**📍 Day 1: ISO/IEC 27001**

**1. What to Study Today**

* **Core concepts**: ISMS (Information Security Management System), Risk-based approach, Annex A controls.
* **Implementer View**: How to establish, implement, maintain, and continually improve ISMS.
* **Auditor View**: How to check compliance, collect evidence, identify non-conformities, and write audit reports.

**2. Free & Accessible Study Materials**

**Official Documents & Standards**

* [ISO 27001:2022 overview (ISO.org)](https://www.iso.org/standard/27001) → high-level intro (official site).
* [ISO 27001 Controls (Annex A 2022 update – Summary PDF)](https://advisera.com/27001academy/iso-27001-2022-controls/) → free breakdown of 93 updated controls.

**Guides & Blogs**

* [Simplilearn ISO 27001 Beginner’s Guide](https://www.simplilearn.com/tutorials/cyber-security-tutorial/iso-27001) → plain-language explainer.
* [27001 Academy Free Learning Center](https://advisera.com/27001academy/iso-27001-knowledgebase/) → practical implementer resources.

**Video Resources**

* YouTube: “ISO 27001 Explained in 5 Minutes” – quick intro.
* YouTube: “ISO 27001 Lead Auditor Training – Free Intro” – shows how auditors approach evidence.

**3. Implementer Checklist (What to Learn Today)**

* Understand **ISMS lifecycle** (Plan → Do → Check → Act).
* Learn **Annex A control categories** (e.g., Access Control, Cryptography, Supplier Relationships).
* Study how to **conduct a risk assessment** (asset → threat → vulnerability → impact).

**4. Auditor Checklist (What to Learn Today)**

* Learn types of **audits**: Internal audit, Certification audit, Surveillance audit.
* Understand **audit evidence** (policies, logs, screenshots, interviews).
* Learn **non-conformity categories** (Minor, Major, Observations).
* Review **sample ISO 27001 audit report** → [Example PDF](https://advisera.com/27001academy/knowledgebase/iso-27001-internal-audit-report-example/)

**5. Practical Task for You Today**

* Create a **1-page framework journal entry**:
  1. Framework Name & Purpose.
  2. ISMS Key Concepts.
  3. Top 5 Annex A controls you understood.
  4. Auditor’s focus areas.
  5. Example: Pick a control (e.g., Access Control) and write one **implementer action** and one **auditor check**.

✅ **End of Today’s Outcome**:

* You’ll have a **practical understanding of ISO 27001** from both sides.
* You’ll have **your first journal page ready** (the start of your GRC playbook).
* Tomorrow, we’ll move to **NIST CSF**.

In ISO/IEC 27001:2022, the **mandatory clauses and subclauses** (i.e., you must have documented evidence for them, otherwise you fail) are in **Clauses 4–10**. Clauses 1–3 are just scope/reference.

Here’s the breakdown:

**✅ Mandatory Clauses (with Subclauses)**

**Clause 4 – Context of the Organization**

* **4.1** Understanding the organization and its context
* **4.2** Understanding the needs and expectations of interested parties
* **4.3** Determining the scope of the ISMS
* **4.4** Information Security Management System (establish, implement, maintain, continually improve)

**Clause 5 – Leadership**

* **5.1** Leadership and commitment
* **5.2** Information security policy
* **5.3** Organizational roles, responsibilities and authorities

**Clause 6 – Planning**

* **6.1** Actions to address risks and opportunities
  + **6.1.1** General
  + **6.1.2** Information security risk assessment
  + **6.1.3** Information security risk treatment
* **6.2** Information security objectives and planning to achieve them
* **6.3** Planning of changes

**Clause 7 – Support**

* **7.1** Resources
* **7.2** Competence
* **7.3** Awareness
* **7.4** Communication
* **7.5** Documented information
  + **7.5.1** General
  + **7.5.2** Creating and updating
  + **7.5.3** Control of documented information

**Clause 8 – Operation**

* **8.1** Operational planning and control
* **8.2** Information security risk assessment
* **8.3** Information security risk treatment

**Clause 9 – Performance Evaluation**

* **9.1** Monitoring, measurement, analysis and evaluation
* **9.2** Internal audit
  + **9.2.1** General
  + **9.2.2** Internal audit programme
* **9.3** Management review

**Clause 10 – Improvement**

* **10.1** Nonconformity and corrective action
* **10.2** Continual improvement

**✅ Mandatory Documentation / Records for Audit**

(These are minimum “must-have” evidence auditors check)

* **ISMS Scope** (Clause 4.3)
* **Information Security Policy** (Clause 5.2)
* **Risk assessment and risk treatment methodology** (Clause 6.1.2 & 6.1.3)
* **Statement of Applicability (SoA)** → shows which Annex A controls are applied/excluded
* **Risk treatment plan & Risk register**
* **Information security objectives** (Clause 6.2)
* **Competence records** (Clause 7.2)
* **Awareness training evidence** (Clause 7.3)
* **Internal audit programme & reports** (Clause 9.2)
* **Management review minutes** (Clause 9.3)
* **Nonconformity & corrective actions log** (Clause 10.1)

👉 **In short:** Clauses **4–10** are mandatory, and you **must show evidence** of policies, risk assessments, SoA, objectives, training, audits, and reviews. Missing any of these = **Major Nonconformity** → certification fail.

**📅 Day 2 Focus – *Annex A Controls Deep Dive (ISO/IEC 27001:2022)***

* **Understand the 4 Themes (Categories):**
  1. Organizational Controls
  2. People Controls
  3. Physical Controls
  4. Technological Controls
* **Learn the 14 Control Domains** (from the older version, still widely used in practice for audits). Compare how 2022 has simplified into 93 controls from 114.
* **Perspective Split:**
  1. **Implementer view:** How to put each control into practice (e.g., A.5.1 Information Security Policies → drafting and communicating policies).
  2. **Auditor view:** What evidence to check (policy doc, approval signatures, awareness logs).
* **Deliverable for the day:**
  1. Make a **2-column table** for at least 20 controls:
     + *Column 1 = Control Name & Objective*
     + *Column 2 = Implementation & Audit Evidence*