

ManageEngine's guide to implement the NIST Cybersecurity Framework

ManageEngine



Table of content

- The NIST Cybersecurity Framework 04
- The benefits of implementing the NIST Cybersecurity Framework 05
- Components framework 06
- How can ManageEngine help you implement the five functions of the framwork? 10
 - Identify 11
 - Protect 18
 - Detect 26
 - Respond 30
 - Recover 34
- How can you establish or improve a cybersecurity program? 36
- Parting thoughts 37
- About ManageEngine 37

Disclaimer

Copyright © Zoho Corporation Pvt. Ltd. All rights reserved. This material and its contents (“Material”) are intended, among other things, to present a general overview of how you can use ManageEngine’s products and services to implement the NIST Cybersecurity Framework in your organization. Full implementation of the NIST Cybersecurity Framework requires a variety of solutions, processes, people, and technologies.

The solutions mentioned in this Material are some of the ways in which IT management tools can help with some of the NIST Cybersecurity Framework implementation. Coupled with other appropriate solutions, processes, and people, ManageEngine’s solutions help organizations implement the NIST Cybersecurity Framework. This Material is provided for informational purposes only and should not be considered as legal advice for implementing the NIST Cybersecurity Framework.

ManageEngine makes no warranties, express, implied, or statutory, and assumes no responsibility or liability as to the information in this Material. You may not copy, reproduce, distribute, publish, display, perform, modify, create derivative works, transmit, or in any way exploit the Material without ManageEngine’s express written permission.

The ManageEngine logo and all other ManageEngine marks are registered trademarks of Zoho Corporation Pvt. Ltd. Any other names of software products or companies referred to in this Material, and not expressly mentioned herein, are the trademarks of their respective owners. Names and characters used in this Material are either the products of the author’s imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, is purely coincidental.



The NIST Cybersecurity Framework

With the evolving cybersecurity threat landscape, organizations are racing to find and implement effective cybersecurity solutions that help them manage and mitigate security risks preemptively.

The National Institute of Standards and Technology (NIST) developed a framework that could bolster the critical infrastructure of the US, as per the **Cybersecurity Enhancement Act of 2014**.

The framework was originally imagined as a cybersecurity risk management system for the critical infrastructures of the US.

Today, it has been widely implemented in private and public sectors across organizational departments and around the globe. Organizations, regardless of their size and industry, can leverage the best practices outlined in the framework to understand, manage, and mitigate the cybersecurity risks associated with their data and networks.

The NIST Cybersecurity Framework offers guidelines and standards to manage cybersecurity risks across an entire organization or its critical infrastructures. The framework offers organizations a flexible, repeatable, and cost-effective approach towards managing cybersecurity risks on a voluntary basis.

The **benefits** of implementing the NIST Cybersecurity Framework

- **Strengthen cybersecurity posture:**

Organizations can discover their current security posture and prioritize opportunities to strengthen it by taking guidance from the informative references outlined in the framework.

- **Measure organizational risks:**

Assess risks objectively and formulate an action plan considering the budget and resources available to bring risks within tolerance levels.

- **Comply with global standards:**

Comply with other existing global standards and mandates

easily as the framework references multiple standards for its implementation.

