[Insert Company Logo]

Risk Assessment Strategy and Risk Assessment Program

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800**
Mapping	**(1). NIST SP 800-53, rev. 5 (RA-3, PM-9).**

Overview

An organization-wide risk management strategy – and accompanying risk assessment program - includes an expression of the security and privacy risk tolerance for the organization, security and privacy risk mitigation strategies, acceptable risk assessment methodologies, a process for evaluating security and privacy risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

Furthermore, per NIST, the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Introduction

The Risk Management Strategy and Risk Assessment Program referenced within this document defines the measures undertaken by [company name] that strive to ensure the effective management of all relevant risks to the organization, and ultimately, to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, the Risk Management Strategy and Risk Assessment Program is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Risk Management Strategy and Risk Assessment Program is to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Risk Management Strategy and Risk Assessment Program is to document the organization's strategy and implementation measures for effectively managing a wide range of risks (i.e., organization level, mission/business process level, or information system level) that ultimately, can impact the Confidentiality, Integrity, and Availability (CIA) of [company name]'s people, processes, and technologies.

Scope

The Risk Management Strategy and Risk Assessment Program encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is described as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.* Additionally, the Risk Management Strategy and Risk Assessment Program can be informed by security and privacy risk-related inputs from other sources, both internal and external to the organization, to ensure that the strategy is broad-based and comprehensive.

Risk Management Strategy [NIST PM-9]

Applicability
It is fundamentally important to gain a strong understanding of the overall applicability of the entire risk management framework and lifecycle – and more specifically – the risk assessment processes to be undertaken, Specifically, in terms of applicability, when developing the organization's Risk Management Strategy and Risk Assessment Program, the following is to be assessed:

- External factors, ranging from client requirements/commitments to contractual requirement/commitments, regulatory compliance mandates, and associated laws, rules, and regulations.
- Internal factors, ranging from security, privacy, and operational/business specific best practices for managing and mitigating risks to specific requests from senior leadership, advisory boards, audit committees, etc.
- Any other factor, both external and internal, deemed relevant to [company name]'s overall Risk Management Strategy and Risk Assessment Program.

Risk Model and Framework
When assessing, considering, and ultimately, implementing a risk model and framework, [company name] is to reference the following models/frameworks, publications, and other appropriate artifacts:

- *NIST Risk Management Framework:* The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to effective information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector.
- *NIST 800-30, Guide for Conducting Risk Assessments*
- *NIST 800-39, Managing Information Security Risk: Organization, Mission, and Information System View*

- *NIST 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- *NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM)*

Risks

[Company name] is to be aware of the numerous risk factors that could impact the organization in a detrimental manner. As such, today's complex global economy requires [company name] to ensure that all necessary measures are taken for identifying – then defining, and ultimately, including in the annual risk assessment program – all relevant areas of risk, including, but not limited to, the following:

- Operations
- Supply Chain
- Information Security/Cybersecurity
- External Suppliers
- Insider Threats
- Data Privacy
- Regulatory Compliance
- Artificial Intelligence (AI)

Relevant Risk Categories

A key element of [company name]'s risk management strategy is to identify the relevant risk categories deemed in-scope for the organization. While there are many risk categories and elements that can be applied to an organization's infrastructure, it is critical that authorized personnel identify the specific risk categories, and then apply them throughout the risk management process by assessing them via a documented and formalized risk assessment program.

The following risk categories are to be evaluated on an annual basis to ensure their applicability in terms of performing an annual risk assessment for [company name].

- **Key Risks:** These are risks that arise from issues relating to geography, industry, and the relevant background of the actual third-party. Specifically, for "geographic" risks, these are risks relating to the physical location of the third-party and the related risks of where they reside – in terms of safety and security. For "industry" risk, these are risks relating to the actual industry for which the third-party operates within. For "background" risks, these are risks relating to the overall identity of the organization, and what negative or concerning factors arise out of initial due-diligence activities performed by [company name].

- **Information Technology & Information Security Risk(s):** These are risks arising from any number of information technology and information security issues, such as inadequate I.T. resources (i.e., hardware and software) along with lack of manpower. Additionally, risks can arise from abuse, misuse of information technology resources, while data breaches and security compromises can occur because of improperly designed networks, little to no information security policies, procedures, etc. Other serious information technology risks can include not correctly provisioning and hardening critical information systems, failing to implement “defense in depth” and layered security protocols, etc.

