1. Access Control
- Limit information system access to authorized users
- Separate the duties of individuals to reduce the risk of malevolent collusion
- Limit unsuccessful login attempts
- Require encryption and authentication of various devices (including mobile devices), and route remote access through managed access control points

2. Awareness and Training
- Educate managers, systems administrators, and users about security risks associated with their activities and applicable policies, standards and procedures
- Provide security awareness training on recognizing and reporting potential indicators of insider threat

3. Audit and Accountability
- Use automated mechanisms to integrate and correlate audit and reporting processes
- Support on-demand analysis and reporting

4. Configuration Management
- Limit the types of programs users can install
- Control and monitor all user-installed software

5. Identification and Authentication
- Prevent reuse of identifiers for a defined period
- Disable identifiers after a defined period of inactivity
- Enforce minimum password complexity, i.e., “smart passwords”

6. Incident Response
- Develop and test an incident response plan

7. Maintenance
- Ensure equipment removed off-site is sanitized of any CUI
- Require multi-factor authentication to establish nonlocal maintenance sessions
NIST Risk Assessment Checklist

8. Media Protection
☐ Protect (i.e., physically control and securely store) information system media (paper and digital) containing CUI
☐ Sanitize or destroy information system media containing CUI before disposal or release or reuse

9. Personnel Security
☐ Screen individuals prior to authorizing access to systems containing CUI

10. Physical Protection
☐ Maintain audit logs of physical access
☐ Control and manage physical access devices

11. Risk Assessment
☐ Scan for and remediate vulnerabilities in the information system and applications

12. Security Assessment
☐ Periodically assess and monitor security controls for effectiveness in their applications
☐ Develop and implement plans of action designed to correct deficiencies and reduce/eliminate vulnerabilities

13. System and Communications Protection
☐ Separate user functionality from information system management functionality
☐ Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission
☐ Control and monitor the use of Voice over Internet Protocol technologies

14. System and Information Integrity
☐ Update malicious code protection mechanisms when new releases are available
☐ Identify unauthorized use of the information system