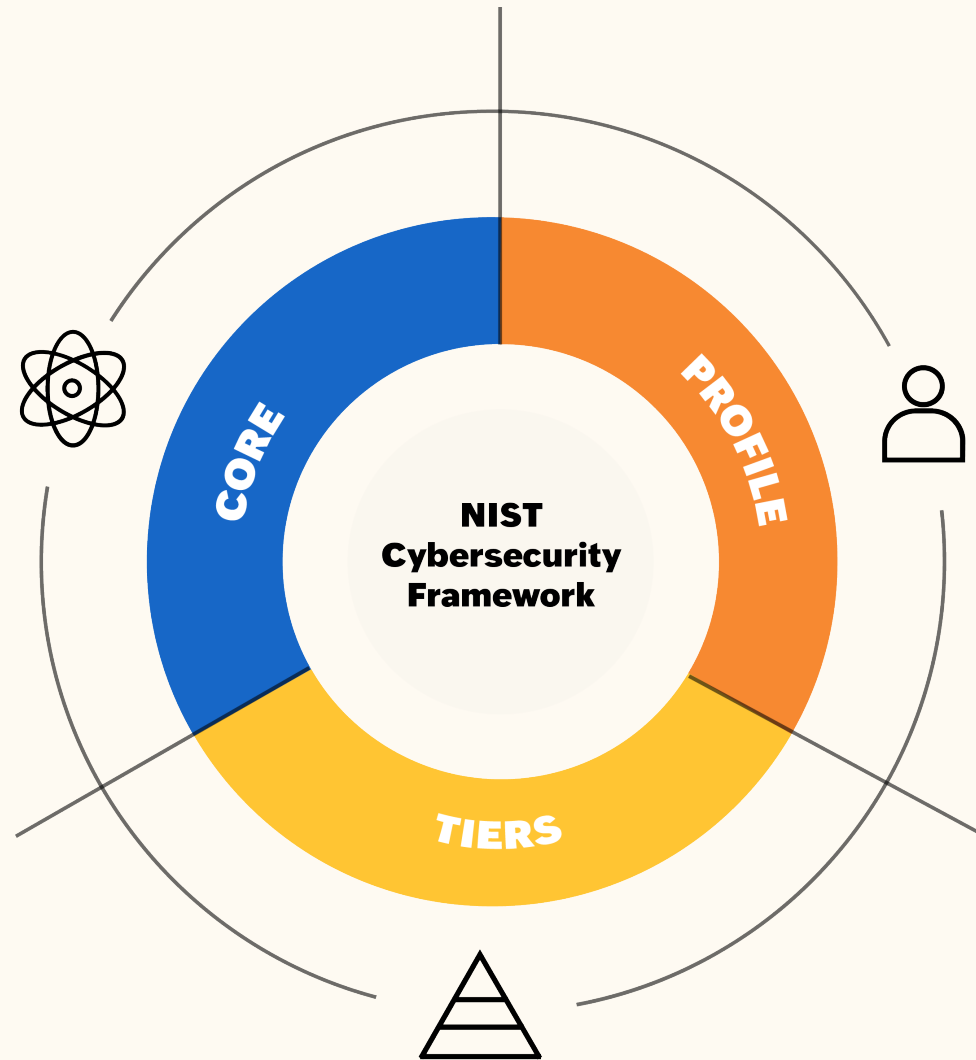
- **Maximize ROI:**

Focus on critical service delivery components to make the implementation process cost-effective by reprioritizing resources.

- **Become risk-informed:**

Transform reactive cybersecurity practices to an agile, risk-informed approach, and continuously adapt to the evolving threat landscape.

Components of the framework



Framework core

The framework core consists of key risk management activities that pave the way for organizations to realize cybersecurity outcomes that align with their business objectives. This outcome-driven approach allows for tailor-made action plans to meet business requirements.

The core comprises five concurrent functions and offers a holistic strategy to understand potential security threats, mitigate their impact, and recover from any business disruptions. It can leverage the best practices outlined in the framework to understand,

Functions are not meant to be a serial path to a desired state but to be performed concurrently and continuously to develop an organizational culture that addresses emerging cybersecurity risks.

- **Identify:** Understand and identify important systems, people, assets, and data and their associated risks to manage cybersecurity.
- **Protect:** Implement appropriate safeguards to protect the critical infrastructure and resources of an organization.
- **Detect:** Monitor systems continuously to discover the occurrence of a cybersecurity incident or anomaly promptly.
- **Respond:** Take actions against a detected cybersecurity attack and limit its impact.
- **Recover:** Ensure business continuity and undertake recovery activities to restore business operations.

Framework

implementation tiers

The implementation tiers illustrate the degree to which an organization's established cybersecurity program reflects the characteristics outlined in the framework. It helps in understanding the scope of cybersecurity practices established to manage risks.

Tier 1: Partial	Tier 2: Risk informed	Tier 3: Repeatable	Tier 4: Adaptive
Irregular, reactive risk management practices with limited awareness of cybersecurity risks.	Some awareness of cybersecurity risks, but limited establishment of a risk management program at an organizational level	A consistent cybersecurity risk management program across an organization with processes to respond based on changes in the threat landscape.	An advanced response system capable of effectively improving its risk management program based on previous incidents and predictive indicators.

Framework profile

The framework profile represents an organization's desired target cybersecurity posture. An organization can develop its profile by selecting all the most important outcomes based on its business goals, risk tolerances, and resources from the categories and subcategories of the framework core.

By creating a current profile and comparing it with the target profile, organizations can identify opportunities to improve their

cybersecurity program. Based on the priority and estimated cost of the corrective efforts, organizations can plan for cybersecurity improvement measures.

Organizations can use the framework profile to communicate the cybersecurity requirements that their partners and external stakeholders, who deliver critical products and services, need to meet in order to keep their supply chain secure.

How can ManageEngine help you implement the **NIST Cybersecurity Framework?**

While the NIST Cybersecurity Framework consists of technical and non-technical controls to manage cybersecurity risks, we can help you implement the technical aspects of it.

