**Risk Assessment Checklist to Help Prepare for  
NIST Cybersecurity Framework Implementation**



Disclaimer

*This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.*

*This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.*

*This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal, reference purposes.*

*The information contained in this document must not be construed as legal advice. Customers must seek their own legal counsel for advice on compliance with regulatory requirements impacting their organization*

*Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.*

*NOTE: Certain recommendations in this document may result in increased data, network, or compute resource usage, and may increase a customer’s license or subscription costs.*

*Version 1.1*

*© 2017 Microsoft. All rights reserved.*

# **Introduction**

On May 11, 2017, the President released Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. This Executive Order calls for organizations to provide a risk management report, to utilize shared IT services, and develop an action plan to implement the [NIST Cybersecurity Framework (CSF)](https://www.nist.gov/cyberframework).

The NIST CSF has four Implementation Tiers that describe how an organization views and addresses cybersecurity risk and risk management processes: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). External guidance from Federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), and other sources can be leveraged to assist in determining your organization’s current and desired Implementation Tier with respect to the Framework outcomes. This risk assessment checklist can be used to help your organization establish a high-level understanding of your security practices and identify areas of potential cybersecurity risk. By understanding the areas that have a higher risk, your organization can develop a plan to implement the full scope of outcomes described in the NIST CSF. Additional testing and evaluation should be conducted to determine the ability of your organization to align risk management practices with the NIST CSF as well as to determine a plan to implement requirements that are less than fully satisfied by current organization processes and procedures.

This checklist presents a series of broad questions that cover each of the Functions (Identify, Protect, Detect, Respond, and Recover) in the “Framework for Improving Critical Infrastructure Cybersecurity.” In addition to the questions themselves, guidance has been provided on how to interpret responses. When addressing the questions below to gauge your organization’s risk posture, responses may be assigned a designation of satisfactory, medium risk, or high risk. The “Response Assessment” section at the end of this document describes how to use the response assignments to assemble an overall picture of your organization’s risk posture as it relates to the NIST CSF outcomes. Based on your responses, your organization can determine the areas in which your cybersecurity processes need improvement. These areas will need to be included in your action plan for implementing the NIST CSF outcomes at one of the Implementation Tiers mentioned above.

The [Service Trust Portal](https://servicetrust.microsoft.com/) contains NIST CSF enablement whitepapers which demonstrate how your organization can use Microsoft Azure services to achieve the cybersecurity outcomes described in the NIST CSF Functions. For additional resources regarding customer responsibilities related to NIST CSF and the Cybersecurity Executive Order, or to provide feedback, please e-mail [CyberEOHelp@Microsoft.com](mailto:CyberEOHelp@Microsoft.com).

