NIST SP 800-53 Checklist

There are 19 NIST security control families, which are broken into three classes based on impact (Low, Moderate, and High). Organizations can select the controls that are most applicable to their requirements and impact level.

Cyvatar will assist you in addressing all applicable controls and getting you ready for your NIST 800-53 audit.

Let's take a look at the NIST 800-53 security controls:

1. **Access Control**

Ensure the least privilege, separation of duties for access management, and continuous monitoring.

2. **Awareness and Training**

Ensure technical and user training on threats and access.

3. **Assessment, Authorization, and Monitoring**

Complete regular penetration testing and review of connections to external and public systems.

4. **Configuration Management**

Identify and define configuration change control and software policies.

5. **Contingency Planning**

Review, document, and test business continuity strategies and alternate processing or storage sites.

6. **Identification and Authentication**

Ensure effective credential management and authentication policies for users, devices, and services.

7. **Individual Participation**

Review consent and privacy authorization processes.

8. **Incident Response**

Develop, document, and communicate how security incidents will be managed and reported.

9. **Maintenance**

Ensure regular personnel, system, and tool maintenance.

10. **Media Protection**

Enforce secure access, storage, transmission, and sanitization of media.

11. **Privacy Authorization**

Protect the collection, use, and sharing of personally identifiable information.

12. **Physical and Environment Protection**

Ensure secure physical access, temperature control, fire protection, and emergency power.

13. **Planning**

Identify and define the security architecture and network restrictions.

14**. Program Management**

Develop, test, review, and maintain a risk management strategy, security architecture, and insider threat program.

15. **Personnel Security**

Ensure personnel screening and training. Monitoring personnel terminations, transfers, and sanctions.

16. **Risk Assessment**

Complete regular risk assessments, vulnerability assessments, and privacy impact assessments.

17. **System and Services Acquisition**

Ensure the security of your system development life cycle, acquisition process, and supply chain risk management.

18. **System and Communications Protection**

Ensure application segmentation, boundary protection, and cryptographic key management.

19. **System and Information Integrity**

Ensure ongoing system monitoring, alerting, and remediation.

ABOUT CYVATAR.AI

Cyvatar is leading the future of cybersecurity by making it accessible, achievable, and easy for startups and SMBs. By bringing the subscription economy to the world of cybersecurity, we've created a whole new membership-based experience to create an all-inclusive, seamless, and transparent operating system for cybersecurity.

530 Technology Drive,
Suite 100 Irvine,
California 92618 USA
getoutcomes@cyvatar.ai