**1️⃣ FedRAMP (Federal Risk and Authorization Management Program)**

**Purpose**

* Standardized approach for **security assessment, authorization, and continuous monitoring** for cloud services used by U.S. federal agencies.
* Based on **NIST SP 800-53** controls.

**Applicability**

* Applies to **Cloud Service Providers (CSPs)** wanting to sell to U.S. federal agencies.
* Ensures CSPs meet federal data security requirements before use.

**Key Concepts**

| **Term** | **Meaning** |
| --- | --- |
| **JAB** | Joint Authorization Board (DOD, DHS, GSA) – issues Provisional ATO (P-ATO) |
| **ATO** | Authority to Operate – formal approval to use a system |
| **P-ATO** | Provisional ATO issued by JAB, agencies can leverage |
| **Impact Levels** | Low, Moderate, High – based on FIPS 199 data categorization |
| **3PAO** | Third Party Assessment Organization – conducts independent security assessment |

**Process**

1. **Initiation** – Choose authorization path: JAB or agency sponsorship.
2. **Preparation** – Implement NIST 800-53 controls, prepare documentation (SSP, POA&M, etc.).
3. **Assessment** – 3PAO tests security controls.
4. **Authorization** – Agency or JAB grants ATO.
5. **Continuous Monitoring** – Monthly scans, annual reassessment.

**Interview Points**

* Difference between **JAB vs Agency ATO**
* FedRAMP’s basis on **NIST 800-53 Rev 5**
* Continuous monitoring requirements

**2️⃣ FISMA (Federal Information Security Modernization Act)**

**Purpose**

* U.S. federal law requiring federal agencies (and contractors handling federal data) to implement **information security programs**.
* Enforced by OMB (Office of Management and Budget) & DHS.

**Applicability**

* Federal agencies
* State/local agencies handling federal programs
* Contractors/vendors managing federal information

**Key Requirements**

* Maintain **agency-wide security program**
* Perform **annual risk assessments**
* Use **NIST RMF** for risk management
* Classify systems via **FIPS 199** (Low, Moderate, High)
* Select controls via **FIPS 200** & **NIST 800-53**
* Conduct **annual independent security review**
* Report to OMB/DHS

**Interview Points**

* Relationship: **FISMA → NIST RMF → NIST 800-53**
* Federal data classification levels
* Annual reporting obligations

**3️⃣ NERC CIP (North American Electric Reliability Corporation – Critical Infrastructure Protection)**

**Purpose**

* Security standards for **Bulk Electric System (BES)** in North America.
* Protects power grid from physical & cyber threats.

**Applicability**

* Power generation, transmission, distribution entities meeting **BES criteria**.

**Key Standards (CIP-002 to CIP-014)**

| **CIP Standard** | **Scope** |
| --- | --- |
| **CIP-002** | Asset identification & categorization |
| **CIP-003** | Security management controls |
| **CIP-004** | Personnel & training |
| **CIP-005** | Electronic security perimeters |
| **CIP-006** | Physical security of BES cyber systems |
| **CIP-007** | System security management |
| **CIP-008** | Incident reporting & response |
| **CIP-009** | Recovery plans for BES cyber systems |
| **CIP-010** | Configuration change management |
| **CIP-011** | Information protection |
| **CIP-013** | Supply chain risk management |
| **CIP-014** | Physical security of critical transmission stations |

**Interview Points**

* The link between **CIP standards & NERC enforcement**
* Incident reporting requirements
* Supply chain risk management in CIP-013

**Implementation vs Audit View Across All 3**

**Implementation**

* FedRAMP: Build NIST 800-53 control baseline, prepare SSP, manage POA&M.
* FISMA: Implement risk-based security program, continuous monitoring.
* NERC CIP: Implement physical & cyber protection for BES systems, train staff.

**Audit**

* FedRAMP: Review 3PAO reports, verify continuous monitoring evidence.
* FISMA: Check risk assessments, test selected controls, verify annual reviews.
* NERC CIP: Review compliance evidence for each CIP standard, test incident response drills.