### 📢 Internal Team Briefing: The "Big Three" Saudi Frameworks

**Objective:** Understand the regulatory landscape of Saudi Arabia to build the logic for our GRC (Governance, Risk, Compliance) App.

#### 1. The Hierarchy: Who makes the rules?

In Saudi Arabia, there is no "single" audit. Companies must answer to different "bosses" depending on who they are.

| **Acronym** | **Full Name** | **Who are they?** | **Who listens to them?** | **Our App's Role** |
| --- | --- | --- | --- | --- |
| **NCA** | National Cybersecurity Authority | The "FBI" of Cyber. They set the baseline security rules for the whole country. | **Everyone.** Especially Government & Critical Infrastructure. | **The "Default" Audit.** Every customer gets this. |
| **SAMA** | Saudi Central Bank | The "Federal Reserve" of KSA. Extremely strict. | **Banks, Fintechs, Insurance.** (Our highest-paying target clients). | **The "Premium" Audit.** Complex, strict, high-value. |
| **SDAIA** | Saudi Data & AI Authority | The "Privacy Police." They own the Data Protection Law (PDPL). | **Everyone.** Any company holding customer data. | **The "Privacy" Module.** Mandatory for all. |

#### 2. The Files We Downloaded (Our "Data Fuel")

We have secured the official source documents. Here is how we use each one in the application:

**A. ECC--2024-EN.pdf (NCA Essential Cybersecurity Controls)**

* **What is it?** The absolute minimum security standard for Saudi Arabia.
* **Key Concept:** It has **"Domains"** (Categories) like *Cybersecurity Governance*, *Defense*, *Resilience*.
* **For the Dev Team:** This file contains the **Base Schema**.
  + *Table:* nca\_controls
  + *Columns:* Control ID (e.g., 2-1-1), Requirement, Evidence\_Type.
* **Why it matters:** If a company fails this audit, they cannot work with the government.

**B. Cyber Security Framework.pdf (SAMA CSF)**

* **What is it?** The specific rules for Banks. It is stricter than NCA.
* **Key Concept:** "Maturity Levels." Banks aren't just Compliant/Non-Compliant; they are graded (3.0, 4.0, 5.0).
* **For the Dev Team:** This introduces **"Logic Complexity."**
  + *Overlap:* SAMA Control 3.1 is almost identical to NCA Control 2-1.
  + *Feature:* Our app must link these two so the user doesn't do the work twice.

**C. Personal Data Protection Law (PDPL).pdf**

* **What is it?** The "Saudi GDPR."
* **Key Concept:** **Consent.** Did the user agree to give their data?
* **For the Dev Team:** This creates a new **"Form Type."**
  + Instead of just "Server Security," this audit asks for "Legal Documents" (Privacy Policy, Consent Forms).

#### 3. How This Impacts Our Product Logic

We are not just building a form builder. We are building a **Compliance Engine**.

**Scenario 1: The "Smart Onboarding"**

* **User:** "I am a **Fintech Startup**."
* **Our Code:** Detects Industry = Finance.
* **Action:** Automatically provisions **SAMA CSF** (Primary) + **NCA ECC** (Secondary) + **PDPL** (Privacy).
* **Value:** The user logs in and sees exactly what they need. No configuration required.

**Scenario 2: The "Kill the Excel" Feature**

* **User:** Uploads a "Password Policy PDF" for **NCA Control 2-9**.
* **Our Code:**
  1. Checks nca\_controls table -> Marks as **Done**.
  2. Checks mapping\_table -> Finds that SAMA Control 3.1 *also* needs a password policy.
  3. Auto-fills SAMA Control 3.1.
* **Value:** "Upload Once, Comply Everywhere." (This is our killer feature).

#### 4. Why is this technically difficult? (The Challenge)

* **Structure:** NCA uses Domain > Sub-Domain > Control. SAMA uses Domain > Principle > Control. We need a **flexible database schema** that can handle both trees.
* **Language:** The data is bilingual. Our database must store text\_en (English) and text\_ar (Arabic) for every single parameter.

#### 5. Summary for the Team

* **NCA** = The Baseline (Everyone).
* **SAMA** = The Bank Boss (Strict).
* **ECC / CSF** = The names of the PDF files (The Standards).
* **Our Job:** Take these static PDF rules and turn them into a dynamic, "Red/Green" dashboard.

### Suggestion for You (The Founder)

When you present this:

1. **Show the PDFs:** Open the NCA PDF and show them the table on Page 20. Say *"This text goes in our Database."*
2. **Show the "Overlap":** Show the SAMA PDF and point out a similar control. Say *"Our AI connects these two dots."*
3. **End with the Vision:** *"We are building the first tool that understands 'Saudi Context' out of the box."*