FISMA Audit Checklist

*This checklist is provided for informational purposes only and does not constitute legal advice or a comprehensive FISMA compliance solution.

gart.

gartsolutions.com

info@gartsolutions.com

1. Inventory of Information Systems

□ Identify all information systems used in your organization.

□ Document system boundaries and components (e.g., hardware, software, networks, databases).

□ Assign security categorizations for each system according to FIPS 199 (Low, Moderate, High impact).

2. System Security Plan (SSP)

□ Develop and maintain an SSP for each system, detailing:

- System architecture and design.
- Security controls in place.
- Roles and responsibilities.
- Interconnections and dependencies with other systems.

□ Ensure the SSP is updated regularly to reflect system changes or evolving threats.

3. Risk Assessment

□ Conduct a formal risk assessment for each system:

- Identify threats and vulnerabilities.
- Assess potential impact on confidentiality, integrity, and availability.
- Calculate the likelihood of threat events.

□ Document risk assessment results and recommend mitigation strategies.

4. Security Controls Selection

□ Use NIST SP 800-53 to select security controls based on the system's categorization (Low, Moderate, High).

□ Ensure that baseline security controls are tailored to your environment.

□ Document compensating controls if standard controls cannot be implemented.

5. Implementation of Security Controls

□ Ensure that all security controls are implemented and operating as intended, including:

- Access control mechanisms (e.g., least privilege, role-based access).
- Audit logs for monitoring system events.
- Encryption for data at rest and in transit.
- Continuous monitoring tools to detect incidents and vulnerabilities.
- Physical security controls for sensitive systems and data.

□ Keep a record of security patches and updates applied to software and systems.

6. Access Control

□ Review user access levels to ensure they are consistent with job responsibilities (least privilege principle).

□ Implement multi-factor authentication (MFA) where applicable.

□ Ensure that user accounts are disabled immediately when no longer needed (e.g., employee termination).

□ Conduct periodic access reviews to verify that only authorized personnel have access.

7. System Authorization

□ Ensure that each system has an Authority to Operate (ATO) granted by a senior official after the system’s security posture is assessed.

□ The ATO should be renewed periodically or after significant system changes.

□ Prepare an Authorization Package for each system, including the SSP, risk assessment, and security control assessment.

8. Security Awareness Training

□ Implement a security awareness and training program for all employees and contractors:

- Train users on cybersecurity best practices and phishing.
- Conduct regular training sessions for staff based on their access levels.
- Maintain records of completed training.

9. Incident Response Plan (IRP)

□ Develop and maintain an Incident Response Plan that includes:

- Procedures for detecting, responding to, and recovering from security incidents.
- Designation of an incident response team with clear roles.
- Incident reporting mechanisms (internal and external) and timelines.
- Procedures for preserving evidence and conducting post-incident reviews.

□ Test the incident response plan periodically through simulated exercises.

10. Continuous Monitoring

□ Implement a continuous monitoring strategy to maintain awareness of security controls and system vulnerabilities:

- Deploy automated tools for monitoring network traffic, system logs, and security alerts.
- Conduct vulnerability scans and penetration testing regularly.
- Monitor compliance with security controls and identify deviations.

11. Contingency Planning

□ Develop a Contingency Plan to ensure continuity of operations in case of an incident:

- Define recovery objectives (Recovery Time Objective - RTO and Recovery Point Objective - RPO).
- Identify critical systems and data that must be restored first.
- Implement and regularly test backup and recovery procedures.
- Document the roles and responsibilities during recovery efforts.
- Conduct tabletop exercises and simulations to test the plan.

12. Data Protection

□ Implement encryption for sensitive data:

- Encrypt data at rest and in transit using FIPS-validated algorithms.
- Use key management practices to protect encryption keys.

□ Ensure the proper classification of data and apply protections based on data sensitivity.

13. Configuration Management

□ Establish a configuration management process to track system changes:

- Document and track all software and hardware configurations.
- Use a change control board to approve system changes.
- Conduct regular audits of configurations to ensure consistency.

□ Implement baseline configurations and ensure deviations are authorized.

14. Audit Logging

□ Enable audit logging for critical system events, including:

- Access attempts (both successful and unsuccessful).
- Changes to system configurations.
- System administrator activities.

□ Retain logs in a secure location for a period required by regulations.

□ Implement tools to review and analyze logs regularly for anomalies.

15. System Maintenance

- □ Document and track all system maintenance activities.
- □ Ensure that maintenance personnel are vetted and authorized to perform activities.
- □ Secure and monitor remote maintenance connections (e.g., use encryption, multifactor authentication).
- □ Ensure that any maintenance tools do not introduce security vulnerabilities.

16. Privacy Impact Assessment (PIA)

□ Conduct a Privacy Impact Assessment (PIA) if the system processes Personally Identifiable Information (PII).

□ Document the methods used to protect PII and the consequences of data breaches.

□ Implement controls for the use, storage, and disposal of PII.

17. Security Control Assessment (SCA)

□ Conduct a formal Security Control Assessment to ensure that all security controls are effectively implemented.

Use independent assessors to evaluate the controls.

□ Produce a Plan of Action and Milestones (POA&M) for any security weaknesses identified.

□ Document assessment findings and submit them for review.

18. Third-Party Vendors

- □ Ensure that third-party vendors comply with FISMA security standards.
- □ Review and validate security controls implemented by third-party service providers.
- □ Include security requirements in all vendor contracts.

19. Documentation and Reporting

- □ Maintain comprehensive documentation of all security practices, assessments, and mitigation efforts.
- □ Prepare and submit FISMA compliance reports to the appropriate federal oversight bodies.
- □ Regularly update documentation (e.g., SSPs, risk assessments, IRPs) to reflect changes in system or threats.

20. Program Management

□ Establish a program management plan to ensure continuous FISMA compliance:

- Assign a Chief Information Security Officer (CISO) to oversee the security program.
- Regularly review and update the organization's security policies.
- Conduct annual reviews of the security program and identify improvements.
- Monitor emerging threats and update security practices accordingly.

Simplify FISMA Compliance with Gart Solutions

Gart Solutions makes FISMA compliance easy by specializing in DevOps and cloud services to protect sensitive government data.

- Risk Assessment: We evaluate your systems to meet FISMA security standards.
- Security Controls: We implement NIST-based controls to safeguard your data.
- Automated Monitoring: Continuous compliance tracking reduces manual oversight.
- Ongoing Support: We provide training and resources to keep your team FISMA-ready.

Secure your government data with Gart Solutions. Contact us today!

gart.

gartsolutions.com

info@gartsolutions.com