

# GIAC GSLC Certification Exam Prep Course: Cybersecurity Leadership and Governance

27 September – 1 October 2027
Cairo

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

# GIAC GSLC Certification Exam Prep Course: Cybersecurity Leadership and Governance

**Ref:** 2226_262807 **Date:** 27 September – 1 October 2027 **Location:** Cairo **Fees:** 4100 Euro

## Overview

GIAC GSLC Certification Exam Prep Course: Cybersecurity Leadership and Governance is a one-week course for experienced security managers and technical leads who want an individual GSLC study plan based on their practice results. Participants work through cases with competing answers, annotate the evidence behind their decisions, and compare their initial confidence with scored performance. They use the results to identify gaps across the exam objectives. Agile Leaders Training Center delivers this GSLC exam preparation course.

## Who Should Attend

- Managers who assign security responsibilities and explain control decisions to business owners.
- Operations leads who review alerts and authorize escalation.
- Technology leads who approve network, endpoint, cloud, or application safeguards.
- Risk and assurance staff who challenge evidence and track treatment decisions.
- Project and supplier leads who negotiate security requirements and verify delivery.

The course assumes participants already review security decisions at work and leaves out introductory system administration.

## Departments and Industries

The course draws its cases from teams with different service and risk priorities.

- Technology risk and security assurance in banking
- Network and service operations in telecommunications
- Incident coordination and continuity in healthcare
- Supplier assurance and project delivery in logistics
- Application and cloud security in retail

## Learning Objectives

By the end of this course, participants will be able to:

- Diagnose gaps using a GSLC diagnostic question set and confidence ratings.
- Apply risk and policy criteria to security leadership decisions.
- Analyze technical evidence to select proportionate controls.
- Evaluate incident escalation and recovery choices under time pressure.
- Compare cloud, application, AI, vendor, and project tradeoffs.

AGILE LEADERS
Training Center

- Build a study plan from objective scores and recurring errors.

## Course Agenda

### Day 1: Baseline and decision roles

- GSLC diagnostic question set and confidence rating
- Decision rights matrix for security reporting and personnel responsibilities
- Risk register ranking and business impact comparison
- Policy, standard, guideline, and baseline classification cards
- Awareness intervention scorecard for recurring human errors

### Day 2: Reasoning about technical controls

- Protocol and network threat matching from a packet summary
- Trust boundary diagram and segmentation control selection
- Symmetric, asymmetric, and hashing decision cards
- Data protection matrix for encryption in transit, encryption at rest, and privacy
- Endpoint attack evidence review and vulnerability remediation queue

### Day 3: Interpreting operational evidence

- SOC shift handover and escalation decision log
- SIEM correlation and SOAR playbook comparison with a machine learning alert example
- Incident phase sorting and evidence preservation checklist
- Recovery time and recovery point decision matrix for service continuity
- Timed SOC scenario practice with answer rationale and distractor analysis

### Day 4: Evaluating tradeoffs across services

- Cloud shared responsibility matrix and workload risk cases
- Secure development evidence checklist for DevOps and infrastructure as code
- AI use case register comparing business value, model risks, and safeguards
- Vendor negotiation worksheet for security obligations and acceptance criteria
- Project prioritization board and stakeholder support case questions

### Day 5: Timed practice and capstone

- Exercise: rank competing risk treatments using a decision rights matrix
- Exercise: interpret network, endpoint, and cryptography evidence in a timed case set
- Exercise: resolve a SOC escalation and defend the recovery sequence
- Exercise: score a mixed practice assessment and classify missed answers by objective
- Capstone exercise: build an individual GSLC study plan from the error log

## Practical Exercises

The course uses case packets and scoring sheets to make reasoning visible.

- Suggested activity: mark the evidence that rules out distractors in a compromised endpoint case.
- Suggested activity: use a hospital recovery scenario to defend the restoration order.
- Suggested activity: score a mixed question set and schedule targeted review using the error log.

## FAQs

### Who is suited to GIAC GSLC exam preparation and what experience does it assume?

The course suits managers and technical leads who already interpret security evidence and participate in decisions about risk, controls, and response.

### How does GIAC GSLC exam preparation differ from an introductory cybersecurity governance course?

GSLC preparation uses timed questions to assess decisions across governance and technical domains. Introductory governance courses typically focus on establishing policies and roles.

### How does GIAC GSLC exam preparation use practice questions?

The course uses independently authored scenarios. Participants justify each answer, identify the clue they missed, and record the exam objective they need to revisit.

## Conclusion

Participants leave with an individual GSLC study plan tied to a scored error log. The log shows which choices were affected by missing knowledge, misread evidence, or time pressure. The same method helps participants explain security decisions at work and direct their follow-up study to the topics that need more practice.