Identify:

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

Category	Subcategory	How ManageEngine solutions can help you
<p>Asset Management (ID.AM):</p> <p>The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy</p>	<p>ID.AM-1:</p> <p>Physical devices and systems within the organization are inventoried</p>	<p>Asset Explorer: Discover IP-based devices within the organization with agent-based (Windows, Linux, and macOS) and agentless mechanisms.</p> <p>Endpoint Central: Enroll devices manually or automatically, or have users self-enroll their mobile devices, and then grant corporate network access only to these devices.</p> <p>Network Configuration Manager: Keep track of devices in the network and their device specifics, such as serial numbers, interface details, port configurations, and hardware specifics.</p>
	<p>ID.AM-2:</p> <p>Software platforms and applications within the organization are inventoried</p>	<p>Asset Explorer: Get complete visibility into the software installed in your network, and keep track of purchased software licenses.</p> <p>Endpoint Central: Scan networks periodically to fetch the installed software details.</p>
	<p>ID.AM-3:</p> <p>Organizational communication and data flows are mapped</p>	<p>Asset Explorer: Establish and map data flows between assets, applications, documents, and people with the help of a CMDB.</p> <p>Endpoint Central: Map pending requests, issues, and changes raised to their respective configuration items using a CMDB.</p> <p>DataSecurity Plus: Locate sensitive personal data within files and catalog it.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>ID.AM-4:</p> <p>External information systems are catalogued</p>	<p>DataSecurity Plus: Monitor internal and external cloud applications and gain visibility into the encrypted network traffic of your organization. Catalog and analyze the browsers used to access cloud applications.</p> <p>Cloud Security Plus: Gain visibility into your AWS, Azure, and GCP cloud infrastructure through comprehensive reports and customizable alerts.</p> <p>Log360: Track and monitor the sanctioned and unsanctioned applications in your cloud with an integrated CASB.</p>
	<p>ID.AM-5:</p> <p>Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value</p>	<p>PAM360: Access business-critical resources securely as per assigned privilege level. Classify critical and business-value resources using a CMDB.</p> <p>AD360: Identify user record changes in the HRMS database and automatically modify corresponding user data in Active Directory.</p> <p>Endpoint Central: Configure policy settings on endpoints to restrict user actions and access to applications based on the assigned user privilege, which is based on department or role.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>ID.AM-6:</p> <p>Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established</p>	<p>PAM360: Allow the workforce, third-party stakeholders, and external vendors to access organizational resources securely.</p> <p>Endpoint Central: Map users to customizable roles with a prescribed set of activities and access permissions based on the requirements.</p>
<p>Business Environment (ID.BE):</p> <p>The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>ID.BE-4:</p> <p>Dependencies and critical functions for delivery of critical services are established</p>	<p>Endpoint Central: Map roles and selective privileges to users on Windows, Linux, and Mac devices for effective risk management.</p>
<p>Business Environment (ID.BE):</p> <p>The organization’s mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.</p>	<p>ID.GV-1: :</p> <p>Dependencies and critical functions for delivery of critical services are established</p>	<p>PAM360: Establish strict governance over privileged access pathways to critical assets based on user roles and requirements.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>ID.GV-3</p> <p>Cyber threat intelligence is received from information sharing forums</p>	<p>Log360: Simplify compliance management with audit-ready report templates for PCI DSS, HIPAA, FISMA, CCPA, the GDPR, and more.</p>
<p>Risk Assessment (ID.RA):</p> <p>The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.</p>	<p>ID.RA-1:</p> <p>Dependencies and critical functions for delivery of critical services are established</p>	<p>Vulnerability Manager Plus: Discover, assess, and prioritize vulnerable endpoints in your network.</p> <p>Log360: Discover, analyze, and protect sensitive information stored in your network.</p> <p>Cloud Security Plus: Monitor the log data from AWS, Azure, and GCP cloud infrastructures to identify security threats.</p> <p>M365 Security Plus: Detect and analyze security risks in M365 environments, such as failed logon attempts, file access, role changes, and license modifications.</p>
	<p>ID.RA-2:</p> <p>Cyber threat intelligence is received from information sharing forums</p>	<p>Log360: Leverage STIX, TAXII , and AlienVault OTX format threat feeds to discover malicious IPs, domains, and URLs.</p> <p>Vulnerability Manager Plus: Prioritize threat response based on news feeds with vulnerabilities that attackers are exploiting.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>ID.RA-3:</p> <p>Threats, both internal and external, are identified and documented</p>	<p>Log360: Detect malicious software, services, and processes on endpoints and servers. Mitigate insider threats and account compromise with UEBA. Maintain a tamper-proof log archive to ensure log data from Windows, syslogs, and other applications is secured for future forensic analysis and audits.</p> <p>Vulnerability Manager Plus: Identify all the assets in the network and perform agent-based scans periodically to uncover emerging vulnerabilities, network misconfigurations, high-risk software, active ports, and more.</p> <p>Firewall Analyzer: Analyze firewall security logs to identify network breach attempts and attacks such as a virus, a Trojan, and denial-of-service.</p>
	<p>ID.RA-5:</p> <p>Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>	<p>Log360: Identify the impact of potential risks from rogue users and entities with UEBA and flag the anomalies.</p> <p>Vulnerability Manager Plus: Scan the assets in your networks to identify OS, third-party application, and zero-day vulnerabilities. Understand the impact of the threats through the severity ranking dashboard.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>ID.RA-5:</p> <p>Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</p>	<p>Log360: Identify the impact of potential risks from rogue users and entities with UEBA and flag the anomalies.</p> <p>Vulnerability Manager Plus: Scan the assets in your networks to identify OS, third-party application, and zero-day vulnerabilities. Understand the impact of the threats through the severity ranking dashboard.</p>
	<p>ID.RA-6:</p> <p>Risk responses are identified and prioritized</p>	<p>Log360: Respond to internal and external threats effectively with a set of predefined actions by leveraging automated incident workflows.</p> <p>PAM360: Assign trust scores to users and devices based on their security compliance, and use policy-based access controls to process requests automatically and take custom actions as per organization policies.</p>
<p>Risk Management Strategy (ID.RM)</p> <p>The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.</p>	<p>ID.RM-1:</p> <p>Risk management processes are established, managed, and agreed to by organizational stakeholders</p>	<p>DataSecurity Plus: Discover sensitive data and classify it based on sensitivity to ensure protection and compliance.</p> <p>PAM360: Identify suspicious privileged activity by leveraging AI- and ML-driven capabilities, and terminate malicious behavior.</p>