- **Privacy (PII & PHI) Risk(s):** These are risks that arise from failing to ensure the confidentiality, integrity, and availability (CIA) of Personally Identifiable Information (PII), such as PII, PHI, PIFI, and more. In today’s growing world of cyber security threats and ever-increasing reliance on information systems, the safety and security of PII is now more important than ever. Common risks would be for an organization to violate compliance regarding the safety and security of Personally Identifiable Information (PII), such as having exposed information to unauthorized parties, based on threats from malicious hackers, because of vulnerabilities from weak passwords for accessing systems. PII is a large risk for many financial services and consumer services companies, especially those having to comply with mandates such as Gramm Leach Bliley (GLBA) and other regulatory measures.

  Furthermore, while considered an actual subset of the broader domain of Personally Identifiable Information (PII), Protected Health Information (PHI) has gained much attention due in large part to the continued growth and awareness of the Health Insurance Portability and Accountability Act, simply known as HIPAA to all. More specifically, Covered Entities (CE) and Business Associates (BA) face tremendous risks arising from the failure to ensure the confidentiality, integrity, and availability of Protected Health Information (PII). Huge fines loom for data breaches of PHI, thus it’s critically important that healthcare organizations put in place comprehensive measures for protecting such information.

- **Cardholder Data Risk(s):** These are risks that arise from failing to ensure the confidentiality, integrity, and availability (CIA) of cardholder data in accordance with the Payment Card Industry Data Security Standards (PCI DSS). In today’s growing world of cyber security threats and ever-increasing reliance on information systems, the safety and security of cardholder data is now more important than ever.

- **Compliance Risk(s):** These are risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of internal operational, business specific, and information security policies, procedures, and processes. Regulatory compliance is a large and critically important element within risk management, requiring constant monitoring and oversight for ultimately ensuring adherence to numerous compliance mandates. Common compliance initiatives for which organizations should abide by, along with the numerous laws, legislative mandates, and industry specific requirements, include, but are not limited to, the following: Sarbanes-Oxley, HIPAA, HITECH, SOC 1 SSAE 18, SOC 2 and SOC 3 AT 101, GLBA, PCI DSS, and many others.

- **Reputation Risk(s):** These are risks arising from negative public perception and opinion for almost any imaginable reason, such as unethical business practices, data breaches resulting in loss of sensitive and confidential consumer information (i.e., Personally Identifiable Information - PII), investigations from regulators into questionable business practices, etc. It's important to note that in today's world of transparency and close media scrutiny, any perceived negative public opinion ultimately affects the reputation of any organization. The rise of social media and many non-traditional media outlets could spread a story, going "viral" in literally minutes.

- **Strategic Risk(s):** These are risks arising from the organization failing to implement business initiatives that align with its overall goals and ideas, such as not offering services that provide an acceptable return on investment, both short term and long term. Ultimately, when the long-term strategic vision of an organization is not clearly laid out and aligned, relevant risks begin to surface which can significantly impact the organization, often in a negative manner.

- **Operational Risk(s):** These are risks arising from a failed system of operational internal controls relating to personal and the relevant policies, procedures, processes, and practices. This becomes a large issue due to the fact the many organizations obviously rely heavily on their daily operational activities, thus a "breakdown" seriously impacts the organization, ultimately affecting productivity, workflow efficiency, and many other issues.

- **Transaction Risk(s):** These are risks arising from the organization failing to deliver as promised, such as product delivery, operational efficiency - or worse - unauthorized transactions and theft of information due to a weak system of operational and information security internal controls. An important component of mitigating such risks is having comprehensive, well-documented operational and information security policies, procedure, processes, and practices in place for guiding the organization on a daily basis.

- **Credit Risk(s):** These are risks arising from the financial condition of the organization, such as any "going concern" issues - a business that functions without the threat of liquidation for the foreseeable future, usually regarded as at least within 12 months. Not being able to meet routine expenses can result in large risks, along with a ceasing of operations because of credit risks, not being able to secure financial funding as needed, etc.

- **Country Risk(s):** These are risks arriving from the politic, economic, and social landscape - and other relevant events - within a foreign country that can impact the services being provided by an organization. Managing such risks can be extremely challenging and complex, especially when one considers the diverse political landscape in various regions around the globe. Legal issues also can pose significant country risks, as laws and regulations differ greatly from region to region.

