NIST ASSESSMENTS
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

CONTACT US FOR MORE INFO
WWW.MEGAPLANIT.COM
NIST SP 800-53

NIST Special Publication 800-53 recommends the standards used by federal agencies, except those designed for national security, to implement the Federal Information Security Management Act (FISMA). It covers the Risk Management Framework steps that address security control selection for information systems in accordance with the security requirements in the Federal Information Processing Standard (FIPS) 200. With the increased threats found in today's climate, many private sector companies are finding that NIST SP 800-53 guidance provides greater assurance and peace of mind for securing their environment.

Our Approach:

Our expert assessors partner with your team to ensure your systems are sufficient to maintain the integrity, confidentiality, and security of your critical and sensitive information. Receive trusted advisory support throughout the process, as well as guidance on how to address any weaknesses in your environment.

Control Families:

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Personnel Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit and Accountability</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Planning</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Program Management</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Incident Response</td>
<td>Security Assessment and Authorization</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Media Protection</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>Physical Protection</td>
<td>System and Services Acquisition</td>
</tr>
</tbody>
</table>
NIST SP 800-171

Initially published in June 2015, NIST Special Publication 800-171 is a set of standards that define how to safeguard and distribute material deemed sensitive but not classified, otherwise referred to as Controlled Unclassified Information (CUI).

Both the CUI designation and the NIST SP 800-171 framework are intended to standardize and replace previous designations and frameworks. For companies doing business with the Federal Government, adherence to this standard is mandatory if any data will be transmitted to, stored on, or processed by your information systems.

Our Approach:

We partner with your team to ensure your systems are sufficient to protect the confidentiality of CUI both at rest and in transit. Receive trusted advisory support throughout the process, as well as guidance on how to address any weaknesses in your processes and systems.

Control Families:

- **Access Control**
- **Audit and Accountability**
- **Awareness and Training**
- **Configuration Management**
- **Identification and Authentication**
- **Incident Response**
- **Maintenance**

- **Media Protection**
- **Physical Protection**
- **Personnel Security**
- **Risk Assessment**
- **Security Assessment**
- **System and Information Integrity**
- **System and Communications Protection**
NIST Cybersecurity Framework Assessment

The NIST Cybersecurity Framework (CSF) was originally published in 2014, following a collaborative process involving industry, academia, and government agencies, as directed by presidential executive order. It is a set of optional standards, best practices, and recommendations for improving cybersecurity at the organizational level.

Our Approach:

Our security and compliance experts will partner with your team to assess your organization’s security program against the NIST CSF framework. We start with a current state analysis of your risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business objectives, supply chain cybersecurity requirements, and organizational constraints. Once the current state is defined, our experts work with you to define your desired state goals; these are defined as Framework Implementation Tiers. Our step-by-step process will identify any weaknesses that need to be addressed for you to meet your desired Implementation Tier, and our team provides thorough recommendations and guidance on how to bring your program in line with NIST CSF guidelines.

Framework Core Functions and Categories

**Detect (DE)**
- DE.AE – Anomalies and Events
- DE.CM – Security Continuous Monitoring
- DE.DP – Detection Processes

**Respond (RS)**
- RS.RP – Response Planning
- RS.CO – Communications
- RS.AN – Analysis
- RS.MI – Mitigation
- RC.IM – Improvements

**Protect (PR)**
- PR.AC – Identity Management and Access Control
- PR.AT – Awareness and Training
- PR.DS – Data Security
- PR.IP – Information Protection Processes and Procedures
- PR.MA – Maintenance
- PR.PT – Protective Technology

**Recover (RC)**
- RC.RP – Recovery Planning
- RC.CO – Communications
Risk Heat Map

A fundamental aspect of every NIST assessment is the Risk Analysis. This is the process of identifying risks to system security, determining the likelihood of occurrence and resulting impact, and identifying any additional safeguards needed to mitigate the impact. When conducting any NIST assessment, the MegaplanIT security consultant will identify gaps that represent risks to your organization. Those risks are mapped against the likelihood of occurrence and impact to your organization if they were to transpire. The resulting heat map can help identify control failures, prioritize mitigation efforts, and be used with executive management to obtain buy-in for your remediation efforts.

### Category Summary

<table>
<thead>
<tr>
<th>ID</th>
<th>ID Description</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP</td>
<td>Response Planning</td>
<td>H</td>
</tr>
<tr>
<td>AC</td>
<td>Access Control</td>
<td>H</td>
</tr>
<tr>
<td>PT</td>
<td>Protective Technology</td>
<td>H</td>
</tr>
<tr>
<td>AM</td>
<td>Asset Management</td>
<td>H</td>
</tr>
<tr>
<td>AN</td>
<td>Analysis</td>
<td>H</td>
</tr>
<tr>
<td>RA</td>
<td>Risk Assessment</td>
<td>H</td>
</tr>
<tr>
<td>BE</td>
<td>Business Environment</td>
<td>H</td>
</tr>
<tr>
<td>DS</td>
<td>Data Security</td>
<td>H</td>
</tr>
<tr>
<td>GV</td>
<td>Governance</td>
<td>H</td>
</tr>
<tr>
<td>MI</td>
<td>Mitigation</td>
<td>H</td>
</tr>
<tr>
<td>CO</td>
<td>Communications</td>
<td>H</td>
</tr>
<tr>
<td>CM</td>
<td>Security Continuous Monitoring</td>
<td>H</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
<td>H</td>
</tr>
<tr>
<td>AE</td>
<td>Anomalies and Events</td>
<td>H</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness Training</td>
<td>H</td>
</tr>
<tr>
<td>DP</td>
<td>Detection Processes</td>
<td>M</td>
</tr>
<tr>
<td>IP</td>
<td>Information Protection Processes</td>
<td>M</td>
</tr>
<tr>
<td>RM</td>
<td>Risk Management</td>
<td>M</td>
</tr>
<tr>
<td>IM</td>
<td>Improvements</td>
<td>L</td>
</tr>
</tbody>
</table>

### Key Benefits

- Build Resilient Information Systems
- Take Control of Cyber Risk
- Final Reports Suitable for Informing Executive Management
- Protect CUI At Rest & In Transit
- Ensure Compliance of Your Information Systems

MEGAPLANIT

1-800-891-1634 | info@megaplanit.com | www.MegaplanIT.com
Building A Holistic Compliance Experience

Our innovative IT security and compliance solutions are designed to deliver customized, cost-effective service on time—because your priorities are our priorities. Here at MegaplanIT, we will assess your unique company and business environment and design a path to security that will fit all of your needs.

Compliance Services
- PCI DSS Assessment
- PA-DSS Assessment
- Self Assessment Questionnaire (SAQ)
- PCI DSS Gap Analysis
- PCI 3DS Assessment
- Point-To-Point Encryption (P2PE)
- NIST SP 800-53 Assessment
- NIST SP 800-171 Assessment
- NIST Cybersecurity
- SSAE 18 SOC Reports
- HIPAA Risk Assessment
- ISO 27001/27002
- Standardized Control Assessment (SCA)
- Gramm-Leach Bliley Act (GLBA)
- Cybersecurity Maturity Model Certification (CMMC)
- California Consumer Privacy Act (CCPA)
- General Data Protection Regulation (GDPR)

Security Testing Services
- Network Penetration Testing
- Web Application Penetration Testing
- Mobile Penetration Testing
- Social Engineering Penetration Testing
- Vulnerability Scanning
- Secure Code Review
- Cloud Security Architecture Review
- Approved Scanning Vendor

LET'S TALK
1-800-891-1634 | info@megaplanit.com | www.MegaplanIT.com