# Course Title: Auditing Cybersecurity & Information Security Frameworks

- **Duration:** 5 Days (approximately 35-40 instructional hours)
- **Course Goal:** To provide IT auditors, internal auditors, and cybersecurity professionals with the knowledge, methodologies, and practical skills to effectively plan, conduct, and report on audits of an organization's cybersecurity posture and its alignment with leading industry frameworks like the NIST Cybersecurity Framework (CSF) and ISO 27001/27002.
- **Core Focus:** Moving beyond basic IT general controls to provide comprehensive assurance over an organization's ability to identify, protect against, detect, respond to, and recover from cybersecurity threats.

**Learning Objectives:**

Upon successful completion of this workshop, participants will be able to:

- **Understand** the modern cybersecurity threat landscape and its implications for business.
- **Articulate** the structure, purpose, and key components of the NIST Cybersecurity Framework (CSF) and the ISO 27001 Information Security Management System (ISMS).
- **Develop** a risk-based audit plan to assess an organization's cybersecurity capabilities against a chosen framework.
- **Design** and execute audit procedures to test the design and operating effectiveness of key cybersecurity controls.
- **Audit** critical cybersecurity domains, including asset management, access control, vulnerability management, incident response, and business continuity.
- **Assess** the effectiveness of security awareness and training programs.
- **Evaluate** the organization's third-party/vendor cybersecurity risk management program.
- **Interpret** technical evidence, such as vulnerability scan reports, log files, and system configurations.
- **Craft** clear, impactful audit findings and recommendations that are actionable for both technical and executive audiences.
- **Provide** meaningful assurance to the Board and senior leadership on the organization's cybersecurity resilience.

**Target Audience:**

- IT Auditors and Senior IT Auditors.
- Internal Auditors with an interest in or responsibility for technology risk.
- Cybersecurity Professionals, Information Security Managers, and Analysts.
- Risk Management and Compliance Professionals.
- IT Leaders who want to understand how their programs will be audited.

**Prerequisites:**

- A strong understanding of fundamental IT audit principles and IT General Controls (ITGC).
- Familiarity with basic IT and networking concepts.
- Experience in conducting or managing IT audits is highly beneficial. (Certifications like CISA are a plus).

**Teaching Methodology:**

This is a highly interactive and case-based workshop. The methodology includes:

- **Interactive Lectures & Framework Deconstruction:** Breaking down the NIST CSF and ISO 27001 standards into auditable components.
- **Case Study-Based:** A central case study of a fictional organization will be used for all risk assessment and audit planning exercises.
- **Hands-on Workshops:** The core of the course. Participants will work in teams to develop risk & control matrices, audit programs, and test procedures.
- **Technical Evidence Review:** Analyzing sample technical outputs (e.g., vulnerability scans, access logs, incident reports) to practice evidence interpretation.
- **Tabletop Exercises & Simulations:** Simulating scenarios like an incident response walkthrough or a third-party risk assessment.
- **Group Discussions & Peer Learning:** A collaborative environment for sharing audit approaches and challenges.

ADEPT TRAINING CENTER

**Materials Provided:**

- Comprehensive digital or printed workbook with key concepts, framework mappings, audit methodologies, and best practices.
- An "Cybersecurity Auditor's Toolkit" with templates for a Cybersecurity Risk & Control Matrix, an ISO 27001 Statement of Applicability (SoA) review guide, and a NIST CSF-based audit program.
- A detailed case study with supporting documents (e.g., security policies, risk assessments, incident reports).
- Publicly available copies of the NIST CSF and summaries of ISO 27001/27002 controls.
- Certificate of Completion.

---

**Detailed Day-by-Day Curriculum**

**Day 1: The Cybersecurity Audit Universe & The NIST CSF**

- **Module 1: The Modern Threat Landscape & The Auditor's Role (Approx. 2 hours)**
    - Welcome, introductions, and course objectives.
    - Overview of the current cybersecurity threat landscape (e.g., ransomware, phishing, supply chain attacks, insider threats).
    - The business impact of a cyber breach.
    - The strategic role of the auditor in providing assurance over cybersecurity resilience.
    - Key stakeholders for a cybersecurity audit (Board, CISO, CIO, business leaders).
- **Module 2: Introduction to Cybersecurity Frameworks (Approx. 2 hours)**
    - Why use a framework? (Structure, repeatability, comparability, best practices).
    - Overview of leading frameworks:
        - **NIST Cybersecurity Framework (CSF):** The primary focus for its risk-based and business-friendly approach.
        - **ISO 27001/27002:** The international standard for an Information Security Management System (ISMS).
        - CIS Controls, COBIT (briefly).
- **Module 3: Deep Dive into the NIST Cybersecurity Framework (CSF) (Approx. 3.5 hours)**
    - The three parts of the CSF: The **Framework Core**, **Implementation Tiers**, and **Framework Profiles**.
    - **The Framework Core:** A detailed walkthrough of the 5 Functions:

1. **Identify:** Asset Management, Risk Assessment, Governance.
2. **Protect:** Access Control, Training, Data Security.
3. **Detect:** Anomalies & Events, Continuous Monitoring.
4. **Respond:** Response Planning, Communication, Analysis.
5. **Recover:** Recovery Planning, Improvements.