Protect:

Develop and implement appropriate safeguards to ensure delivery of critical services.

Category	Subcategory	How ManageEngine solutions can help you
<p>Identity Management, Authentication and Access Control (PR.AC):</p> <p>Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.</p>	<p>PR.AC-1</p> <p>Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes</p>	<p>AD360: Automate authorization of user access to resources based on their organization role.</p> <p>PAM360: Identify and authorize access to business-critical resources, and spot unusual privileged activities.</p> <p>FileAnalysis: Prevent privilege abuse by analyzing users' access permissions.</p>
	<p>PR.AC-3:</p> <p>Remote access is managed</p>	<p>PAM360: Allow privileged users to access remote hosts without any endpoint agents. Provision secure access to critical data center components through SSH, Telnet, and RDP connections.</p> <p>Endpoint Central: Establish a secure, web-based connection to remote computers in the LAN and WAN through VPN or internet.</p>
	<p>PR.AC-4:</p> <p>Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties</p>	<p>PAM360: Establish strict governance over privileged access pathways and critical infrastructure. Assign just-in-time controls and provision higher privileges only when required by users.</p> <p>AD360: Streamline identity access management tasks by imposing least privilege access policies to users based on their roles and responsibilities.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>PR.AC-5:</p> <p>Network integrity is protected (e.g., network segregation, network segmentation)</p>	<p>Network Configuration Manager: Configure the network configlets and maintain control over change workflow and changes within network infrastructure.</p> <p>AD360: Streamline identity access management tasks by imposing least privilege access policies to users based on their roles and responsibilities.</p>
	<p>PR.AC-6:</p> <p>Identities are proofed and bound to credentials and asserted in interactions</p>	<p>PAM360: Onboard privileged user accounts into a secure vault mechanism that offers role-based access to the critical assets in the network.</p> <p>AD360: Streamline identity access management tasks by imposing least privilege access policies to users based on their roles and responsibilities.</p>
	<p>PR.AC-7:</p> <p>Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)</p>	<p>ADSelfService Plus: Implement MFA techniques such as biometrics and QR codes to authenticate user identity.</p> <p>Identity Manager Plus: Centrally manage application access and usage, and provide SSO for your end users.</p>