# **Risk Assessment Questionnaire:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **What is your organization’s IT security policy?** | | | | | | |
| **Function** | **Category** | **Questions to gauge risk posture** | **Satisfactory Response**  **(Score of 1)** | **Medium Risk Response**  **(Score of 2)** | **High Risk Response**  **(Score of 3)** | **Score** |
| Identify | Governance  Asset Management | 1. Do you have a policy in place to manage and monitor your organization’s security posture? **(ID.GV-1)** 2. Do you have clearly defined information security roles and responsibilities? **(ID.AM-6)** 3. Are your security roles coordinated and aligned with internal roles and external partners? **(ID.GV-2)** 4. Do you have an awareness of the legal and regulatory security requirements in place for your organization? **(ID.GV-3)** | A rigorous policy document with clearly defined procedures and roles exists, and there is organization-wide enforcement. Security is incorporated into day to day activities. | There are some ambiguous procedures and enforcement is not prioritized. Some individuals within the organization may have defined roles and responsibilities but there is not an organization-wide focus on security. | No policy document exists and there is no organization-wide enforcement. Users are not aware of security requirements or how to incorporate security into daily tasks. |  |
| Identify  Protect | Business Environment  Data Security  Protective Technology | 1. Do you perform business impact analysis for your organization’s services and the infrastructure hosting those services? **(ID.BE)** 2. Have you identified and communicated your organization's role in the supply chain? **(ID.BE-1)** 3. What is your organization's place in the critical infrastructure and your overall industry? **(ID.BE-2)** 4. Have you established priorities for your organization's mission, objectives and activities and are they clearly communicated to all stakeholders? **(ID.BE-3)** 5. Have you performed an analysis identifying critical functions and dependencies for the services that your organization provides? **(ID.BE-4)** 6. Have you established functional states in order to keep your services operational under times of normal operation, duress/attack, and recovery? Do those requirements include planning for adequate capacity in order to maintain system availability? **(ID.BE-5 PR.PT-5 PR.DS-4)** | Based on the criticality of your services, your organization understands and prioritizes mission goals and infrastructure and how they relate to the industry. Your organization understands its role in the supply chain. Furthermore, a plan for continued availability and operation of your organization’s assets is established. | Understands mission goals and infrastructure and how they relate to the industry; however, priorities are not adjusted accordingly which may impact availability and operation. | Functional states, mission goals, your organization’s place in the supply chain, and infrastructure are not prioritized or understood. |  |
| Protect | Awareness & Training | 1. Does your organization have a security or risk awareness and training process in place? **(PR.AT-1)** 2. Are roles and responsibilities clearly defined and understood by privileged users, third-party stakeholders (e.g. suppliers, customers, partners), senior executives; and physical and information security personnel? **(PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5)** | A thorough training program is implemented, and participation is tracked; there is an organization-wide awareness of established roles and responsibilities. | An informal training program is available for personnel to attend, and the organization publishes a guide for roles and responsibilities. | No training or awareness programs exist. Users must seek training on their own and there are no systems in place to track course completion. |  |
| **Section Risk Total** | | | | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **How does your organization protect data and systems?** | | | | | | |
| **Function** | **Category** | **Question to gauge risk posture** | **Satisfactory Response**  **(Score of 1)** | **Medium Risk Response**  **(Score of 2)** | **High Risk Response**  **(Score of 3)** | **Score** |
| Protect | Data Security  Identity Management & Access Control  Information Protection | 1. Who has access to data? **(PR.DS)** 2. How are least privilege and separation of duties managed? **(PR.AC-4)** 3. How are access restrictions managed and maintained? (Username/ password, RSA keys, Smartcards, remote access) **(PR.AC-1 PR.AC.2 PR.AC.3)** 4. Do you validate the identity of personnel when issuing credentials and is their identity linked to those credentials? **(PR.AC-6)** 5. Are your assets managed including removal, transferal and disposition? **(PR.AC-2 PR.DS-3)** 6. Is data protected at rest and in transit?Is encryption used (i.e., SSL, TLS)? **(PR.DS-1 PR.DS-2)** 7. Is the network segregated where appropriate? **(PR.AC-5)** 8. Do you use a testing and development environment? **(PR.DS-7)** 9. Does your organization consider cybersecurity when managing human resources? **(PR.IP-11)** | Data kept is encrypted on your organization’s servers with security measures in place; two-factor authentication is required to access data; digital resources are managed; clear network segregation exists for sensitive data; development and testing environments are used. | Data kept in secure cloud storage; data access is reasonably controlled; users only utilize passwords to access data; digital resources are partially managed (e.g. removal is managed, however transfer is not); testing and development environments are considered but not segregated. | Data kept in low-security cloud storage or unprotected servers; personnel could call a help desk or another employee for account data without identity verification; resources are unmanaged; the network is not segregated; testing and/or development environments do not exist. |  |
