F

FORGE

CYBER DEFENSE

FISMA Readiness Checklist

This checklist covers the key requirements for FISMA compliance using the NIST Risk Management Framework (RMF). Use this to assess your federal information system's security posture.

SYSTEM INFORMATION

System Name: _____

System Owner: _____

ISSO: _____

FIPS 199 Impact Level: ☐ Low ☐ Moderate ☐ High

STEP 1: CATEGORIZE INFORMATION SYSTEM

- ☐ Identify information types processed, stored, or transmitted
- ☐ Determine impact levels (confidentiality, integrity, availability)
- ☐ Complete FIPS 199 Security Categorization
- ☐ Document system boundary
- ☐ Obtain AO approval of categorization

STEP 2: SELECT SECURITY CONTROLS

- ☐ Identify baseline controls from NIST 800-53 (based on impact level)
- ☐ Apply tailoring guidance
- ☐ Document control selection rationale
- ☐ Identify common controls (inherited from organization)
- ☐ Develop continuous monitoring strategy

STEP 3: IMPLEMENT SECURITY CONTROLS

- ☐ Implement selected security controls
- ☐ Document implementation in System Security Plan (SSP)
- ☐ Update system architecture documentation
- ☐ Configure systems according to security requirements

F FORGE
CYBER DEFENSE

FISMA Readiness Checklist

STEP 4: ASSESS SECURITY CONTROLS

- [ ] Develop Security Assessment Plan (SAP)
- [ ] Select or engage independent assessor
- [ ] Conduct security control assessment
- [ ] Document findings in Security Assessment Report (SAR)
- [ ] Conduct vulnerability scanning
- [ ] Perform penetration testing (as required)

STEP 5: AUTHORIZE INFORMATION SYSTEM

- [ ] Prepare authorization package (SSP, SAR, POA&M)
- [ ] Conduct risk determination
- [ ] Submit package to Authorizing Official (AO)
- [ ] Obtain Authorization to Operate (ATO)
- [ ] Document authorization decision

STEP 6: MONITOR SECURITY CONTROLS

- [ ] Implement continuous monitoring program
- [ ] Conduct ongoing security control assessments
- [ ] Perform monthly vulnerability scanning
- [ ] Maintain and update POA&M
- [ ] Report security status to AO
- [ ] Manage configuration changes
- [ ] Conduct annual security reviews

REQUIRED DOCUMENTATION

- [ ] System Security Plan (SSP)
- [ ] Security Assessment Plan (SAP)
- [ ] Security Assessment Report (SAR)
- [ ] Plan of Action and Milestones (POA&M)
- [ ] Authorization Decision Letter
- [ ] Contingency Plan
- [ ] Incident Response Plan
- [ ] Configuration Management Plan