    - Understanding the Categories and Subcategories within each Function.
    - **Workshop:** Participants map their organization's existing security activities to the 5 Functions of the NIST CSF.
    - **End of Day 1 Recap & Q&A.**

**Day 2: Planning the Cybersecurity Audit & Auditing the "Identify" & "Protect" Functions**

- **Module 4: Scoping & Planning a NIST CSF-Based Audit (Approx. 2.5 hours)**
    - Defining the audit scope and objectives.
    - Using the NIST CSF to structure a risk-based audit plan.
    - Creating a **Framework Profile:** Defining the organization's "Current Profile" vs. its "Target Profile."
    - Developing a Cybersecurity Risk & Control Matrix based on the CSF subcategories.
- **Module 5: Auditing the "Identify" Function (Approx. 2 hours)**
    - Audit procedures for:

ADEPT TRAINING CENTER

        - **Asset Management:** Hardware/software inventories, data classification.
        - **Risk Assessment:** Reviewing the cybersecurity risk assessment process.
        - **Governance:** Auditing the information security policy framework and roles/responsibilities.
- **Module 6: Auditing the "Protect" Function – Part 1 (Access Control & Training) (Approx. 3 hours)**
    - Audit procedures for:
        - **Identity Management & Access Control:** User provisioning/de-provisioning, privileged access management (PAM), password policies, multi-factor authentication (MFA).
        - **Awareness & Training:** Assessing the effectiveness of security awareness training and phishing simulations.
    - **Evidence Review Workshop:** Participants analyze sample user access review reports and phishing campaign results.
    - **End of Day 2 Recap & Q&A.**

**Day 3: Auditing the "Protect" & "Detect" Functions**

- **Module 7: Auditing the "Protect" Function – Part 2 (Data & System Security) (Approx. 2.5 hours)**
    - Audit procedures for:
        - **Data Security:** Data encryption (at rest, in transit), data loss prevention (DLP) controls.
        - **Protective Technology:** Reviewing configurations of firewalls, endpoint protection, etc.
        - **Maintenance & Vulnerability Management:** Auditing the patch management and vulnerability scanning processes.
    - **Evidence Review Workshop:** Participants interpret a sample vulnerability scan report and identify key audit issues.
- **Module 8: Auditing the "Detect" Function (Approx. 2.5 hours)**
    - Audit procedures for:
        - **Anomalies & Events:** Assessing the logging and monitoring capabilities.
        - **Security Continuous Monitoring:** Reviewing the Security Information and Event Management (SIEM) system's effectiveness.
        - **Detection Processes:** How alerts are generated, correlated, and escalated.
- **Module 9: Introduction to the ISO 27001/27002 Framework (Approx. 2.5 hours)**
    - What is an Information Security Management System (ISMS)?
    - The Plan-Do-Check-Act (PDCA) cycle in ISO 27001.
    - The relationship between the management clauses (4-10) and the Annex A controls.
    - The **Statement of Applicability (SoA):** The central document for an ISO 27001 audit.
    - **Workshop:** Mapping key ISO 27001 Annex A controls to the NIST CSF Functions.
    - **End of Day 3 Recap & Q&A.**

**Day 4: Auditing "Respond" & "Recover" & The ISO 27001 Audit**

- **Module 10: Auditing the "Respond" Function (Approx. 3 hours)**
    - Audit procedures for:
        - **Response Planning:** Reviewing the Incident Response (IR) Plan.
        - **Communication:** Assessing internal and external communication plans for a breach.
        - **Analysis:** Auditing the process for analyzing incidents to determine impact.
        - **Mitigation:** Evaluating the effectiveness of incident containment activities.
    - **Tabletop Simulation:** A facilitated walkthrough of an incident response scenario to test the plan and decision-making.
- **Module 11: Auditing the "Recover" Function (Approx. 2 hours)**
    - The link between Incident Response, Disaster Recovery (DR), and Business Continuity (BCP).
    - Audit procedures for:
        - **Recovery Planning:** Reviewing DR/BCP plans and testing results.

ADEPT TRAINING CENTER

        - **Improvements:** Auditing the post-incident "lessons learned" process.

- **Module 12: Conducting an ISO 27001 Based Audit (Approx. 2.5 hours)**
    - Scoping the ISMS audit.
    - Auditing against the management clauses (e.g., leadership commitment, risk assessment, internal audit, management review).
    - Using the Statement of Applicability (SoA) to test the implementation and effectiveness of selected Annex A controls.
    - The concept of non-conformities (major and minor).
    - **Workshop:** Participants review a sample SoA and develop audit test steps for a selection of controls.
    - **End of Day 4 Recap & Q&A.**

**Day 5: Reporting, Third-Party Risk & Your Audit Plan**

- **Module 13: Auditing Third-Party & Supply Chain Cybersecurity Risk (Approx. 2.5 hours)**
    - The critical risk of supply chain attacks.
    - Audit procedures for assessing the third-party risk management program:
        - Vendor due diligence and risk tiering.
        - Contractual security requirements.
        - Reviewing SOC 2 reports and other third-party attestations.
        - Ongoing monitoring of third parties.
- **Module 14: Reporting Cybersecurity Audit Findings (Approx. 2 hours)**
    - The challenge of communicating technical risks to a non-technical board and executive audience.
    - Structuring the cybersecurity audit report.
    - Writing clear, concise findings and actionable, risk-based recommendations.
    - Using maturity models and heat maps to visualize cybersecurity posture.
- **Module 15: Capstone: Developing a Cybersecurity Audit Program (Approx. 2.5 hours)**
    - **Capstone Workshop:** Participants work in groups to develop a high-level, risk-based cybersecurity audit program for the case study organization.
    - The program will be based on the NIST CSF and will include:

1. Audit Objectives and Scope.
2. Key Risk Areas to be covered in each of the 5 Functions.
3. Examples of key controls to test and evidence to be gathered.
    - Groups present their programs for peer and instructor feedback.

- **Module 16: Course Review & Your Action Plan (Approx. 1 hour)**
    - Review of the key frameworks and audit approaches.
    - Open forum for final questions.
    - **Action Planning:** Participants identify key steps they can take to implement or enhance cybersecurity auditing in their organization.
    - Course evaluation and closing.

ADEPT TRAINING CENTER