| Protect | Data Security | 1. Is there a process in place to verify the integrity of software, firmware, hardware and information? **(PR.DS-6 PR.DS-8)** | Your organization has a rigorous verification process of software, firmware, hardware and information integrity. | Your organization has a verification process in place but is not always utilized in verifying software, firmware, hardware and information integrity. | There is no process in place to verify software, firmware, hardware and information integrity. |  |
| Protect | Protective Technology | 1. How does your organization protect communications and networks? **(PR.PT-4)** | Your organization encrypts remote user traffic, and it understands, implements, and configures network monitoring devices such as IPS/IDS/Firewall at all boundary points and defined points within the system. Your organization utilizes VLANs where possible to segregate sensitive network data and traffic. TLS is utilized for internal and external web traffic. When implementing all of the methods listed above, your organization configures them with industry standard best practices for security. | Your organization implements many of the methods listed in the "satisfactory response" section above, however, it does not use industry standard best practices for configuring these methods. For example, your organization does not implement the following: deny all statements after explicit allow, configuration of remote sessions with a strong encryption method, using the most up to date version of TLS.  Another response may be that your organization uses some of the methods listed above with industry standard best practices, but your organization does not have a well-structured defense-in-depth approach due to implementing only a few of the solutions instead of a larger suite. | You are unsure of the methods in place securing your organization’s communications and networks. Technical protections are not well defined and documented. |  |
| Protect | Information Protection | 1. Do you maintain your physical operating environment for organizational assets in line with established policies and regulations? **(PR.IP-5)** | Your organization implements policies and regulations for maintaining the physical operating environment and the established standards are consistently met. | Your organization has established policies and regulations for maintaining the physical operating environment however those standards are not consistently met. | There is no policy or regulations in place for maintaining the physical operating environment. |  |
| Protect | Protective Technology | 1. How does your organization protect and restrict the use of removable media, and is it in line with policy? **(PR.PT-2)** | Your organization has a policy identifying how removable media should be used and it is communicated and well understood by all system users. | Your organization has a policy identifying how removable media should be used but it is not followed or understood by all system users. | No removable media policy exists for the use of removable devices. Removable media is not limited through technical means. |  |
| Protect | Data Security | 1. Does your organization employ any additional processes to limit data leaks? **(PR.DS-5)** | Your organization has a comprehensive plan for managing and mitigating data leaks. Mitigation methods include many or all of the following: access control methods, established system configuration processes, encryption, intrusion detection, and end-user awareness. | Your organization has identified some data leak protection mechanisms, but the risk of data leaks is not reduced to an acceptable level using the industry standard methods. | There is no plan or mechanisms in place to control or mitigate data leaks. |  |
| Protect | Information Protection | 1. Does your organization continuously improve protection processes and is the effectiveness of those processes communicated to the appropriate stakeholders? **(PR.IP-7 PR.IP-8)** | Your organization has a well-defined review cycle for reviewing all protection processes. The review cycle includes an internal review and a continuous monitoring process. All inefficiencies discovered during review are documented, considered, and subjected to change and approval. The overall effectiveness is communicated with the appropriate parties. | Your organization has a review cycle for all protection processes, but that review process is not well defined or rarely followed and acted upon. | Your organization does not review protection processes. |  |
| **Section Risk Total** | | | | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **How are assets managed?** | | | | | | |
| **Function** | **Category** | **Question to gauge risk posture** | **Satisfactory Response**  **(Score of 1)** | **Medium Risk Response**  **(Score of 2)** | **High Risk Response**  **(Score of 3)** | **Score** |
| Identify  Protect | Asset Management  Protective Technology | 1. How are assets mapped, categorized and prioritized? **(ID.AM)** 2. How are information flows mapped? **(ID.AM-3)** 3. Do you document the use of external systems? **(ID.AM-4)** 4. Are your organizational resources (e.g., hardware, devices, data, time, and software) prioritized? **(ID.AM-5)** 5. Does your organization use audit logs and are they reviewed according to policy? **(PR.PT-1)** | Your organization has documented organizational data flows which include the use of any external systems. If any external systems are leveraged, the use case and information related to the external system is documented. Organizational resources including hardware, data, time, and software, are all prioritized based on their classification and criticality in relation to performing business objectives. Your organization has implemented the use of audit logs for assets/systems and the review of auditable events is performed as defined by your organization’s policy. | Your organization has some documentation related to data flows and connections to external systems, but the documentation is not updated regularly. Some organizational resources are prioritized but many are left undefined. | There is no documentation around organizational data flows and the connections to any external systems. Organizational resources are not prioritized. |  |