Category	Subcategory	How ManageEngine solutions can help you
<p>Data Security (PR.DS):</p> <p>Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.</p>	<p>PR.DS-1:</p> <p>Data-at-rest is protected</p>	<p>DataSecurity Plus: Secure and control access to USBs, selectively block file copy actions for business-critical information, and prevent leakage of confidential files via email attachments.</p> <p>Endpoint DLP Plus: Automate detection and classification of personal data, audit file access, and establish policies to ensure secure usage.</p>
	<p>PR.DS-2:</p> <p>Data-in-transit is protected</p>	<p>Key Manager Plus: Manage SSH keys and digital certificates to ensure secure, encrypted data communication.</p>
	<p>PR.DS-3:</p> <p>Assets are formally managed throughout removal, transfers, and disposition</p>	<p>Asset Explorer: Handle the complete life cycle of every asset from procurement to disposal.</p>
	<p>PR.DS-4:</p> <p>Adequate capacity to ensure availability is maintained</p>	<p>OpManger Plus: Monitor and optimize your network bandwidth, the performance of critical network devices, the firewall, and servers.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>PR.DS-5:</p> <p>Protections against data leaks are</p>	<p>Endpoint Central:</p> <p>Identify emails containing sensitive information using fingerprinting, keyword search, and RegEx, and block emails as per your policy. Block the transfer of sensitive information via unauthorized USB devices. Control the download and printing limit for trusted devices.</p>
	<p>PR.DS-6:</p> <p>Privileged users understand their roles and responsibilities</p>	<p>DataSecurity Plus:</p> <p>Maintain file integrity by monitoring permission changes, file creation, and move and modify events.</p> <p>Network Configuration Manager:</p> <p>Identify potential firmware security vulnerabilities in your network and perform corrective measures periodically.</p> <p>Vulnerability Manager Plus:</p> <p>Monitor network endpoints to detect end-of-life software, peer-to-peer apps, and remote-sharing tools. Eliminate the associated security risks by uninstalling unsafe software.</p>

Category	Subcategory	How ManageEngine solutions can help you
<p>Information Protection Processes and Procedures (PR.IP):</p> <p>Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. protect the confidentiality, integrity, and availability of information.</p>	<p>PR.IP-1:</p> <p>A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)</p>	<p>Network Configuration Manager: Back up incremental versions of network configurations and choose the most stable version as the baseline configuration.</p>
	<p>PR.IP-3:</p> <p>Configuration change control processes are in place</p>	<p>Network Configuration Manager: Automate configuration backups and database backups to withstand network mishaps.</p> <p>ServiceDesk Plus: Configure change types, roles, and statuses to manage your change cycle.</p>
	<p>PR.IP-4:</p> <p>Backups of information are conducted, maintained, and tested</p>	<p>RecoveryManager Plus: Back up your AD, Azure AD, Microsoft 365, Google Workspace, and Exchange environments.</p> <p>Network Configuration Manager: Automate network device configuration backups and reduce downtime.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>PR.IP-5:</p> <p>Policy and regulations regarding the physical operating environment for organizational assets are met</p>	<p>PAM360: Secure administrative access to critical systems through privileged pathways.</p> <p>Endpoint Central: Configure stringent passcode and device lock policies to protect corporate assets.</p> <p>Mobile Device Manger Plus: Configure device settings and functions on corporate mobile devices based on assigned groups. Set up alerts and schedule custom reports to gain visibility into compliance violations.</p>
	<p>PR.IP-6:</p> <p>Data is destroyed according to policy</p>	<p>Endpoint Central: Perform a corporate wipe to remove corporate data, leaving personal data intact in personnel's mobile assets.</p>
	<p>PR.IP-9:</p> <p>Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed</p>	<p>ServiceDesk Plus: Streamline major incident management by configuring multiple criteria to execute custom actions. Reduce repeat incidents by defining closure rules.</p>
<p>Maintenance (PR.MA):</p> <p>Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.</p>	<p>PR.MA-1:</p> <p>Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools</p>	<p>ServiceDesk Plus: Configure workflows for regular maintenance tasks and gain visibility into assets that are in repair, expired, or maintenance mode.</p> <p>Patch Manager Plus: Automate the distribution of OS and third-party patches to endpoints as per configured deployment policies.</p>

Category	Subcategory	How ManageEngine solutions can help you
<p>Protective Technology (PR.PT):</p> <p>Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>PR.PT-1:</p> <p>Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</p>	<p>Log360:</p> <p>Collect logs from devices, servers, network devices, firewalls, and more. Encrypt the log data for future forensic analysis, compliance, and internal audits.</p> <p>Firewall Analyzer:</p> <p>Collect and analyze log data from the firewall and other security devices to discover security threat attempts and perform bandwidth management.</p>
	<p>PR.PT-3:</p> <p>The principle of least functionality is incorporated by configuring systems to provide only essential capabilities</p>	<p>Application Control Plus:</p> <p>Limit malware intrusions by blocklisting malicious executables.</p> <p>PAM360:</p> <p>Adopt a Zero Trust security approach to reduce security risks by using least privilege workflows for access provisioning.</p> <p>DataSecurity Plus:</p> <p>Detect ransomware with threshold-based alerts by inspecting sudden spikes in file rename and other change events. Shut down infected devices to contain the ransomware spread in your network quickly.</p>
	<p>PR.PT-5:</p> <p>Mechanisms (e.g., fail-safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations</p>	<p>OpManager Plus:</p> <p>Secure your network with the Advanced Security Analytics Module to detect zero-day network intrusions, firewall rule anomalies, and rogue devices.</p> <p>Endpoint Central:</p> <p>Protect data by managing BitLocker encryption in endpoints. Prevent ransomware attacks with behavioral detection and fail-safe recovery. Secure sensitive information from theft by using advanced data loss prevention strategies.</p>

