sifma

Internal Auditors Society

Leading Practices in Auditing Cyber Security

December 2017

The Audit Guidelines (the "guidelines") are intended to provide members of the Internal Auditors Society ("IAS"), a society of the Securities Industry and Financial Markets Association ("SIFMA"), with information for the purpose of developing or improving their approach towards auditing certain functions or products typically conducted by a registered broker-dealer. These guidelines do not represent a comprehensive list of all work steps or procedures that can be followed during the course of an audit and do not purport to be the official position or approach of any one group or organization, including SIFMA, or any of its affiliates or societies. Neither SIFMA, nor any of its societies or affiliates, assumes any liability for errors or omissions resulting from the execution of any work steps within these guidelines or any other procedures derived from the reader's interpretation of such guidelines. In using these guidelines, member firms should consider the nature and context of their business and related risks to their organization and tailor the work steps accordingly. Internal auditors should always utilize professional judgment in determining appropriate work steps when executing an audit. Nothing in these guidelines is intended to be legal, accounting, or other professional advice.

Background

Cyber related incidents represent a growing threat to the reputation and economic stability of financial institutions. The types of threats financial organizations face today are far more sophisticated, pervasive and coordinated than in the past. Increasingly, threat actors from organized crime and hacktivists to nation-states and malicious insiders, use targeted, advanced and evasive strategies and tactics to perpetrate cyber-crimes that can result in reputational, financial, and regulatory impacts. In response to these challenges, SIFMA IAS has developed Cyber Security Audit Guidelines based largely on the National Institute of Standards and Technology (NIST) Framework. In accordance with the Presidential Executive Order 13636, the NIST organization utilized a year-long consultative process with stakeholders to create the Framework for Improving Critical Infrastructure Cybersecurity (the Framework). Released in February 2014, the Framework consists of a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. Recently, the May 2017 Presidential Executive Order was issued to strengthen Federal Networks and Critical Infrastructure following NIST.

Risk Management

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. Armed with this information, organizations can determine the acceptable level of risk, expressed as their risk tolerance. With an understanding of risk tolerance, organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. All types and sizes of organizations are at risk, not only the financial services firms, defense organizations and high profile names which make the headlines.

The risks and opportunities which digital technologies, devices and media bring us are numerous. Cyber risk is never a matter purely for the technology teams, although they clearly play an important and vital role. An organization's risk management function needs a thorough understanding of the constantly evolving risks as well as the practical tools and techniques available to address them. Currently, many public, private and corporate organizations are adopting the NIST Risk Management Framework. The framework includes nine key risk and security life cycle elements aimed at managing risks resulting from the operation of internal and public facing information systems: categorize, select, refine, document, implement, assess, determine, authorize and monitor.

Regulatory Landscape

Cyber threats and risk management have been a persistent and current regulatory focus in recent times, with US financial services regulators including FINRA, FDIC, FRB, SEC, OCC and NY State (DFS) issuing recent bulletins. Outside the US, several countries have enacted cyber laws with enforcement by local, regional and national regulators, some key examples include:

- UK - Financial Conduct Authority
- EU - NIS and 95/46/EC Directives
- Privacy Commission of Canada
- France - CNIL and Data Protection Act
- Germany - BaFin and IT Security Act
- Estonia - Information Systems Authority
- UAE - Telecomm Regulatory Authority
- India - IT Act and Privacy Laws
- China - National Security Law
- Japan - Ministry of Trade and Industry
- Singapore - Computer Misuse and Cybersecurity Act
- Australian - Information Commission

Audit Coverage

Due to the complexity of regulations and cyber-related risks a comprehensive framework is needed to ensure adequate coverage in this very challenging area. As such, the following audit guidance will be based primarily on the NIST Cybersecurity Framework and supplemented by various other practices, guidelines and directives, such as Cobit 5, ISO 27001 Annex A and SANS Critical Controls which are pertinent to the securities and financial services industry.