| Identify | Asset Management | 1. How are assets tracked? **(ID.AM)** 2. Is there a hardware inventory of devices and systems within your organization? **(ID.AM-1)** 3. Do you keep a software inventory of platforms and applications within your organization? **(ID.AM-2)** | Your organization has an established inventory of all system assets which uses automated processes for updating and adding key information of those assets. Changes made to the inventory are monitored and/or only allowed by explicit personnel/processes. | Your organization’s inventory is incomplete and/or there is key information missing for the listed assets. Inventory is updated at a monthly frequency or less often, and changes made to the inventory are not subjected to be performed by defined personnel and/or processes. | Your organization does not have an inventory of system assets, or changes to the inventory that have been documented are done at an ad-hoc frequency by undefined personnel. |  |
| Protect | Protective Technology  Information Protection | 1. How are assets configured? **(PR.IP)** 2. Is there a configuration baseline currently in use? **(PR.IP-1)** 3. Is there a change management process? **(PR.IP-3)** 4. Is there an SDLC process in place? **(PR-IP-2)** 5. Is the principle of least functionality incorporated in your SDLC and current systems? **(PR.PT-3)** | Your organization uses a baseline configuration for all system assets. The configuration baseline and any changes made throughout the system are subjected to a well-defined SDLC and change management process (i.e. changes are authorized, tested, and approved). All configurations and changes consider the principle of least privilege. | Your organization uses baseline configurations for system assets, however the baselines are not well maintained or subjected to your SDLC or change management processes when maintenance or changes occur. Furthermore, the principle of least privilege is often an afterthought when configuring or making changes to system assets. | Your organization does not use a defined baseline configuration for system assets. There are not well-documented SDLC and change management processes and/or they are not implemented. Additionally, the least privilege principle is not considered in when making changes or configurations. |  |
| Protect | Maintenance | 1. Does your organization maintain and repair its assets in a timely manner and are such maintenance activities, including remote maintenance, logged and approved? **(PR.MA-1 PR.MA-2)** | Your organization has a thorough response team to address maintenance issues in a timely manner. Any maintenance activities are documented and approved including any remote maintenance sessions. | Your organization has personnel assigned to maintenance issues however, they are also tasked with other organizational processes, which in turn does not allow for a quick response time to maintenance issues. Remote activities are approved but not logged. | Your organization does not have defined personnel assigned to maintenance activities and there is no documentation of maintenance activities performed. |  |
| Protect | Information Protection | 1. How is data safely disposed of and/or destroyed? **(PR.IP-6)** 2. Do assets undergo data sanitization? **(PR.IP-6)** | Your organization has a well-defined and understood policy describing the destruction/disposal of data and the sanitization of system assets containing organizational data. Disposal/destruction processes leverage third-party services providing certificates of device destruction and/or your organization takes elaborate measures to ensure devices are properly destroyed and/or disposed of. Your data sanitization process is consistent with the industry wide best practices. | Your organization has a policy describing how organizational assets and data are disposed of and sanitized. That policy is not well understood by all personnel performing disposal and/or sanitization processes. | Your organization does not have a process for the destruction/disposal of organizational assets, nor are you concerned with the sanitization of organizational assets containing data. |  |
| **Section Risk Total** | | | | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **How are vulnerabilities and suspicious activities detected and managed?** | | | | | | |
| **Function** | **Category** | **Question to gauge risk posture** | **Satisfactory Response**  **(Score of 1)** | **Medium Risk Response**  **(Score of 2)** | **High Risk Response**  **(Score of 3)** | **Score** |
| Detect | Security Continuous Monitoring  Detection Processes | 1. Does your organization perform scans for vulnerabilities, malicious code, and unauthorized mobile code? **(DE.CM-4 DE.CM-5 DE.CM-8)** 2. Have you clearly defined scanning roles and responsibilities? (**DE.DP-1)** 3. Are your scan definitions kept up to date? (**DE.DP-5)** | Daily or weekly scans are performed with strictly defined timelines for remediation and rigorous patch deployment procedures. Your organization uses a widely recognized scanning technology (i.e., Nessus, Qualys, or other major tools) Furthermore, your organization prioritizes vulnerabilities according to a severity score from CVSS, SCAP, or other vulnerability tracking standard. | Monthly or quarterly scans are performed with frequent slippage on remediation timelines. Roles and responsibilities are poorly defined for scanning and analysis. Scan definitions are updated on an ad hoc and not automated basis prior to scanning. | No scans performed. Remediation is performed, and patches are applied on an ad-hoc basis. |  |
