



NIST ASSESSMENTS  
**NATIONAL INSTITUTE  
OF STANDARDS AND  
TECHNOLOGY**

---

CONTACT US FOR MORE INFO  
**[WWW.MEGAPLANIT.COM](http://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:

 Access Control

 Audit and Accountability

 Awareness and Training

 Configuration Management

 Identification and Authentication

 Incident Response

 Maintenance

 Media Protection

 Physical Protection

 Personnel Security

 Physical and Environmental Protection

 Planning

 Program Management

 Risk Assessment

 Security Assessment and Authorization

 System and Communications Protection

 System and Information Integrity

 System and Services Acquisition

# 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

### Identify (ID)

- ID.AM** – Asset Management
- ID.BE** – Business Environment
- ID.GV** – Governance
- ID.RA** – Risk Assessment
- ID.RM** – Risk Management Strategy
- ID.SC** – Supply Chain Risk Management

### 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

### Detect (DE)

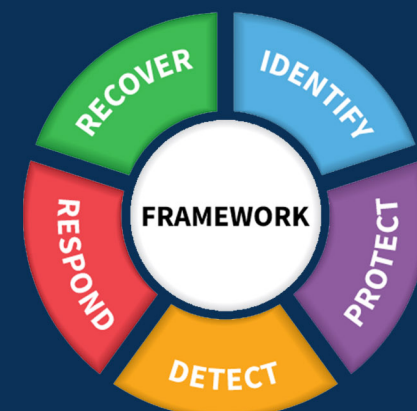
- DE.AE** – Anomalies and Events
- DE.CM** – Security Continuous Monitoring
- DE.DP** – Detection Processes

### Respond (RS)

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

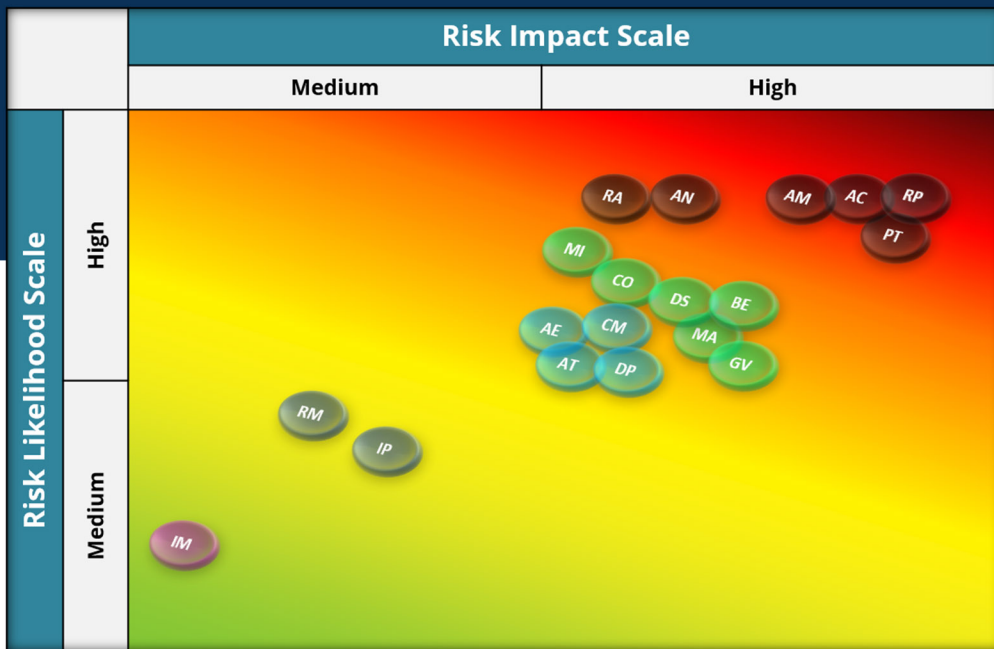
### Recover (RC)

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

## 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**

# 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