- **Third Party Risk(s):** When using the services of various third-party outsourcing entities, a certain element of risk arises as responsibilities for critical initiatives are now in the hands of another organization. It's important to understand these risks, what they are, and how organizations can readily identify any issues, concerns, or constraints pertaining to these risks. Failure to mitigate and prevent these risks can result in significant financial loss, legal issues, and public opinion misconceptions, ultimately damaging the organization.

- **Interest Rate Risk(s):** These are risks arising from current and prospective risk to earnings or capital arising from movements in interest rates. Specifically, relevant interest rate risk(s) arises from differences between the timing of rate changes and the timing of cash flows (i.e., re-pricing risk), along with other relevant interest rate issues. **Please note:** "Interest Rate Risk(s)" is often a risk exhibited within the banking & financial services community, however, examining one's "Interest Rate Risk(s)", regardless of your industry, is a best practice that should be taken seriously. In essence, you can assess such a risk for its applicability directly to your industry, and ultimately, your organization.

- **Liquidity Risk(s):** These are risks arising from current and prospective risk to earnings or capital arising from an organization's inability to meet its obligations when they come due without incurring unacceptable losses. Additionally, liquidity risk includes the inability to manage unplanned decreases or changes in funding sources. Moreover, liquidity risk also can arise from the failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value. **Please note:** "Liquidity Risk(s)" is often a risk exhibited within the banking & financial services community, however, examining one's "Liquidity Risk(s)", regardless of your industry, is a best practice that should be taken seriously. In essence, you can assess such a risk for its applicability directly to your industry, and ultimately, your organization.

- **Legal Risk(s):** These are risks arising from all relevant contracts, lawsuits and/or adverse judgments, along with other related legal risks. In today's world of growing regulatory compliance mandates and legal complexities, legal risk(s) has become an important type of risk. It means ensuring all contractual documentation is in place, has been reviewed, favorable to your terms, etc.

- **Market Risk(s):** These are risks arising from changes in the market that can impact revenue, earnings, and ultimately, one's balance sheet and other applicable financial reports. **Please note:** "Market Risk(s)" is often a risk exhibited within the banking & financial services community, however, examining one's "Market Risk(s)", regardless of your industry, is a best practice that should be taken seriously. In essence, you can assess such a risk for its applicability directly to your industry, and ultimately, your organization.

Risk Assessment Personnel

It's also vitally important to identify relevant personnel responsible for assisting in all matters of the entire risk management lifecycle, particularly those involved in performing the numerous risk assessment activities. This ultimately requires input from a considerable number of personnel, ranging from senior management, I.T. individuals, and other select individuals. Risk management requires collaborative input by everyone to ensure all relevant risks are identified, assessed, and ultimately remediated as necessary. As a good rule of thumb, it's important to identify the risk assessment personnel as early as possible, assigning general roles and responsibilities for any number of activities that need to be undertaken.

Each phase within the entire risk management lifecycle – including the critically important risk assessment processes – needs to have personnel with clearly defined tasks and deliverables. After all, assessing risk is a project, no different than any other project where companies identify certain issues, tasks, roles, and responsibilities.

Risk management personnel assigned to perform that actual risk assessment for [company name] consist of the following:

Name	Role and Responsibility	Area of Subject Matter Expertise	Contact Information

Risk Treatment Strategies

After thoroughly assessing and identifying all risks, it's important to implement comprehensive risk treatment strategies for mitigating the risks to the lowest, acceptable level. It's therefore important to be practical in that completely removing the likelihood of an event occurring is near impossible in today's complex and ever-changing world, thus the goal is risk reduction. With that said, the four (4) primary risk treatment strategies generally consist of the following:

- **Risk Reduction:** Putting place all necessary practices for reducing the risk to its lowest, acceptable level, as just discussed.

- **Risk Sharing | Transfer of Risk:** In today's growing world of continued outsourcing, organizations can effectively share and transfer risk to other third parties. This type of risk treatment ultimately places a greater burden and responsibility on the actual third-party provider.
- **Risk Avoidance:** Simply not engaging in an activity or practice that would result in the actual risk to be present is another way of treating risk. Avoidance is obviously one the best risk treatment strategies, but unfortunately, it's not always very practical.
- **Risk Acceptance:** Simply accepting the risk because organizations tolerate the risk, or the financial and operational costs and constraints of ensuring the risk are greater than the risk itself, is another commonly used risk treatment strategy.

