1. Record Nr. UNINA9911117699903321

Autore	Edwards Jason
Titolo	Cybersecurity Auditing : Principles, Practices, and Frameworks
Pubbl/distr/stampa	Newark : , : John Wiley & Sons, Incorporated, , 2026 ©2026
ISBN	9781394423057
Edizione	[1st ed.]
Descrizione fisica	1 online resource (593 pages)
Disciplina	005.8
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Half Title Page -- Title Page -- Copyright -- Contents -- Preface -- Acknowledgments -- About the Companion Website -- Chapter 1: The Role of Audit in Security Governance, Risk, and Compliance -- Assurance Mandate Within the Three Lines Model -- Audit Charter, Authority, and Independence Boundaries -- Governance Interfaces: Board/Audit Committee, CISO, Legal, Privacy -- Policy-Standards-Procedures Architecture (Audit View) -- GRC Architecture: Control Library and Risk Register -- Exception and Waiver Governance -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 2: Security Standards and Regulations -- Auditor's Use of Frameworks -- Common Control Set and Cross-framework Traceability -- Multi-regime Scoping: Entities, Systems, and Data Classes -- Equivalency and Mapping Rules: Sufficiency and Residual Gaps -- Portfolio Evidence Packs and Evidence Reuse -- Inherited/Shared Controls and Third-party Reliance (SOC, Certifications) -- Deviations and Compensating Controls: Carve-outs and Documentation -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 3: Risk Assessment and Control Design for Modern Systems -- Cyber Risk Taxonomy and Materiality -- Control Design Choices -- Traceability -- Design Reviews and Auditor Boundaries -- Integration with Enterprise Architecture and Change Governance -- Design Documentation: Approvals, RACI, and Version Control -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 4: Evidence, Sampling, and Testing Techniques -- Evidence Quality and

Chain of Custody -- Building Populations and Defensible Sampling Strategies -- Test Types: Design vs. Operating Effectiveness -- Inspection and Re-performance Procedures -- Analytics-assisted Testing and Tooling Considerations -- Period Coverage, Timing, and Frequency of Tests.
Workpaper Standards and Reviewability -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 5: Auditor Ethics, Independence, and Professional Judgment -- Code of Ethics and Objectivity in Cyber Audits -- Independence Threats and Safeguards -- Confidentiality, Data Handling, and Sensitive Evidence -- Professional Skepticism and Cognitive Bias Awareness -- Forming Conclusions Under Uncertainty and Incomplete Evidence -- Managing Management Pressure and Disagreement -- Documenting Judgment -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 6: Identity and Access Management -- Identity Life cycle: Joiner-Mover-Leaver and Sources of Truth -- Authentication Controls: MFA, SSO, Federation, and Risk-based Access -- Privileged Access: PAM, Break-glass, Session Monitoring -- Service Accounts, Nonhuman Identities, and Secrets Handling -- Evidence Locations: IdP, PAM, HRIS, Ticketing, and Logs -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 7: Network and Perimeter Security -- Network Segmentation and Trust Zones -- Firewall and Egress Controls (Allowlists, Rule Hygiene, Change History) -- Secure Edge/SASE and Remote Access (VPN/ZTNA Posture) -- DNS, Web Proxies, and URL Filtering (Policy Alignment) -- Intrusion Prevention/Threat Intel at the Edge -- Device/Config Management: Baselines, Backups, and Drift -- Evidence Locations -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 8: Application and API Security/CI-CD -- SDLC Governance and "Policy as Code -- Code and Dependency Scanning: SAST, SCA, and Secrets Detection -- Dynamic Testing and API Security: DAST, AuthN/AuthZ, and Rate Limits -- Infrastructure as Code and Environment Hardening -- Release Governance: Change Approval Gates and Rollback Paths -- Evidence Locations: Repos, Pipelines, Registries, and API Gateways.
Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 9: Cloud and SaaS Security -- Shared Responsibility and Tenant Scope (IaaS/PaaS/SaaS) -- Identity Boundaries in Cloud: Roles, Policies, and SCPs/Guardrails -- Baseline Configurations -- Logging/Telemetry in Cloud and SaaS -- Data-plane Protections: Keys, Secrets, and Segmentation -- Evidence Locations: CSP Config State, Org Policies, SaaS Admin Exports -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 10: Data Protection -- Data Classification and Handling Requirements -- Encryption in Transit and at Rest -- Key Management: Generation, Rotation, Custody, and Separation of Duties -- Hardware/Cloud KMS/HSM Controls and Access Boundaries -- Tokenization, Masking, and DLP Policy Design -- Data Flow Mapping and High-risk Stores/Paths -- Evidence Locations: KMS/HSM Logs, Key Policies, DLP Events, and Configs -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 11: Logging, Monitoring, and Detection -- Log Coverage Model: Sources, Depth, and Retention Targets -- Integrity and Tamper Resistance -- Detection Content Quality: Precision/Recall, Tuning, and Suppression -- Use-case Catalog and Ownership -- Alert Triage Interfaces and Escalation Paths -- Telemetry Gaps and Compensating Signals -- Evidence Locations: SIEM/Log Platform, Detection Repositories, and Tuning Records -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 12: Incident Response and Crisis Management -- IR Operating Model -- Detection Handoffs and Case