| Detect  Respond | Security Continuous Monitoring  Detection Processes  Anomalies & Events  Analysis  Mitigation | 1. How does your organization detect suspicious activity? **(DE.DP)** 2. Have you clearly defined detection roles and responsibilities? **(DE.DP-1)** 3. Are detection activities compliant with requirements and communicated to appropriate parties? **(DE.DP-2 DE.DP-4)** 4. Are detection processes tested and continuously improved? **(DE.DP-3 DE.DP-5)** 5. Is the network, physical environment and personnel activity monitored to detect cybersecurity events? **(DE.CM-1 DE.CM-2 DE.CM-3)** 6. How is external service provider activity monitored? **(DE.CM-6)** 7. How are unauthorized personnel, connections, devices, and software monitored? **(DE.CM-7)** 8. Are multiple data sources and logical and/ or physical sensors considered when reviewing an event? **(DE.AE-3)** 9. When a notification from a detection system is received, does your organization investigate, contain, mitigate and categorize the incident consistent with the response plan? **(RS.AN-1 RS.AN-4 RS.MI-1 RS.MI-2)** | Your organization has a strong detection system that monitors the following for cybersecurity events: network, physical environment, personnel and external service providers. Furthermore, your organization continuously monitors your system and physical infrastructure for unauthorized personnel, connections, devices or software. Individuals are notified and held accountable for detection activities as per the roles and responsibilities established by a policy document or responsibility matrix. A notification is sent for any suspicious activity, and dependent on roles and responsibilities, individuals work to resolve the issue per the response plan in a timely manner. The detection process is regularly tested and improved. | While a detection system is in place, your organization does not have well-defined roles and responsibilities for detection. Accountability is not established for specific detection activities and the detection process is not frequently updated. Cybersecurity events are resolved, but the response plan is not followed. | Your organization does not have a system or process for detecting suspicious activity. Identifying incidents is reliant upon individuals and disparate efforts across the organization. |  |
| Detect | Anomalies & Events | 1. Does your organization establish and manage a baseline of network operations and expected data flows for users and systems? **(DE.AE-1)** 2. Is incident alerting in place for any event falling outside of the established threshold? **(DE.AE-5)** 3. Are detected events analyzed to determine attack targets and methods, as well as the impact those events may have on the system? **(DE.AE-2 DE.AE-4)** | Your organization continuously maintains a baseline for expected network operations, and user and system data flows. An automated incident alerting system is in place and alerting thresholds are set for when deviations occur from the baseline. When an event occurs, the attack methods and targets are analyzed, and the impact of the event is ascertained. | A baseline for expected network operations, user and system data flows are established; The baseline and data flows are not, however managed or updated on a regular basis. There is a systematic alerting system in place for when deviations from this baseline occur. Additionally, your organization has no formalized process of how events are analyzed. | There is no systematic incident alerting established, and incidents are investigated and resolved on an ad-hoc basis. |  |
| **Section Risk Total** | | | | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **How are security incidents handled?** | | | | | | |
| **Function** | **Category** | **Question to gauge risk posture** | **Satisfactory Response**  **(Score of 1)** | **Medium Risk Response**  **(Score of 2)** | **High Risk Response**  **(Score of 3)** | **Score** |
| Identify, Protect & Respond | Information Protection  Communications  Response Planning  Supply Chain Risk Management | 1. Is there an incident response plan and when is it executed? **(RS.RP-1 PR.IP-9)** 2. How often is the plan tested? **(PR.IP-10)** 3. Do personnel understand their role and the actions required of them when a response is needed? **(RS.CO-1)** 4. Is response planning and testing conducted in coordination with stakeholders, including critical suppliers and providers? **(RS.CO-4 ID.SC-5)** | There is an extensive incident response plan with clearly defined roles and responsibilities, frequent testing with internal and external stakeholders, early detection, and constant updates. | There is an incident response plan, but it is out-of-date and infrequently tested. Roles and responsibilities are not understood by all personnel that partake in the incident response process. | There is no established incident response plan and/or processes and procedures documented in the plan are not used in the actual response to incidents. |  |
| Respond Recover | Communications | 1. Are security incidents reported? **(RS.CO-2)** 2. Are recovery activities communicated to the appropriate personnel and is the information shared consistent with the response plan? **(RC.CO-3 RS.CO-3)** 3. Does your plan include disclosure instructions regarding other required parties for notification of incidents, including any external stakeholders, as necessary? **(RC.CO-1 RC.CO-2 RS.CO-5)** | There is an established criteria or standard for the reporting of events, that is understood and followed by your organization’s personnel. Those reported events are documented which include records of remediation timelines and disclosure to any internal or external stakeholders. | There is an ad-hoc response to reporting security incidents. Information disclosure is not always performed with internal or external stakeholders when needed. | There is no process to report security incidents. Incidents are handled on an ad hoc basis. |  |
