

LDR514

Security Strategic Planning, Policy, and Leadership



LDR514 equips cybersecurity leaders with an MBA-level training in strategy, policy, and executive influence. Through real-world scenarios, business case analysis, and Cyber42 Leadership Simulations, participants align security to business goals and mature their programs. The course prepares leaders for the GIAC Strategic Planning, Policy, and Leadership (GSTRT) certification.

“Cyberthreats can destabilize societies, erode trust in institutions and even threaten national security. **Cybersecurity today is as much about leadership, governance and resilience as it is about technology.**

Protecting systems is only part of the task; leaders must also manage polarization as a result of cyberattacks that are eroding public trust, uphold ethics and safeguard society.”

(Source: *Cybersecurity is no longer just a technical challenge – it's a leadership one*, World Economic Forum 2025)

2026 Update: Deepens AI integration across the course and refreshes executive business school style case studies to reflect the latest in AI, cloud, and digital transformation. The update highlights AI risk within the Political, Economic, Social, and Technological (PEST) framework, incorporates GenAI into mission and metrics, and expands strategic planning tools to strengthen executive decision-making and communication.

New Content



- More explicit AI transformation narrative added to case study, positioning AI as a competitive differentiator rather than a future consideration.
- AI cyber risk introduced as a first-class concern, including data exposure, GenAI misuse, and dependency on cloud-based AI services.
- Regulatory pressure expanded to include modern European requirements (for example, NIS2), elevating compliance into a strategic driver.
- Talent risk tied to AI and cloud adoption, highlighting workforce displacement fears, reskilling needs, and retention challenges.
- A new Cloud Adoption Model helps leaders approach cloud migration as a phased, business-driven decision

Updated Features



- Thunderbolt case study reframed from a cloud-only debate to a combined AI, cloud, and digital transformation decision at the executive level.
- PEST analysis expanded to explicitly call out AI-driven political, economic, social, and technological risk factors.
- Mission and metrics discussions updated to include GenAI as part of organizational purpose, value delivery, and measurement.
- Strategic planning tools enhanced, including deeper application of:
 - 3D Blueprint
 - Cyber Risk Map
 - Crown Jewels analysis
- CISO role is re-enforced as a strategic advisor enabling innovation while managing risk.

Refreshed Exercises



- Case study discussions now include AI tradeoff analysis, forcing students to balance innovation, security, compliance, and talent impact.
- PEST analysis updated for AI-specific threats, regulatory uncertainty, and geopolitical considerations.
- Mission and metrics labs refreshed to account for GenAI-enabled capabilities and business value.
- Further policy labs expansion in AI and cloud policy considerations.
- Cyber42 simulations updated with AI- and cloud-related decision events that test executive communication, prioritization, and risk tolerance.

For more information: sans.org/LDR514

SANS

GIAC
CERTIFICATIONS