NIST 800-53 Compliance Checklist

This checklist provides a comprehensive guide to help organizations meet the NIST 800-53 security framework standards. It includes preparatory steps, key control areas, detailed compliance actions, and ongoing compliance management. Use the checkboxes to track progress and add notes to document any relevant information during the compliance process.

Overview:

- Preparation for compliance, including gap analysis and workforce training.
- Key control areas such as access control, audit, incident response, and risk assessment.
- Detailed actions for securing systems and managing security configurations.
- Ongoing compliance management to ensure continuous adherence to NIST 800-53 standards.

Step	Description	Actions	Check	Notes
Preparation for NIST 800-53 Compliance				
Conduct a Gap Analysis	Assess current security practices vs. NIST 800-53 requirements.	Perform a thorough gap analysis to understand where current security falls short.		
Understand the Context	Classify information and apply controls based on sensitivity and criticality.	Segment systems and apply relevant controls based on the classification of data.		
Build Cross-Functional Teams	Involve key stakeholders from IT, security, compliance, and business operations.	Create a cross-functional team to handle compliance from multiple perspectives.		
Educate Your Workforce	Train employees on the importance of NIST 800-53 compliance.	Develop a training program and conduct role-based security training.		
Key Control Areas for Compliance				
Access Control	Restrict access to systems and data using least privilege and strong authentication.	Implement least privilege access and multi factor authentication (MFA).		
Awareness and Training	Regular security training for all personnel.	Conduct ongoing training, including specialized training for roles with security responsibilities.		

Audit and Accountability	Implement logging and monitoring mechanisms.	Centralize logs, protect them from tampering, and regularly review audit logs for anomalies.		
Security Assessment and Authorization	Regular assessments of security controls and system authorization.	Perform security assessments and maintain updated authorization packages for systems.		
Configuration Management	Maintain secure configurations for all systems and software.	Create baseline configurations and monitor for deviations.		
Contingency Planning	Develop and test disaster recovery plans.	Establish and regularly test contingency and recovery plans.		
Identification and Authentication	Implement strong user identification and authentication methods.	Use MFA and update authentication methods periodically.		
Incident Response	Create and practice an incident response plan.	Develop a formal plan with assigned roles and conduct regular incident response drills.		
Risk Assessment	Identify and assess risks to organizational operations.	Perform qualitative and quantitative risk assessments regularly.		
System and Services Acquisition	Ensure security is included in the procurement process.	Integrate security into contracts and evaluate vendors' security practices.		
System and Communications Protection	Protect data in transit and at rest with encryption and firewalls.	Use encryption, segment networks, and monitor communications at internal and external boundaries.		
System and Information Integrity	Protect systems and data from malware and unauthorized access.	Use anti-malware solutions and timely patching of vulnerabilities.		
Detailed Actions for Compliance				
Access Control	Manage user accounts and permissions.	Regularly review and update user accounts, enforce session lock and failed login attempt thresholds.		

Awareness and Training	Develop tailored security training for different roles.	Maintain training records for compliance audits and continuous improvement.		
Audit and Accountability	Centralize logs and protect them from unauthorized access.	Review audit logs regularly for signs of unauthorized activity or anomalies.		
Security Assessment and Authorization	Schedule regular security control assessments.	Document system security assessments and keep the authorization package updated.		
Configuration Management	Implement baseline configurations and respond to deviations.	Respond promptly to any detected deviations in configuration.		
Contingency Planning	Conduct regular contingency plan tests.	Run drills and simulations to ensure recovery plans are actionable and effective.		
Identification and Authentication	Regularly update user authentication methods.	Implement multi factor authentication wherever feasible.		
Incident Response	Assign and train incident response roles.	Ensure team members are trained and prepared for incident response situations.		
Risk Assessment	Assess and document potential threats and vulnerabilities.	Use both qualitative and quantitative methods to assess risks and prioritize corrective actions.		
System and Services Acquisition	Evaluate vendor security practices.	Include security requirements in all procurement processes and regularly audit third-party compliance.		
System and Communications Protection	Secure communication channels with encryption and firewalls.	Monitor and control external and internal communications to prevent unauthorized access.		
System and Information Integrity	Implement anti-malware and timely patching of systems.	Ensure systems are updated with the latest security patches and protected from malware.		

Ongoing Compliance Management				
Continuous Monitoring	Monitor security controls and system activities in real time.	Implement monitoring tools for real-time compliance checks and incident detection.		
Regular Risk Assessments	Reassess risks periodically to ensure controls remain effective.	Conduct regular risk assessments and update controls to address new threats.		
Revisiting and Updating Policies	Update security policies, procedures, and training regularly.	Regularly review and update policies based on incident outcomes or audit findings.		
Ongoing Education and Training	Keep staff informed of new threats and compliance requirements.	Maintain a schedule for updating training programs as threats and compliance standards evolve.		
Engagement with the Compliance Community	Participate in forums, workshops, and industry groups.	Stay informed about best practices, industry challenges, and updates in the compliance landscape.		