| Identify, Protect & Recover | Information Protection  Recovery Planning  Supply Chain Risk Management | 1. Is there a recovery plan in place and what is the timeline for restoration? **(RC.RP-1 PR.IP-9)** 2. How often is the plan tested? **(PR.IP-10)** 3. Is recovery planning and testing conducted with critical suppliers and providers? **(ID.SC-5)** 4. Does your organization have backups in place to restore from and do you test them? **(PR.IP-4)** | There is an extensive recovery response plan with clearly defined roles and responsibilities, restoration timeline, and it is frequently tested with internal and external stakeholders. Incremental and/or full backups of information are regularly performed and the backup and restore mechanism is tested at least on at least an annual basis. | A recovery plan exists, but it is not up-to-date and is not frequently tested. Backups of information are performed; however, the restoration process is not tested periodically. | There is no recovery plan in place and an untested backup mechanism is utilized. Backups are not available for all systems. |  |
| Respond Recover | Analysis  Mitigations  Improvements | 1. Are the response and recovery processes updated as incidents occur? **(RS.IM-2 RC.IM-2)** 2. Are lessons learned incorporated? **(RS.IM-1 RC.IM-1)** 3. Is a root-cause analysis performed for each incident and is the impact determined? **(RS.AN-2 RS.AN-3)** 4. Does your organization mitigate newly identified vulnerabilities and when resolution is not possible, is the accepted risk documented? **(RS.MI-3)** | The response and recovery strategies are updated incorporating any lessons learned and takeaways from a root cause analysis. Your organization records vulnerabilities that cannot be mitigated and documents them as an accepted risk. | Forensics are not frequently performed to determine the root cause of an incident. As such, the response and recovery strategies are not updated in the aftermath of new incidents, but rather, on an ad-hoc basis. | Response and recovery plans are not updated as incidents occur. Root cause is often not determined or documented as part of incident response. |  |
| **Section Risk Total** | | | | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **How do you manage security risks?** | | | | | | |
| **Function** | **Category** | **Question to gauge risk posture** | **Satisfactory Response**  **(Score of 1)** | **Medium Risk Response**  **(Score of 2)** | **High Risk Response**  **(Score of 3)** | **Score** |
| Identify  Protect | Risk Management Strategy  Governance  Risk Assessment  Information Protection | 1. Does your organization have a process to manage risk including cybersecurity risk? **(ID.RM-1 ID.GV-4)** 2. Do you identify and document both internal and external threats, vulnerabilities, the likelihood of impact and the potential impact to your organization? Do you document the associated risk levels? **(ID.RA-1 ID.RA-3 ID.RA-4 ID.RA-5)** 3. Do you use forums or other shared sources to gather cyber threat or vulnerability information? **(ID.RA-2)** 4. Have you implemented a plan to manage vulnerabilities? **(PR.IP-12)** 5. Does your organization have a clearly defined and documented risk tolerance taking into consideration infrastructure and industry risk? **(ID.RM-2 ID.RM-3)** 6. Are resources prioritized to high risk items? **(ID.RA-6)** | The risk management process is kept up-to-date and is extensively used in security decisions. Your organization has documented its risk tolerance and there is good external and internal threat modeling with impact analysis. A plan is established to manage vulnerabilities based on the risk analysis and tolerance levels. Furthermore, there is good prioritization of resources, and priorities are adjusted when the level of risk changes, which allows for resources to be dedicated to high risk areas as appropriate. | The risk management process is infrequently updated, and it is used for some security decisions. There is a weakly defined risk tolerance and resources are not always prioritized per risk. As such, high risk areas may not receive prioritization when allocating resources | There is no risk management, resources are not allocated toward high-priority incidents when they occur, and there is little to no documentation or implementation to assist in the case of an incident. Stakeholders have no or little idea of current threats facing the organization. |  |
| Identify | Supply Chain Risk Management | 1. Has your organization established a process to manage cyber supply chain risk, including identifying, prioritizing and assessing both suppliers and partners of critical systems and services? **(ID.SC-1 ID.SC-2)** 2. Does your organization monitor your suppliers and partners to evaluate that they are meeting obligations and your information security objectives as contracted? **(ID.SC-3 and ID.SC-4)** | The cyber supply chain risk management process is kept up-to-date and is used in supply chain decisions. Cyber supply chain risk tolerances are appropriately defined. On at least an annual basis, your organization reviews audit summaries or conducts independent evaluations of suppliers and partners to validate that all contracted obligations are met and that the suppliers and partners have implemented measures to meet your organization's information security and cyber supply chain management standards. | A cyber supply chain risk management process exists, but it is infrequently updated and is not used for all cyber supply chain security decisions. As such, prioritization of resources is not always considered. Information security and cyber supply chain management standards are communicated to the suppliers and partners; however, they are not formally contracted nor are the partners and suppliers regularly monitored to determine whether they are meeting obligations. | No risk management processes for cyber supply chain exist. Your organization has not performed an analysis to identify suppliers and partners of your critical systems, components and services, and thus priorities have not been adjusted accordingly with the presented risk. |  |
| **Section Risk Total** | | | | | |  |

