culture and distinguish it from traditional awareness initiatives.
- Examine the link between human behavior and security breaches.
- Review human risk management principles.
- Explore leadership influence on organizational security behavior.
- Analyze real case studies of incidents caused by behavioral failures.
- Conduct a practical exercise to identify cultural gaps within a sample organization.

This foundation ensures a structured understanding of behavioral security dynamics.

Day 2: Measuring Security Culture Maturity

The second day focuses on assessment and data-driven decision-making.

- Review security culture maturity models.
- Design assessment surveys tailored to organizational contexts.
- Interpret assessment results and identify behavioral patterns.
- Connect measurement results to enterprise risk indicators.
- Prioritize interventions based on data findings.
- Participate in a practical workshop to build a culture assessment framework.

This day emphasizes quantifiable and evidence-based leadership decisions.

Day 3: Designing Evidence-Based Security Culture Programs

The third day transitions from analysis to implementation.

- Identify target groups within the organization.
- Develop risk-based communication strategies.
- Select appropriate engagement channels for different employee levels.
- Build a phased implementation roadmap.
- Integrate awareness initiatives into operational workflows.
- Complete a structured design exercise for a full security culture program.

The focus is on structured execution supported by measurable outcomes.

Day 4: Leading Behavioral Change and Organizational Alignment

The fourth day centers on leadership and change management skills.

- Understand organizational change management principles.
- Address resistance to behavioral and procedural change.
- Strengthen accountability mechanisms.
- Establish cross-functional culture champions.
- Use incentives and evaluation systems to reinforce secure behaviors.
- Study applied examples of successful cultural transformation initiatives.

This module ensures sustainability beyond short-term campaigns.



Day 5: Performance Evaluation and Continuous Improvement

The final day concentrates on long-term governance and optimization.

- Develop key performance indicators for security culture effectiveness.
- Prepare executive-level reporting structures.
- Identify recurring gaps and improvement opportunities.
- Update policies based on performance data.
- Conduct a final evaluation of a pilot culture initiative.
- Create a forward-looking improvement roadmap.

The fifth day ensures structured and continuous maturity progression.

Why Attend This Course? Wins & Losses!

- Develop advanced insight into human-centered security risk.
- Gain practical assessment and measurement tools.
- Improve organizational resilience against behavioral threats.
- Strengthen compliance and governance alignment.
- Connect security initiatives with strategic priorities.
- Increase return on security investments.
- Establish sustainable accountability mechanisms.
- Obtain a globally recognized professional certification.

Conclusion

LDR521: SANS Security Culture for Leaders provides a structured and data-driven framework for building sustainable security culture within organizations. The course begins with foundational behavioral concepts and human risk management principles. It then advances into maturity measurement and data analysis techniques. Participants learn to design evidence-based programs aligned with organizational objectives. Leadership and change management principles are integrated to ensure adoption and sustainability. The program concludes with structured evaluation methods and continuous improvement strategies.

This comprehensive approach transforms security culture from isolated awareness activities into a measurable governance function. It supports stronger institutional resilience, reduces human-related vulnerabilities, and enables leaders to make informed strategic security decisions.