Detect:

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Category	Subcategory	How ManageEngine solutions can help you
<p>Anomalies and Events (DE.AE):</p> <p>Anomalous activity is detected and the potential impact of events is understood.</p>	<p>DE.AE-1:</p> <p>A baseline of network operations and expected data flows for users and systems is established and managed</p>	<p>Log360: Group users in the network based on their behaviors and establish a baseline for their group. Use the baseline as a reference to flag any deviations as anomalies and raise alerts.</p> <p>OpUtils: Scan routers and subnets periodically to detect rogue devices in the network and block their access.</p> <p>NetFlow Analyzer: Leverage the network behavior anomaly detection system to analyze server traffic, diagnose network anomalies, and identify any threats in the network.</p> <p>DataSecurity Plus: Monitor file activities, data transfers, and application usage to spot anomalous activities.</p>
	<p>DE.AE-2:</p> <p>Detected events are analyzed to understand attack targets and methods</p>	<p>Log360: Analyze and correlate logs with visual dashboards to discover security incidents, attacks, and suspicious or malicious user behavior.</p>
	<p>DE.AE-3:</p> <p>Event data are collected and correlated from multiple sources and sensors</p>	<p>Log360: Collect and analyze event logs from the endpoints, servers, network devices, and firewalls in your environment to spot security threats.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>DE.AE-4:</p> <p>Impact of events is determined</p>	<p>Log360:</p> <p>Understand the impact of incidents by conducting post-attack analysis and identify patterns to stop attacks through log forensics.</p>
	<p>DE.AE-5:</p> <p>Incident alert thresholds are established</p>	<p>Log360:</p> <p>Configure alert thresholds by selecting the number of anomalies, interval, and time range that would trigger the alert.</p>
<p>Security Continuous Monitoring (DE.CM):</p> <p>The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.</p>	<p>DE.CM-1:</p> <p>The network is monitored to detect potential cybersecurity events</p>	<p>Log360:</p> <p>Gain insights into your security incidents by monitoring and collecting extensive audit data from servers, firewalls, applications, and endpoints.</p> <p>NetFlow Analyzer:</p> <p>Utilize flow technologies to aid in network forensics and security analysis to discover internal or external security threats, zero-day vulnerabilities, and network anomalies.</p>
	<p>DE.CM-3:</p> <p>Personnel activity is monitored to detect potential cybersecurity events</p>	<p>Log360:</p> <p>Monitor privileged user activities, data access, and network access, and receive real-time alerts for incidents.</p>

Category	Subcategory	How ManageEngine solutions can help you
	<p>DE.CM-7:</p> <p>Monitoring for unauthorized personnel, connections, devices, and software is performed</p>	<p>OpUtils: Identify rogue device intrusions in the network and block access.</p> <p>Endpoint Central: Limit cyberattacks by blocking non-business applications and malicious executables.</p> <p>Log360: Discover the entire list of shadow IT applications in the network automatically and track users requesting access to these applications.</p>
	<p>DE.CM-8:</p> <p>Vulnerability scans are performed</p>	<p>Vulnerability Manager Plus: Scan your networks periodically to detect vulnerabilities and remediate patch deployment.</p>
<p>Detection Processes (DE.DP):</p> <p>Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.</p>	<p>DE.DP-4:</p> <p>Event detection information is communicated</p>	<p>Log360: Correlate log data to detect attack patterns, conduct root cause analysis, and automate immediate notifications via email and SMS.</p> <p>AD360: Set up alert profiles to notify security personnel via email and SMS on detection of suspicious user activity with UBA.</p> <p>Firewall Analyzer: Send security alerts to admins through email or SMS on detection of anomalous traffic behavior.</p>
	<p>DE.DP-5:</p> <p>Detection processes are continuously improved</p>	<p>Analytics Plus: Gather insights from anomaly patterns and drill down to specific metrics to identify areas that need improvement.</p>

Respond:

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

Category	Subcategory	How ManageEngine solutions can help you
<p>Response Planning (RS.RP):</p> <p>Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.</p>	<p>RS.RP-1:</p> <p>Response plan is executed during or after an incident</p>	<p>Vulnerability Manager Plus: Remediate threats and vulnerabilities by automating the deployment of patches to operating systems and third-party applications.</p> <p>ADManager Plus: Modify or revoke NTFS permissions to limit the exposure of sensitive files.</p> <p>Log360: Automate and accelerate threat response through standard workflows, and streamline incident management by integrating with ticketing tools.</p> <p>ServiceDesk Plus: Automate major incident workflows to improve resolution time and streamline major incident management.</p>
<p>Communications (RS.CO):</p> <p>Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).</p>	<p>RS.CO-3:</p> <p>Information is shared consistent with response plans</p>	<p>ServiceDesk Plus: Automate custom notifications to various relevant stakeholders through email when a high priority tickets are created.</p>
	<p>RS.CO-5:</p> <p>Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness</p>	<p>Site24x7 StatusIQ: Keep all stakeholders in the loop about an incident by posting on your status page or sending out notifications via SMS or email.</p>

Category	Subcategory	How ManageEngine solutions can help you
<p>Analysis (RS.AN):</p> <p>Analysis is conducted to ensure effective response and support recovery activities.</p>	<p>RS.AN-1:</p> <p>Notifications from detection systems are investigated</p>	<p>Log360:</p> <p>Mitigate internal and external threats by collecting and analyzing real-time data from all critical resources.</p>
	<p>RS.AN-2:</p> <p>The impact of the incident is understood</p>	<p>Vulnerability Manager Plus:</p> <p>Scan your networks periodically to detect vulnerabilities and remediate patch deployment.</p>
	<p>RS.AN-3:</p> <p>Forensics are performed</p>	<p>NetFlow Analyzer:</p> <p>Detect security threats using Continuous Stream Mining Engine technology. Track network anomalies that infiltrate your firewall and identify context-sensitive anomalies by analyzing traffic patterns.</p> <p>Log360:</p> <p>Conduct forensics analysis by identifying network and system anomalies.</p>
	<p>RS.AN-4:</p> <p>Incidents are categorized consistent with response plans</p>	<p>ServiceDesk Plus:</p> <p>Classify incidents based on their urgency and the severity of their impact on users or the business.</p>
	<p>RS.AN-5:</p> <p>Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)</p>	<p>Vulnerability Manager Plus:</p> <p>Test and deploy patches to multiple operating systems and third-party applications.</p>

Category	Subcategory	How ManageEngine solutions can help you
<p>Mitigation (RS.MI):</p> <p>Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.</p>	<p>RS.MI-1:</p> <p>Incidents are contained</p>	<p>OpManager:</p> <p>Automate fault remediation actions based on incident alerts.</p>
	<p>RS.MI-2:</p> <p>Incidents are mitigated</p>	<p>ServiceDesk Plus:</p> <p>Reduce repeat incidents through root cause analysis.</p> <p>Log360:</p> <p>Automate incident response and create incident workflows triggered by alerts.</p>
	<p>RS.MI-3:</p> <p>Newly identified vulnerabilities are mitigated or documented as accepted</p>	<p>Log 360:</p> <p>Prioritize security threats and automate response to detected incidents.</p> <p>Vulnerability Manager Plus:</p> <p>Mitigate the exploitation of security loopholes in your network and prevent further loopholes from developing.</p>
<p>Improvements (RS.IM):</p> <p>Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.</p>	<p>RS.IM-2:</p> <p>Response strategies are updated</p>	<p>Vulnerability Manager Plus:</p> <p>Remedy web server security flaws by acquiring details on the incident cause and impact. Prioritize vulnerable areas susceptible to exploitation by using attacker-based analytics.</p>

Recover:

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Category	Subcategory	How ManageEngine solutions can help you
<p>Recovery Planning (RC.RP):</p> <p>Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.</p>	<p>RC.RP-1:</p> <p>Recovery plan is executed during or after a cybersecurity incident</p>	<p>RecoveryManager Plus: Automate incremental or complete backups of ADs, virtual machines, and Windows servers to restore affected files in case of any cyberattacks.</p> <p>Network Configuration Manager: Restore network functions in case of a misconfiguration disaster by implementing a rollback mechanism to a trusted network configuration version.</p>
<p>Improvements (RC.IM):</p> <p>Recovery planning and processes are improved by incorporating lessons learned into future activities.</p>	<p>RC.IM-1:</p> <p>Recovery plans incorporate lessons learned</p>	<p>Analytics Plus: Identify areas of improvement using data from all your enterprise applications or databases.</p>
<p>Communications (RC.CO):</p> <p>Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).</p>	<p>RC.CO-3:</p> <p>Recovery activities are communicated to internal and external stakeholders as well as executive and management teams</p>	<p>Site24x7 StatusIQ: Keep all stakeholders in the loop about an incident by posting on your status page or sending out notifications via SMS or email.</p>

How can you establish or improve a cybersecurity program?