Life Cycle (from Alert to Closure) -- Forensics and Evidence Handling (Chain of Custody) -- Communications and Regulatory Notifications -- Backup/Restore Readiness and BCP/DR Alignment (RTO/RPO) -- Tabletop Exercises and Post-incident Learning.
Evidence Locations: IR Plans, Case Systems, Forensic Repositories, and DR Reports -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 13: Vulnerability Management and Pen Test Oversight -- Asset Coverage and Scan Cadence -- Prioritization: KEV, EPSS, Exploitability, and Business Context -- Remediation SLAs, Exceptions, and Risk Acceptance -- Validation of Fixes and Regression Controls -- Penetration Testing Governance: Independence, Scope, and Reporting -- Findings Life cycle and Cross-team Accountability -- Evidence Locations: Scanners, Ticketing, Exception Registers, and Pen Test Artifacts -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 14: Third-party and Supply-chain Security -- Vendor Risk Segmentation and Due Diligence Depth -- Contractual Security Clauses and Right-to-audit/Assurance Rights -- Assurance Artifacts: SOC Reports, SIG/CAIQ, and Certifications -- Continuous Monitoring: Questionnaires, Signals, and Triggers -- Software Supply Chain: SBOM, Dependency Risk, and Build Provenance -- Remediation and Offboarding/Exit Strategies -- Evidence Locations: Procurement/TPRM Systems, Contracts, and Assurance Repos -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 15: OT/ICS and Critical Infrastructure Audits -- Safety and Availability Constraints (Risk Trade-offs) -- Zones and Conduits: Network Segmentation for ICS -- Allowlist/Whitelist Controls and Remote Access Methods -- Patch/Change Realities: Compensating Controls and Windows -- Monitoring and Physical/Environmental Dependencies -- Regulatory and Standards Context -- Evidence Locations: ICS Diagrams, Change Logs, Site Procedures, and Operator Logs -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 16: Sector Overlays (Financial, Healthcare, Public.
Overlay Scoping: Identifying In-scope Systems, Data, and Obligations -- Financial Services (FFIEC/GLBA): Controls Emphasis and Artifacts -- Healthcare (HIPAA/HITRUST): Safeguards, Mappings, and Evidence Nuances -- Public Sector (FedRAMP, State/Local): Authorizations and Continuous Monitoring -- PCI DSS: Prescriptive Requirements and Segmentation/Scope Control -- Reconciling Conflicts: Precedence Rules and Documentation -- Evidence Locations: Regulator-specific Workpapers, ATO Packages, ROC/SAQ -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 17: Automation, Continuous Auditing, and Advanced Analytics -- Objectives and Scope of Automated Assurance -- Data Sources and Pipelines (Lineage, Quality, and Access Controls) -- Job Design and Governance (Change Control, Versioning, and Approvals) -- Automated Control Tests: Types, Frequencies, and Coverage Models -- Accuracy and Reliability: Ground-truthing, Thresholds, and Drift in Tests -- Dashboards and Variance Analysis (Interpreting Results and Triggering Follow-ups) -- Conclusion -- Auditor Recommendations -- Chapter Questions -- Chapter 18: AI Threat Modeling and Attack Surfaces -- Scoping AI Assets: Models, Datasets, Prompts, Tools, and Agents -- Threat Modeling Methods for AI Systems (STRIDE/ATT&amp -- CK Extensions) -- Core Attack Surfaces: Prompt Injection, Data Leakage, and Model Theft/Extraction -- Data Integrity Risks: Poisoning, Backdoors, and Training Set Governance -- Abuse Paths via Integrations: Plugins, Connectors, and Tool Invocation -- Control Objectives and Risk Acceptance Criteria for AI Systems -- Documentation and Traceability: from Threat to Control to Evidence -- Conclusion -- Auditor

	Recommendations -- Chapter Questions -- Chapter 19: Secure MLOps and Model/Endpoint Controls -- Supply Chain Integrity: Artifacts, Registries, Signing, and Provenance. Environment Hardening: Build/Train/Serve Isolation and Access Boundaries.
Sommario/riassunto	Practical guide to cybersecurity controls, systems, programs, and management This book is a comprehensive, field-tested guide to the full spectrum of cybersecurity auditing, enabling readers to assess, evaluate, and improve security controls across today's complex IT environments.