Risk Remediation Procedures

After successfully identifying the various risk treatment strategies, it's then vitally important to start implementing the necessary procedures. While some risk treatment strategies require essentially little to no procedural activities (i.e., "risk acceptance" – you're simply accepting risk), most require some type of process, such as authoring additional policies, making necessary operational and technical changes and modifications, etc. Ultimately, the decision on what remediation procedures to embark on should be based on several internal – and external – factors, for which your organization should have a strong understanding of.

Risk Reporting, Documentation, Communicating, and Information Sharing

Just as important in undertaking a risk assessment for [company name] is reporting the results, recommendations, and post risk assessment activities to be done. After all, what good is any type of risk analysis if there's no real communication link that exists throughout the organization for discussing the various components of risk management? Risk reporting should consist of providing all evidence to appropriate personnel, those with a true "need-to-know" function. Additionally, risk documentation should consist of highly formalized, easy-to-digest, read, and assess information that's not cumbersome and vague. It essentially entails open and transparent communication with all necessary parties, which is ultimately a large part of successful risk management. More specifically, it entails the following:

- **Risk Reporting:** Risk reporting requires comprehensive, objective, and detailed reporting of information regarding all elements of risk, and the associated threats, vulnerabilities, likelihood, impact, and other supporting information. Simply stated, it's about effectively documenting the entire risk management process, from beginning to end, complete with all necessary testing procedures. This documentation should be considered quite voluminous and used for authoring an abridged executive summary report to management.

- **Risk Documentation:** An output of the risk reporting process is often large amounts of documentation, for which organizations can then extract relevant points for creating an executive summary for management and other in-scope personnel. The executive summary should highlight critical issues regarding the broader subject of risk management, focusing on areas for removing risk from the organization.

- **Communication:** Effective communication means having all parties clearly aware of the issues, threats, challenges, and constraints presented because of the risk assessment process. It’s much more than just informing; it’s about making the right decisions in terms of mitigating risks to one’s organization. Lastly, it’s about getting everyone involved within the organization, as the topic of risk management is something every employee should be aware of.
- **Information Sharing:** Giving individuals the information they need for making informed decisions about risk is vital, and it’s why all parties need to have access to all relevant documentation. From the initial scope assessment as to what elements of risk are included in an annual risk assessment process – and many other pieces of data – people need to be able to always rely on in-depth and factual documentation. Simply stated, information sharing is a critical component of successful risk management.

Continuous Monitoring

As defined by the National Institute of Standards and Technology (NIST), information security continuous monitoring (ISCM) is “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.” [Company name]’s ISCM measures are to be standardized across the organization to the greatest extent possible to minimize use of resources and to maximize leveragability of security-related information. Upon analysis, the resulting information will inform the discrete processes used to manage the organization’s security posture and overall risk.

Furthermore, the ISCMP is to help provide situational awareness of the security status of the organization’s systems based on information collected from resources (e.g., people, processes, technology, environment) and the capabilities in place to react as the situation changes.[i]

Additionally, [company name]’s the ISCMP is to be well-devised and thoughtfully implement to help support risk-related decision-making at the organization level (Tier 1), the mission/business process level (Tier 2), and the information systems level (Tier 3).

- **TIER 1 – Organization:** Per NIST, “Security controls, security status, and other metrics defined and monitored by officials at this tier are designed to deliver information necessary to make risk management decisions in support of governance.”
- **TIER 2 – Mission/Business Processes:** Per NIST, “Tier 2 criteria for continuous monitoring of information security are defined by how core mission/business processes are prioritized with respect to the overall goals and objectives of the organization, the types of information needed to successfully execute the stated mission/business processes, and the organization-wide information security program strategy.”
- **TIER 3 – Information Systems:** Per NIST, “activities at Tier 3 address risk management from an information system perspective. These activities include ensuring that all system-level security controls (technical, operational, and management controls) are implemented correctly, operate as intended, produce the desired outcome with respect to meeting the security requirements for the system, and

continue to be effective over time. ISCM activities at Tier 3 also include assessing and monitoring hybrid and common controls implemented at the system level.”