The purpose of this document is to provide guidance in covering cyber risk within your organization. For financial institutions with large global networks and technology infrastructures, it would be very challenging to cover cyber risk within one audit or auditable entity. Accordingly, large and medium size firms should consider the areas below as separate audits or auditable entities and provide assurance according to a rotational or risk-based coverage model. For smaller firms, electing to cover cyber risk as one audit or auditable entity, the areas below should be considered as key coverage areas within the scope of the review, and audited on a frequency commensurate with level of risk within the organization.

Core Function	**Auditable Entities/ Auditable Processes/ Audits**
IDENTIFY	IT Asset Risk Assessment and Inventory Management Systems Development and Project Management Third Party Assessments and Third Party Connections IT Governance, Policies, Procedures and Standards IT Risk Management and Risk Assessment
PROTECT	Access, Identity and Highly Privileged Account (HPA) Management Information Security Practices Data Security and Data Leakage Protection Network Architecture, Design, Engineering Network Security / Perimeter Security Patch Management Change Management
DETECT	Threat Intelligence Management Malware and Anti-Virus
RESPOND	Incident Response Planning and Management Legal/ Compliance/ Regulatory and Public Disclosure
RECOVER	Business Continuity Disaster / Event Recovery

It is recognized that different audit organizations may follow particular IT and cyber coverage models (such as the NIST Framework, Cobit 5, ISO 27001 Annex A, SANS Critical Controls). As such, the auditable areas mentioned above are further explained and mapped (see Appendix A) to help rationalize coverage for your individual organization.

Detailed Audit Examination Procedures

The objective of this document is to convey guidance in covering cyber risk within your organization. The guidance does not provide detailed audit examination procedures. However, within Appendix A, examination guides are referenced. Some of the commonly used cyber examination guides and tools include:

- FFIEC examination guide
- FFIEC Cyber assessment tool
- FSSCC Cybersecurity assessment tool
- SEC OCIE Cybersecurity examination initiative
- SEC OCIE national examination program priorities

Cyber Incident resulting in a Data Privacy Breach

Multiple US federal and state, as well as international, laws and regulations, require legal assessment as to whether a particular law or regulation may be implicated in any security incident. In addition, it has become commonplace for contractual counter-parties to require adherence to laws, regulations, or best practice standards pursuant to contract terms. Laws and regulations mandate a wide variety of controls and many require notifications to various constituents depending on whether the security incident triggers the respective reporting requirements. Often, this analysis turns on whether the security incident satisfies the applicable laws' or regulations' legal definition of a "breach." Examples of laws and regulations often reviewed by legal counsel are Graham-Leach Bliley Act, HIPAA, and state privacy laws. Additionally, industry standards (such as the Payment Card Industry Data Security Standard (PCI DSS)) and international laws and regulations (such as the European Union's long-awaited General Data Protection Regulation (GDPR) are often reviewed. Importantly, data breach notification requirements may require notifying various constituents, such as consumers, investors, contractual counter-parties, regulators, and law enforcement (such as U.S. states' attorneys general).

Recently, data breach notification regulations have proliferated in the U.S., with increasing stringency, complexity and ambiguity. The New York Department of Financial Services recent proposal for a cyber regulation exemplifies the complexity for industry to remain legally compliant with the patchwork of regulations. If a "breach" is determined, notification to regulatory authorities and affected individuals may be required, and the organization's compliance with the applicable legal standards may be challenging since timelines and thresholds that trigger data breach notifications vary among U.S. states. Thus, an organization should stay apprised of the rapidly changing regulatory landscape in the U.S. and elsewhere impacting, and at times dictating, reasonable security protocols and controls.

