Today we are stepping into **NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations** — the *heaviest* and *most detailed* framework you’ll study in GRC.

This is the **U.S. Federal Government’s gold standard** for information security and risk management. Even if you don’t work in the U.S., many organizations map their controls to NIST 800-53 because of its depth.

**📅 Day Plan: NIST SP 800-53**

**🔹 Step 1 – Understand the Structure**

* **Control Families**: 20 groups of controls (like ISO’s Annex A, but far more detailed).
* **Controls & Enhancements**: ~1,189 controls (Rev. 5). Each family has a set of base controls and “control enhancements” for higher maturity.
* **Baselines**: Low, Moderate, High (depending on system criticality).

**🔹 Step 2 – The 20 Control Families (with examples)**

1. **AC – Access Control** (least privilege, RBAC, separation of duties)
2. **AT – Awareness & Training** (security awareness programs)
3. **AU – Audit & Accountability** (log management, monitoring)
4. **CA – Security Assessment & Authorization** (system authorization, continuous monitoring)
5. **CM – Configuration Management** (secure baseline configs, change control)
6. **CP – Contingency Planning** (disaster recovery, backups)
7. **IA – Identification & Authentication** (MFA, unique IDs)
8. **IR – Incident Response** (IR policy, reporting, testing)
9. **MA – Maintenance** (system maintenance security)
10. **MP – Media Protection** (secure handling of data/media)
11. **PE – Physical & Environmental Protection** (facilities, physical access)
12. **PL – Planning** (system security plans)
13. **PS – Personnel Security** (background checks, terminations)
14. **RA – Risk Assessment** (periodic risk analysis)
15. **SA – System & Services Acquisition** (security in procurement/contracts)
16. **SC – System & Communications Protection** (encryption, boundary defense)
17. **SI – System & Information Integrity** (anti-malware, patching)
18. **SR – Supply Chain Risk Management** (vendor security)
19. **PM – Program Management** (governance, roles & responsibilities)
20. **PT – Privacy Controls** (data privacy & consent management)

**🔹 Step 3 – Implementer vs Auditor Lens**

* **Implementer:**
  + Start with baseline (Low/Moderate/High)
  + Select controls → implement policies, tools, processes
  + Document in a **System Security Plan (SSP)**
  + Perform risk assessments & POA&M (Plan of Action & Milestones)
* **Auditor:**
  + Verify SSP & evidence (logs, configs, awareness records)
  + Interview stakeholders
  + Test effectiveness of controls
  + Check POA&M closure and continuous monitoring

**🔹 Step 4 – Practical Deliverable for You Today**

Make a **study table with 5 most critical families** (AC, AU, IA, IR, SC).  
Columns:

1. **Family**
2. **Example Control**
3. **Implementation (how to apply)**
4. **Audit Evidence (what to check)**

👉 This will give you a **ready audit vs implementer cheat sheet** for the most frequently asked families.

**📚 Study Materials for Today**

* **NIST SP 800-53 Rev. 5 Official PDF** → link
* **NIST Control Family Quick Reference Sheets** → search “NIST 800-53 control families cheat sheet”
* ISACA / SANS whitepapers on mapping ISO 27001 ↔ NIST 800-53

⚡ My tip: Don’t try to memorize all 1,000+ controls. Focus on:

* **Family names**
* **Core purpose of each family**
* **Typical evidence** (logs, policies, configs, awareness docs).