[Insert Company Logo]

Risk Assessment Program [NIST RA-3]

Appendix A is a Microsoft Word document containing numerous sections that cover all "types" of risk categories. The purpose of providing such a comprehensive document is to allow you to pick and choose which types of risks you want to assess and evaluate within your entire risk management process. Performing a risk assessment *(annually or when circumstances arise that require a risk assessment to be performed)* is a strict requirement for NIST RA-3 within NIST SP 800-53, Revision. 5. *Additionally, you will need to determine what the scope of the risk assessment is – specifically – at the organization level, mission/business process level, or the information systems level, or some type of combination of the three (3) tiers just described.*

Most organizations will certainly not use all the risk tabs, but they've been provided to give you all the resources and options available for conducting the most comprehensive risk assessment possible.

There are essentially fifteen (15) different types of risks which any organization would encounter, regardless of industry, size, or location.

1. Information Security Risks
2. Privacy (PII & PHI) Risks
3. Cardholder Data Risks
4. Compliance Risks
5. Reputation Risks
6. Strategic Risks
7. Operational Risks
8. Transaction Risks
9. Credit Risks
10. Country Risks
11. Third-Party Risks
12. Interest Rate Risks
13. Liquidity Risks
14. Legal Risks
15. Market Risks

Appendix A: Risk Assessment

Scope of Risk Assessment

1. **Organization Level:** If the risk assessment is being performed at this level, then discuss accordingly.

2. **Mission/Business Process Level:** If the risk assessment is being performed at this level, then discuss accordingly.

3. **Information Systems Level:** If the risk assessment is being performed at this level, then discuss accordingly.

4. **Combination:** If the risk assessment is being performed is some type of combination of the above three (3) tiers, then discuss accordingly.

Identification of Assets

Identification of system assets is necessary for determining system threats, vulnerabilities, and risks, and the appropriate level of security to apply to the system and related system components. System asset identification includes the following:

- Identifying and documenting the system architecture.
- Identifying system and subsystem assets, including all hardware, software, and ancillary equipment.
- Identifying system interfaces (external and internal).
- Identifying system boundaries.

Key Terms

Vulnerability: A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. Remember that vulnerabilities are not just limited to information systems, as they can be found in operational activities, and many other areas throughout an organization. Vulnerabilities are often a direct result of a lack of, and or insufficient policies, procedures, processes, and other activities.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. The list of "threats" to use for purposes of this risk assessment include the following:

- Unauthorized Access
- Unauthorized Destruction
- Unauthorized Disclosure
- Unauthorized Modification of Information
- Information System Compromise
- Malicious Activity
- Information System Crime
- Other

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity:** Guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.
- **Availability:** Ensuring timely and reliable access to and use of information.

Risk Summary: The summary of the relevant findings of the risk in terms of Confidentiality, Integrity, and Availability.

Risk Likelihood: the likelihood is essentially the probability – and frequency – that the actual event would occur. Or, in more technical terms, according to the NIST publication, SP-800-30, Guide for Conducting Risk Assessments, it is *"…a weighted risk factor based on an analysis of a probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities)."* Additionally, it's important to note the "likelihood" is often expressed in terms of time – specifically – when will the event occur. As for assigning various degrees of "likelihood", the following are best practices:

- **0: No Event:** Event and associated threat is simply Not Applicable (N/A) to control environment.
- **1: Unlikely:** Rare degree of probability that the event will occur within the stated time period.
- **2: Possible:** Moderate degree of probability that the event will occur within the stated time period.
- **3: Likely:** High degree of probability that the event will occur within the stated time period.

- **4: Very Likely:** Very high degree of probability that the event will occur within the stated time period.
- **5: Event will Undoubtedly Occur:** Complete certainty that the event will occur within the stated time period.

Risk Impact Rating (LOW, MODERATE, or HIGH): Per the **United States Federal Information Processing Standards Publication 199 (FIPS PUB 199),** *"Standards for Security Categorization of Federal Information and Information Systems",* details the following three (3) security categories (i.e. "potential impact") that correspond to each one of the respective CIA objectives (confidentiality, integrity, and availability):

- **Impact: LOW**-The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a LIMITED adverse effect on the organization.
- **Impact: MODERATE**- The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a SERIOUS adverse effect on the organization.
- **Impact: HIGH**- The unauthorized disclosure, modification, destruction, deletion, and removal of information along with the disruption of access to information results in a SEVERE | CATASTROPHIC adverse effect on the organization.