Leading Practices in Auditing Cyber Security – Appendix A – Coverage Models

Core Function	Auditable Entities/ Audit Processes/ Audits	NIST Categories (22)	Key Cobit 5.0 Processes (37 total)	ISO 27001 Annex A (14 controls / safeguards)	SANS CIS 20 Critical Controls
IDENTIFY	IT Asset Inventory, Mgmt and Risk Assessment Systems Development and Project Management 3rd Party Assessments & 3rd Party Connections IT Governance, Policies, Procedures, Standards IT Risk Mgmt and Risk Assessment	Asset Management (ID.AM): 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 business objectives and the organization's risk strategy.	BAI09 Manage Assets	A.8 Asset management	1: Inventory of Authorized and Unauthorized Devices 2: Inventory of Authorized and Unauthorized Software
		Business Environment (ID.BE): 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.	BAI01 Manage Programs and Projects BAI02 Manage Requirements Definition BAI05 Manage Organizational Change Enablement DSS06 Manage Business Process Controls	A.7 Human Resources Security A.14 System, acquisition, development and maintenance A.17 Info security aspects of business continuity mgmt	18: Application Software Security
		Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	EDM01 Ensure Governance Framework Setting and Maintenance	A.5 Information security policies A.6 Organization of information security A.18 Compliance	
		Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	AP010 Manage Suppliers MEA02 Monitor, Evaluate and Assess the System of Internal Control MEA03 Monitor, Evaluate and Assess Compliance with External Requirements	A.15 Supplier relationships	17: Security Skills Assessment and Training to Fill Gaps

		Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	EDMO3 Ensure Risk Optimization APO12 Manage Risk	A.18 Compliance	20: Penetration Tests and Red Team Exercises
		Supply Chain Risk Management (ID SC): The organizations priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. Processes are in place to identify, asses and manage supply chain risk.	APO10 Manage Suppliers	A.15 Supplier relationships	
PROTECT	Access, Identity and HPA Mgmt Information Security Practices Data and DLP Security Network Architecture, Design, Engineering Network Security / Perimeter Security Patch Management Change Management	Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	APO13 Manage Security	A.9 Access control A.11 Physical and environmental security	3: Secure Configurations for HW and SW on Mobile Devices, Laptops, Workstations, Servers 5: Controlled Use of Administrative Privileges 7: Email and Web Browser Protections 8: Malware Defenses 9: Limitation and Control of Network Ports, Protocols, and Services 10: Data Recovery Capability 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches 12: Boundary Defense 13: Data Protection 14: Controlled Access
		Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	DSS05 Manage Security Services	A.6 Organization of information security	
		Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	APO13 Manage Security DSS05 Manage Security Services APO10 Manage Suppliers	A.12 Operational security A.15 Supplier relationships	
		Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and	DSS05 Manage Security Services	A.5 Information security policies	

		procedures are maintained and used to manage protection of information systems and assets.			Based on the Need to Know 15: Wireless Access Control 17: Security Skills Assessment and Training to Fill Gaps 18: Application Software Security
		Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	BAI06 Manage Changes	A.14 System, acquisition, development and maintenance	
		Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	APO03 Manage Enterprise Architecture BAI10 Manage Configuration	A.10 Cryptography A.13 Communications security	
DETECT	Threat Intelligence Mgmt Malware and Anti-Virus	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.	DSS05 Manage Security Services	A.16 Info security incident management	4: Continuous Vulnerability Assessment and Remediation 6: Maintenance, Monitoring, and Analysis of Audit Logs 12: Boundary Defense 16: Account Monitoring and Control 19: Incident Response and Management 20: Penetration Tests and Red Team Exercises
		Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	DSS05 Manage Security Services	A.16 Info security incident management	
		Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	DSS04 Manage Continuity	A.16 Info security incident management	
RESPOND	Incident Response Planning and Mgmt Legal/ Comp Regulatory and Public Disclosure	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	DSS02 Manage Service Requests and Incidents DSS03 Manage Problems	A.16 Info security incident management	4: Continuous Vulnerability Assessment and Remediation 6: Maintenance, Monitoring, and Analysis of Audit Logs
		Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to	DSS02 Manage Service Requests and Incidents	A.16 Info security incident management	

		include external support from law enforcement agencies.	DSS04 Manage Continuity		19: Incident Response and Management
		Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	DSS03Manage Problems	A.16 Info security incident management	
		Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	DSS02 Manage Service Requests and Incidents	A.16 Info security incident management	
		Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	DSS03Manage Problems	A.16 Info security incident management	
RECOVER	Business Continuity Disaster / Event Recovery	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	DSS04 Manage Continuity	A.17 Info security aspects of business continuity mgmt	10: Data Recovery Capability
		Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	DSS04 Manage Continuity	A.17 Info security aspects of business continuity mgmt	
		Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	DSS04 Manage Continuity		

