NIST Special Publication 800-53 covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with the security requirements in Federal Information Processing Standard (FIPS) 200. This includes selecting an initial set of baseline security controls based on a FIPS 199 worst-case impact analysis, tailoring the baseline security controls, and supplementing the security controls based on an organizational assessment of risk.

This tip sheet will break it down into 6 easy steps for compliance as well as recommended courses under each of the 5 NIST Cybersecurity Frameworks.

1. Categorize Information System
Assign a Security role to the IT system based on mission and business objectives. This role must be consistent with the organization’s risk management strategy. Guide and inform risk management processes and tasks by determining impact or consequences to the organization with respect to the compromise or loss of assets including the confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems.

2. Select Security Controls
Select Security Controls approved by leadership from the control catalogue contained in NIST SP 800-53. Security controls are hardware, software, and technical processes required to fulfill the minimum assurance requirements as stated in the risk assessment. Identify, select, tailor, and document the security and privacy controls necessary to protect the system and the organization commensurate with the risk to organizational operations and assets, individuals, and other organizations.
3. **Implement Security Controls**
   Implement Security controls while documenting and proving that you've achieved minimum assurance requirements and demonstrated correct use of information system and security engineering methodologies.

4. **Assess Security Controls**
   Assess security controls using appropriate methods and procedures to determine the extent to which controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. If necessary, address and remediate weaknesses or deficiencies found and then document security plan accordingly.

5. **Authorize Information System**
   Determine risk to organizational operations, organizational assets, or to individual resulting from the operation of the system and the decision that a risk is acceptable. Present authorization package for risk assessment and risk determination and submit decision to all necessary parties.

6. **Monitor Security Controls**
   Monitor existent security controls and update based on changes to system or environment. Report security status of the system and remediate any weaknesses. Maintain an ongoing situational awareness about the security and privacy posture of the system and the organization in support of risk management decisions.

---

**Recommended Courses**

**IDENTIFY**
- Essential Identification and Authentication
- Essential Security Planning Policy and Procedures
- Essential Risk Assessment
- Essential Configuration Management
- Essential System and Information Integrity
- Essential Personnel Security Policy and Procedures

**PROTECT**
- Essential Account Management Security
- Essential Session Management Security
- Essential Configuration Management
- Essential Identification and Authentication
- Essential Access Control for Mobile Devices
- Essential Data Protection
- Essential Application Protection
- Essential Security Engineering Principles
- Essential Media Protection
- Essential System and Information Integrity
- Essential Security Maintenance Policies

**DETECT**
- Essential Risk Assessment
- Essential System and Information Integrity
- Essential Audit and Accountability
- Essential Security Engineering Principles
- Essential System and Information Integrity

**RESPOND**
- Essential Incident Response
- Essential Security Assessment and Authorization

**RECOVER**
- Essential Information Security Program Planning
- Essential Incident Response
- Essential Security Audit and Accountability