The framework offers organizations a repeatable set of actions that can be performed to design their cybersecurity practices from scratch or build on their existing program to tackle the evolving cyberthreat landscape

Step 2: Orient

The identified support systems and assets can be used to understand applicable threats and vulnerabilities. This helps in drafting an overall risk approach.

Step 4: Perform a risk assessment

To build a resilient cybersecurity management program, organizations must assess the likelihood of a cybersecurity event and the consequential impact on business approach.

Step 6: Identify and prioritize gaps

By comparing the current and target profiles, organizations can determine the efforts necessary to bridge the gap. By formulating an action plan to address the gap by outlining the budget, risk, benefit, mission drivers, and resources, a cost-effective approach can be spelled out with informed decisions. approach.

Step 1: Prioritize and define the scope

By defining their business objectives and priorities clearly, organizations can understand the underlying support systems and assets that need to be safeguarded from cyberthreats.

Step 3: Create a current profile

Organizations can understand their current cybersecurity posture by creating a profile that illustrates the outcomes of categories and subcategories that are being achieved.

Step 5: Create a target profile

Based on their current profile and the possibility of cybersecurity risks, organizations can determine the chink in their armor. By focusing on the area of vulnerability, the respective outcomes under categories and subcategories are noted down to manage risks.

Step 7: Implement an action plan

Organizations can move towards their desired target state with guidance from the informative references provided for the outcomes. Organizations have the leeway to choose which standards and guidelines better suit their requirements.

Parting thoughts

As with any worthy endeavor, the implementation of the NIST Cybersecurity Framework is more about improving your cybersecurity posture as evolving threats arise rather than racing towards a definite finish line. Keeping your organization secure is an enduring and iterative process that comprises risk assessment and implementation of best practices. The framework acts as a compass that guides organizations in the right direction to plan and prioritize their cybersecurity strategies.

About ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—more than 120 products and free tools—to manage all of your IT operations, from networks and servers to applications, your service desk, AD, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. You can find our on-premises and cloud solutions powering the IT of over

280,000 companies around the world, including 9 of every 10 Fortune 100 companies.

As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize future opportunities.



Enterprise service management

- Full-stack ITSM suite
- IT asset management with a CMDB
- Knowledge base with user self-service
- Built-in and custom workflows
- Orchestration of all IT management functions
- Service management for all departments
- Reporting and analytics

Identity and access management

- Identity governance and administration
- Privileged identity and access management
- AD and Azure AD management and auditing
- SSO for on-premises and cloud apps, with MFA
- Password self-service and sync
- Microsoft 365 and Exchange management and auditing
- AD and Exchange backup and recovery
- SSH and SSL certificate management

Unified endpoint management and security

- Desktop and mobile device management
- Patch management
- Endpoint device security
- OS and software deployment
- Remote monitoring and management
- Web browser security
- Monitoring and control of peripheral devices
- Endpoint data loss prevention

Take control of your IT.

Monitor, manage, and secure your digital enterprise with ManageEngine



ManageEngine crafts comprehensive IT management software for your business needs

Available for
Enterprise IT | Managed service providers (MSPs)
As
Self-hosted on-premises
Self-hosted in public cloud (AWS, Azure)
Zoho Cloud-native

IT operations management

- Network, server, and application performance monitoring
- Bandwidth monitoring with traffic analysis
- Network change and configuration management
- Application discovery and dependency mapping
- Cloud cost and infrastructure monitoring
- End-user experience monitoring
- DNS management
- AIOps

Security information and event management

- Unified SIEM for cloud and on-premises
- AI-driven user and entity behavior analytics
- Firewall log analytics
- Data leak prevention and risk assessment
- Regulatory and privacy compliance

Advanced IT analytics

- Self-service IT analytics
- Data visualization and business intelligence for IT
- Hundreds of built-in reports and dashboards
- Instant, flexible report creation
- Out-of-the-box support for multiple data sources

Low-code app development


- Custom solution builder


9 of every 10 Fortune 100 companies
trust us to manage their IT.




ManageEngine

www.manageengine.com

 [ManageEngine](https://twitter.com/ManageEngine)

 [ManageEngine](https://www.linkedin.com/company/manageengine)

 [ManageEngine](https://www.facebook.com/ManageEngine)