Function	Key Business Objectives	Inherent Risks	Risk Ranking (H, M, L)	Audit Objectives	Audit Procedures
Identify (ID)	**1. Asset Management:** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistently with their relative importance to business objectives and the organization's risk strategy.	Poor asset management may lead to failed strategic business initiatives, IT inventory loss, improper implementation of decisions, non-compliance with laws, regulations, internal policies and procedures, contractual arrangements, or ethical standards.	High	**1a. IT Asset Inventory** Verify that physical devices, systems, software platforms and applications within the organization are inventoried.	1. Confirm the entity maintains IT asset inventory listings for physical devices, systems, software platforms and applications and that the listings contain relevant details, e.g., software version, server name, server location, IP address, network segment, owner, etc. 2. Confirm whether the organization uses an automated asset inventory discovery tool to build a preliminary inventory of systems connected to its public and private networks. 3. Determine whether equipment acquisitions are automatically updated in the organization's inventory system as new and approved devices are connected to the network. 4. Validate whether the asset inventory is maintained, reviewed, and updated as needed throughout the asset lifecycle (e.g., when assets are disposed of or when new assets are added). Verify that the asset inventory also tracks mobile phones, tablets, laptops, and other portable electronic devices that store or process the entity's data. 5. Determine how the entity identifies IT assets that should not be on the network, e.g., incorrect or obsolete versions of software, unlicensed software, etc.

				1b. Data Classification Verify that data classification is integrated into information risk management policies and procedures.	1. Confirm the entity has documented and implemented a formal information asset or data classification policy that includes the classification of data according to sensitivity and other pertinent details, e.g., location and ownership of information assets classification of data according to sensitivity. 2.Inquire and obtain the Data Classification Policy/Process/Procedure to determine if classification schemes and procedures for handling, processing, storing and communicating information are consistent with its classification, criticality, and business value and if they are documented and approved.
				1c. Cybersecurity Roles & Responsibilities Verify that cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., customers, vendors, third-party service providers) are established.	1. Confirm that cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., customers, vendors, third-party service providers) are established and periodically reinforced.

	2. Governance: The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Failure to establish corporate governance may lead to lack of communication, unstructured reporting hierarchy, insufficient control environment, non-compliance with laws, regulations, internal policies and procedures, financial loss, and reputation damage.	High	**2a. Corporate Governance & Reporting Structure** Assess whether corporate governance is established for organization, management, and reporting structure for cybersecurity related issues, including the interaction between information security and core business functions.	1. Confirm that there information/cyber security roles and responsibilities are established for the entire workforce, including board or senior management support for cybersecurity program, and that information security roles and responsibilities are coordinated and aligned with internal roles and external partners. 2. Confirm that the organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program. 3. Confirm that the head of Cyber Sec reports into the CRO or the COO independent of the CTO for proper Segregation of Duties 4. Confirm that a reporting structure exists for managing cybersecurity related issues including the interaction between information security and business functions. 5. Confirm that legal and regulatory requirements regarding cybersecurity including privacy and civil liberties obligations are understood and managed.

				2b. Cybersecurity Policies Assess whether written cyber/information security policies and procedures are designed to address the security goals of confidentiality, integrity, and availability and on the entity's information systems and are periodically reevaluated in light of changing risks, and resources are devoted to information security and overall risk management.	1. Confirm that there is a comprehensive cybersecurity / information security program that is formally documented and periodically reviewed and updated if required. 2. Confirm that the information security policies and procedures address the security goals of confidentiality, integrity, and availability. 3. Security policies and operational procedures should address organization-determined areas and best practices; examples include: - Business Continuity/ Disaster Recovery; - Data Protection/ DLP; - Access Management; - Vendor Management; - Physical Security; - SDLC; - Security Awareness training; - Mobile device management; - Legal/regulatory requirements; - System/ service acquisition; - User agreements. - Incident Management - Network Security - Configuration Management - Application Security - Cryptography and Key Lifecycle Management - Risk Assessment and Treatment - Data confidentiality, integrity and availability across multiple system interfaces, jurisdictions, business functions