Overall Risk Rating: The process of determining the overall risk rating and associated level of risk is a direct reflection of the likelihood that the event would occur, and the impact that it would have. From a matrix perspective, overall risk, one that assigns a risk rating and level of risk, is best expressed in the following manner:

	OVERALL RISK RATING | LEVEL OF RISK			
		IMPACT		
		Low	Moderate	High
Likelihood	Event will Undoubtedly Occur	Medium Risk	High Risk	High Risk
	Very Likely			
	Likely		Medium Risk	
	Possible	Low Risk		
	Unlikely		Low Risk	Medium Risk
	No Event			Low Risk

Risk Category: Information Security						
Information Security Risks are risks arising from inadequate, insufficient, and missing information security policies, procedures, and processes relating to the broader element of information technology within an organization. ***More specifically, according to NIST, "Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interest...."*** **Source:** http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf						
1. **Asset Inventory** – A comprehensive and complete listing and description of the organization's assets, which includes all computing devices, information technology (IT) systems, IT networks, IT circuits, software (both installed instances and a physical instances), virtual computing platforms (common in cloud and virtualized computing), and related hardware (e.g. locks, cabinets, keyboards) ***exists***, and is updated for ensuring it's kept current and accurate.						
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
2. **Intellectual Property** – A comprehensive and complete listing and description of technology related copyrights, trademarks, patents, trade secrets, independent discovery, etc., ***exists***, and is updated for ensuring it's kept current and accurate.						
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
3. **Network Topology –** A comprehensive and complete set of network topology (LAN, WAN, etc.) drawings, and other supporting documents, ***exists***, and is updated for ensuring it's kept current and accurate.						
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations	Choose an item.

choose the primary threat, and then list secondary threats here: 1. 2. 3.					needed for remediating the control that is applicable to the vulnerability.	
4.	**Network Security (Policies and Procedures)** – A comprehensive set of network security policies and procedures regarding the organization's entire information system landscape, ***exists***, and is updated for ensuring it's kept current and accurate.					
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
5.	**Network Security (Firewalls)** – Firewalls are in place and utilized for protecting the organization's network.					
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
6.	**Network Security (Routers, Switches, Load Balancers, other)** – Routers, switches, and load balancer are in place and utilized for protecting the organization's network.					
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.

7.	**Network Security (Additional Network Security Utilities)** – Any additional network security utilities and devices are in place and utilized for protecting the organization's network.					
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
8.	**Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)** – Network based Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) are in place and utilized for protecting the organization's network.					
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
9.	**Data and Information Classification (Policies and Procedures)** – A comprehensive and complete listing and description of the organizations classification levels for all data, ***exists***, and is updated for ensuring it's kept current and accurate.					
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
10.	**Physical and Environmental Security (Secure Area) –** Computer rooms, cages, cabinets, or other designated, secured areas, are utilized for securing information systems and other relevant assets.					
Choose an item.	Provide details as to the overall risk	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control	Choose an item.

What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	summary if such vulnerabilities are not corrected.				status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	
11. **Physical and Environmental Security (Access Control) –** Access control mechanisms (i.e., traditional lock and key, and/or electronic access control systems (ACS), such as badge readers and biometric recognition (i.e., iris, palm, fingerprint scanners/readers), are utilized for helping to ensure only authorized personnel can access critical information systems.						
Choose an item. What type of "Threat" is the organization currently susceptible to "IF" the control is not in place? [Choose from the drop-down list]. If you need to choose more than one, then choose the primary threat, and then list secondary threats here: 1. 2. 3.	Provide details as to the overall risk summary if such vulnerabilities are not corrected.	Choose an item.	Choose an item.	Choose an item.	Provide details as to the current control status applicable to the vulnerability AND Provide details as to the relevant recommendations needed for remediating the control that is applicable to the vulnerability.	Choose an item.
12. **Physical and Environmental Security (Monitorin** [illegible] **S** [illegible] clo [illegible] nito [illegible] ., CCTV) and other as-needed monitoring devices, are utilized for helping ensure the safety and security [illegible] set [illegible]						