Here’s how we’ll structure your **Day Plan for NIST CSF**:

**📌 Step 1 – Core Functions (High-Level)**

NIST CSF is built around **5 Functions** (these are like the backbone of the framework):

1. **Identify** – Know what you need to protect
2. **Protect** – Safeguards to ensure services continue
3. **Detect** – Identify cybersecurity events quickly
4. **Respond** – Take action on detected events
5. **Recover** – Maintain resilience and restore after incidents

👉 Think of this as a **lifecycle**: from knowing your assets → protecting → monitoring → reacting → bouncing back.

**📌 Step 2 – Categories & Subcategories**

Each Function breaks into **Categories** (23 in total) and **Subcategories** (108).

* Example: Under **Protect → Access Control (PR.AC)** → subcategories like unique IDs, role-based access, least privilege.

**📌 Step 3 – Implementation Tiers**

NIST CSF defines **Tiers (1–4)** that show maturity of adoption:

1. **Partial** (ad hoc, reactive)
2. **Risk-Informed** (some risk practices, not consistent)
3. **Repeatable** (policies, procedures followed consistently)
4. **Adaptive** (continuous improvement, proactive)

**📌 Step 4 – Profiles**

* A **Profile** is basically your organization’s **current vs target state**.
* Helps identify **gaps** and plan improvements.

**📌 Step 5 – Implementer vs Auditor View**

* **Implementer:** Build asset inventory, risk assessment, access controls, monitoring tools, IR playbooks.
* **Auditor:** Check for documented policies, monitoring dashboards, incident response drills, evidence of lessons learned.

**📚 Study Material for Today**

* **Official NIST CSF 2.0 PDF (2024 update)** – [direct link](https://www.nist.gov/cyberframework) (free download).
* **NIST CSF Quick Start Guide** – available on same site, simpler view.
* **Practical Guide:** Search “NIST CSF implementation roadmap” (lots of good diagrams).
* **Audit View:** ISACA whitepapers on NIST CSF audits (free if you register).

✅ **Deliverable for you today:**

* Draw a **5-column table** → Functions across the top (Identify, Protect, Detect, Respond, Recover).
* Under each, list **3–5 key categories + 1 example control**.
* Add two extra columns: *Implementation Evidence* and *Audit Evidence*.

That one sheet = **your NIST CSF ready-reference**.