				2c. Acceptable Use Policy Assess whether policies for acceptable use of information technology assets have been established, made accessible to personnel, and are reviewed/updated at least annually.	1. Determine whether a description of the systems and services had been prepared and communicated. 2. Inspect the policy and code of conduct obtained to determine whether it includes rules for acceptable use of information and assets associated with information processing facilities, including mobile computing devices, where applicable, and requires explicit approval from authorized parties to use the technologies. 3. Inspect documents on the organization internal network, or other supporting documentation, to determine whether the policy is made available to employees. 4. Review policies and procedures to confirm they are reviewed/updated at least annually or more frequently if required based on changes in the environment.
				2d. Bios and Job Descriptions Assess whether biographies/resumes and job description of the current Chief Information Security Officer or the individual otherwise responsible for information security, including individual's information security training and experience and all reporting lines for that individual (e.g., all committees and managers), is available.	1. Confirm that the CV and job description of the current Chief Information Security Officer or the individual otherwise responsible for information security, including individual's information security training and experience and all reporting lines for that individual (e.g., all committees and managers), is available.

				2e. Organization Chart Assess whether a current organization chart for the IT and information security functions is available and that the information security function is adequately staffed.	1. Confirm that the IT organization chart is maintained for IT and information security functions. 2. Confirm that there are dedicated and adequately trained resources in information security roles and overall risk management.
	3. Business Environment: 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.	There may be a lack of prioritization of organizational mission, objectives, or activities, and identification of critical functions for delivery of products and services.	Medium	**3a. Organizational Objective Priorities** Verify that priorities for organizational mission, objectives, and activities are established and communicated.	1. Confirm that mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, and other organizations, are defined. 2. Confirm that mission, priorities, and objectives are communicated to operational and business areas and determine fit within critical infrastructure and its dependencies, critical functions and resilience requirements for the protection and delivery of its core services.
				3b. Supplier Management Verify that a formal supplier management program exists. The supplier services have been identified and classified based on service type, criticality, and inherent risk.	1. Confirm that a formal supplier management program exists and whether an inventory of suppliers is maintained. 2. Confirm that suppliers are classified based on criticality, service type, and inherent risk. 3. Confirm that there is a formal process to evaluate and select suppliers.

				3c. Contract Management Verify that contracts are in place detailing the roles and responsibilities of each party, including information security requirements, confidentiality/non-disclosure agreements, obligations, and the obligations of employees and subcontractors.	1. Confirm that all relevant information security requirements are established and agreed with each supplier/ vendor that may access, process, store, communicate, or provide IT infrastructure components for the organization's information. 2. Confirm that contracts between the organization and any subcontractors establish the procedure and time periods for the organization to notify the customer of any legally binding request for disclosure of PII by a law enforcement authority, unless such a disclosure is otherwise prohibited. 3. Confirm that the organization reviews any changes to customer services on an ongoing basis and conducts a risk assessment, if needed, and updates contractual provisions to align with the changes.
				3d. Third-Party Service Providers Due Diligence Process Verify that an information security third-party service provider due diligence process is in place and used in vetting, selecting, and monitoring third-party service providers, vendors and suppliers.	1. Identify the third-party service providers for entity and related risk ranking assigned by entity. 2. Confirm that an information security third-party due diligence process is in place and used in vetting, selecting, and monitoring third-party service providers.

				3e. Inventory of Third Parties Verify that a formalized list of all third parties is in place and includes the vendors criticality level, annual spend, and contracted services/application and that the list is reviewed and updated as needed.	1. Confirm that the organization maintains a list of all third party service providers and a description of the services they provide. 2. Inspect the third party service provider list to determine if it is available, maintained, and includes appropriate details on the services the third party provides including: - vendors criticality level - annual spend - contracted services/application. 3. Inquire whether the list is reviewed and updated as needed.
				3f. IT Portfolio Changes Verify that significant changes to the organization's IT portfolio resulting from mergers, acquisitions, or addition of new business lines and products are understood and managed.	1. Confirm whether changes were made to the business portfolio in the last 24 months. 2. Verify the new applications added to the IT inventory to service the new business portfolio.
	4. Risk Assessment: The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Failure to complete an accurate risk assessment may lead to an ineffective identification of risk and an insufficient control environment resulting in possible regulatory action and/or damage to the reputation.	Medium	**4a. Risk Assessment** Threats, vulnerabilities, likelihoods, and impacts are assessed as part of a comprehensive Risk Assessment	1. Verify that the organization has a formally documented risk assessment methodology that is reviewed and maintained and the criteria for risk acceptance is established. 2. Verify that security threats and vulnerabilities have been identified and documented. Periodic information security risk assessments (at least annually or upon changes to the environment) are conducted to identify, quantify, and prioritize relevant threats and vulnerabilities based on their likelihood and impact to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. 3. Verify the entity performs annual Threat and Vulnerability Assessments from an internal and