# Response assessment and scoring:

With help from the sections above, your organization can assemble a general understanding of in-place security practices and policies. This is not intended to be a formal assessment of all security practices and policies but can serve as a high-level indicator of organizational risk.

Any “high risk” response to the questions above should be considered for review. A high-risk response represents a serious security deficiency and should be addressed. Any high risks areas will likely be identified as findings and reportable compliance items that map to the FISMA framework that your organization follows.

Any “medium risk” response may need remediation and action to align with NIST CSF requirements. Any medium risk areas may be reportable and considered a compliance finding depending on the surrounding circumstances and configurations.

Any implementation receiving a "satisfactory response" is likely to be in alignment with CSF requirements but may be subject to auditor suggestions or comments for improvement of the response and your organization’s overall defense-in-depth strategy.

A score can be assigned to each of the responses above:

* One (1) point for satisfactory responses
* Two (2) points for medium risk responses
* Three (3) points for high risk responses

With a score of 28 or below, your organization has good, serviceable security practices and policies.

With a score of 32 or below, your organization has some processes in place for most of its security operations, even if the processes are not strictly enforced or frequently updated. An organization in this risk range should have a plan to improve its security practices, but still presents a manageable level of risk.

A score of 36 or above implies that there are inefficiencies or security gaps that should be addressed and may require additional implementation. You should seek guidance for improving the security posture of your organization.

Moving toward NIST Cybersecurity Framework alignment

If you need additional assistance or guidance after completing this initial NIST CSF risk assessment checklist, please reach out to [CyberEOHelp@Microsoft.com](mailto:CyberEOHelp@Microsoft.com). Although this checklist helps your organization identify the level of risk for different areas, please note that your organization is still responsible for reporting areas of risk, including any mitigations or accepted risks, as well as an action plan to implement NIST CSF outcomes.

Microsoft Azure can assist your organization with NIST CSF outcomes through a suite of technical solutions. Furthermore, Microsoft has developed resources including a NIST CSF Customer Responsibilities Matrix for customers looking to leverage Azure to assist with NIST CSF outcomes. For additional information regarding Azure security and compliance, visit the [Service Trust Portal](https://servicetrust.microsoft.com/) and the [Microsoft Trust Center](https://www.microsoft.com/en-us/TrustCenter/default.aspx).