FISMA

System Security Plan (SSP)

- System Description & Boundary
- Security Categorization
- Implemented Controls
- Interconnections & Interfaces
- POA&M (Plan of Action & Milestones)

Overview & Purpose

- Enacted 2002, Modernized 2014
- Protect Federal Information Systems
- Applies to Federal Agencies & Contractors
- OMB Oversight & Reporting
- DHS Operational Coordination

Key Supporting Frameworks & Tools

- CDM Program (Continuous Diagnostics & Mitigation)
- FedRAMP (Cloud Services)
- SCAP (Security Content Automation Protocol)
- NIST CSF (Cybersecurity Framework)
- OSCAL (Open Security Controls Assessment)

Key Roles & Responsibilities

- Agency Head (Secretary / Director)
- Chief Information Officer (CIO)
- Senior Agency Information Security Officer (SAISO)
- Inspector General (IG)
- System Owner
- Authorizing Official (AO)

Reporting & Compliance

- Annual FISMA Reports to OMB
- CyberScope / CDM Dashboard
- Inspector General Independent Reviews
- Incident Reporting to US-CERT / CISA
- Congressional Reporting

NIST RMF (Risk Management Framework)

- Step 1: Prepare
  - Establish context & priorities
  - Identify roles & resources
- Step 2: Categorize
  - FIPS 199 impact levels (L/M/H)
  - Confidentiality, Integrity, Availability
- Step 3: Select
  - NIST SP 800-53 Control Baselines
  - Tailor controls to system needs
- Step 4: Implement
  - Apply selected security controls
  - Document implementation
- Step 5: Assess
  - NIST SP 800-53A Assessment Procedures
  - Independent Assessor (3PAO)
- Step 6: Authorize
  - Authorization to Operate (ATO)
  - Plan of Action & Milestones (POA&M)
- Step 7: Monitor
  - Continuous Monitoring (ConMon)
  - Ongoing Authorization

Authorization Types

- ATO (Authorization to Operate)
- IATO (Interim ATO)
- DATO (Denial of ATO)
- Ongoing Authorization (OA)
- Common Control Authorization

Impact Levels

- High Impact
  - Severe / catastrophic effect
  - ~420+ controls (critical systems)
- Low Impact
  - Limited adverse effect
  - ~125 controls (SP 800-53)
- Moderate Impact
  - Serious adverse effect
  - ~325 controls (most systems)

FIPS Standards

- FIPS 140-2/3 Cryptographic Modules
- FIPS 199 Security Categorization
- FIPS 201 Personal Identity Verification (PIV)
- FIPS 200 Minimum Security Requirements

NIST SP 800-53 Control Families

- AC – Access Control
- AU – Audit & Accountability
- CA – Assessment, Authorization & Monitoring
- CM – Configuration Management
- CP – Contingency Planning
- IA – Identification & Authentication
- IR – Incident Response
- RA – Risk Assessment
- SA – System & Services Acquisition
- SC – System & Comms Protection
- SI – System & Info Integrity
- SR – Supply Chain Risk Management

www.hackingarticles.in

@hackinarticles
https://github.com/Ignitetechnologies
https://in.linkedin.com/company/hackingarticles