CONCEPT

Cybersecurity Audit Training: Auditing Cyber Controls and Programme Maturity



Cybersecurity Audit Training: Auditing Cyber Controls and Programme Maturity

Introduction:

Cybersecurity audit training on auditing cyber controls and programme maturity is a one-week course for internal auditors, IT auditors and assurance reviewers, ending with a cybersecurity audit programme and draft audit committee report for a case organisation. Many audit functions report on cyber risk from policy reviews and management assertions, so privileged access gaps, unpatched servers and untested restores stay outside the audit opinion. Nominees already perform audit engagements, and the course is taught through case studies built on scan outputs, access listings, log samples and maturity scores. CoreConcept Training Center delivers this course on cybersecurity audit.

Course Objectives:

- Scope a cybersecurity audit engagement from a cyber asset inventory, a risk ranking and a written scoping memo
- Convert NIST CSF outcomes, ISO/IEC 27001 Annex A controls and CIS Controls safeguards into testable audit criteria
- Test identity, vulnerability, monitoring, incident response and backup controls through inspection, reperformance and data sampling
- Assess third-party and cloud security arrangements and decide how far to rely on supplier assurance reports
- Score cyber programme maturity against evidence thresholds and show the gap between current and target profiles
- Draft cyber audit findings and a report that an audit committee can act on

Target Audience:

- Internal auditors responsible for including cyber risk in assurance engagements
- IT auditors responsible for testing technical security controls and their evidence
- Assurance and second-line reviewers responsible for checking cybersecurity programme claims
- Audit staff responsible for preparing cyber audit workpapers and evidence files
- Risk and control analysts responsible for tracking cyber remediation actions to closure

Course Outline:

Day 1: Cyber Risk, the Auditor's Role and Engagement Scoping

- Cyber Threat Landscape Mapped to Assurance Priorities for Auditors
- Assurance Map of Security, Risk and Audit Functions
- Cyber Asset and Data Flow Inventory for Audit Scoping
- Cybersecurity Audit Universe and Risk-Ranked Engagement Selection
- Engagement Scoping Memo with Objectives, Boundaries and Exclusions

Day 2: Control Frameworks as Cybersecurity Audit Criteria

- NIST CSF Functions Converted into Audit Test Objectives
- NIST CSF Current and Target Profiles for Gap Comparison
- ISO/IEC 27001 Annex A Controls as Testable Criteria
- CIS Controls Safeguards and Implementation Groups as Baselines
- Cross-Framework Criteria Matrix for a Single Audit Programme

Day 3: Testing Core Cyber Controls

- Cyber Policy Set and Security Role Charter Review
- Identity and Access Test Steps for Privileged and Remote Accounts
- Vulnerability Scan Output and Patch Ageing Report Analysis
- SIEM Alert Rules and Log Retention Coverage Testing
- Incident Response Plan, Playbooks and Exercise Record Review

Day 4: Resilience, Third Parties, Maturity Scoring and Evidence Problems

- Backup Restore Test Records and Immutable Copy Verification
- Third-Party Security Questionnaires and Assurance Report Reliance
- Cloud Shared Responsibility Matrix and Configuration Review Evidence
- Cyber Maturity Scoring Scale with Evidence Thresholds per Level
- Evidence Sufficiency Tests Using Inquiry, Inspection and Reperformance

Day 5: Case Study Work on a Cybersecurity Audit Programme and Draft Report

- Case Organisation Scoping Memo and Criteria Matrix Build
- Case Control Test Sheets for Access and Vulnerability Areas
- Case Maturity Heat Map Across NIST CSF Functions
- Cyber Audit Findings Written as Condition, Criteria, Cause, Effect
- Cybersecurity Audit Programme and Audit Committee Draft Report Completion

Skills You Will Gain:

- Cyber Audit Scoping
- Control Criteria Mapping
- Privileged Access Testing
- Patch Ageing Analysis
- Log Coverage Assessment
- Supplier Assurance Reliance
- Cyber Maturity Scoring
- Audit Committee Reporting

Why Attend This Course:

- Deliver a cybersecurity audit programme and draft report for a case organisation to the chief audit executive for adaptation to the next audit plan
- Decide whether scan results, access listings and restore records are sufficient evidence to support a cyber audit opinion
- Avoid issuing cyber assurance that rests on policy reading alone and leaves exploitable control gaps outside the audit opinion
- Share the criteria matrix and control test sheets with audit colleagues so that cyber engagements follow one method

Conclusion:

Back at work, the participant gives the chief audit executive a cybersecurity audit programme and draft report that can be adapted to the organisation's own systems and audit plan. The audit function uses the criteria matrix to agree scope with security management, and the audit committee receives maturity scores and findings tied to evidence rather than assertions. After its first use, the function should review which tests produced reliable evidence, where maturity scores were disputed and how quickly management closed the agreed actions.

Frequently Asked Questions FAQ:

What should participants know before cybersecurity audit training on cyber controls?

Participants should already carry out audit or assurance engagements and understand basic control testing. Familiarity with user accounts, networks and security tools at user level helps, but no engineering background is needed. An anonymised scan report or access listing helps participants apply the case work.

How does cybersecurity audit training differ from a general IT audit course?

It concentrates on the cybersecurity programme itself: framework criteria, access, vulnerability, monitoring, incident response, backup, third-party and cloud controls, and maturity scoring. General IT audit courses spread time across general and application controls and cover cyber topics only briefly.

Why does a cybersecurity audit use maturity scoring as well as control testing?

Control tests show whether individual safeguards operate, while maturity scoring shows how consistently the whole programme is managed and improved. Together they let the audit committee see specific failures and the distance between the current and target state of the programme.

What do participants take back from cybersecurity audit training on cyber controls?

Participants take back a cybersecurity audit programme with a scoping memo, criteria matrix, control test sheets and maturity heat map, plus a draft report for a case organisation. Each part can be adapted to their own audit plan and systems.