					external perspective. 4. Verify the entity performs annual penetration tests of the internal and external network
				4b. Shared Infrastructure Risks Assess whether the risks posed by shared infrastructure are managed.	1. Assess adequacy of risks posed by shared IT infrastructure are managed.
					2. Confirm that threats, vulnerabilities, likelihood, and impacts are used to determine risk.
					3. Confirm that risk responses are identified and prioritized.
				4c. CIA Threats Assess whether threats to confidentiality, integrity, and availability of personal and confidential information, both internal and external, are identified and documented.	1. Confirm that threats to confidentiality, integrity, and availability of personal and confidential information, both internal and external, are identified and documented.
	5. Risk Management: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Failure to establish risk management priorities, constraints, risk tolerances and assumption may lead to project failure, information security and cybersecurity	High	5a. Risk Management Strategy: The organization has developed and implemented a comprehensive strategy to manage enterprise risk in alignment with its established level of risk tolerance.	1. Verify that risk strategies are updated as needed. Determine if the information security strategy outlines the initiatives required to achieve security objectives, resources and budget required, associated roles and responsibilities, timelines for completion, and key metrics for evaluation of success of the security strategy. Verify that the strategy is

		related issues, and non-compliance with regulations.			aligned with the security objectives, takes into account results of the risk assessment, and is periodically updated and communicated to key stakeholders.
				5b. Risk Tolerance: Organizational risk tolerance is determined and clearly expressed.	1. Determine whether the organization evaluates the external environment, internal environment, its role in the critical infrastructure, business objectives, and sector specific risks, while determining risk tolerance. 2. Determine whether risk tolerance is considered while designing business processes. 3. Understand mechanisms in place to incorporate risk tolerance while defining business processes. 4. Determine how information protection needs for defined mission/business processes are developed based on risk tolerance and how business processes are revised until the risk tolerance levels are achieved.
				5c. Key Metrics Key goals and metrics of risk management processes are monitored.	1. Determine whether KPIs/KRIs have been defined to monitor cybersecurity processes and whether KPI/KRIs are generated using automated/manual mechanisms. 2. Confirm that Management periodically reviews KPI/KRI dashboards and provides guidance on managing deviations. 3. Confirm that corrective actions taken are reviewed for effectiveness.

				5d. Insurance Coverage and Third-Party Protections Assess whether cybersecurity insurance coverage and other third-party protections are in place.	1. Confirm that cybersecurity insurance coverage and other third-party protections are in place.
				5e. Legal and regulatory requirements regarding intellectual property rights, use of proprietary software, and cybersecurity, including privacy and civil liberties obligations, are understood and managed.	1. Confirm that all relevant legislative, statutory, regulatory, contractual obligations and intellectual property rights, along with the organization's approach to meeting these requirements are explicitly identified, documented and updated for each information system and the organization. 2. Determine whether appropriate procedures are implemented to maintain ongoing awareness and incorporation of legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products to the organization's processes.
				5f. Regulatory Exam Issue Follow-up Verify that previously identified issues (Regulatory Examinations) have been reviewed and resolved.	1. Review recent regulatory exams and identify any relevant issues to this audit for further follow-up.
				5g. Prior Audit Issue Follow-up Verify previously identified issues (Internal/External Audits) have been reviewed and resolved.	1. Review recent audit reports and prior audit reports issued that are related to this audit and identify any relevant issues to this audit for further follow-up.
Protect (PR)	**6. Access Control:** Access to assets and associated facilities is limited to authorized	Failure to establish effective identity and access management systems may lead to	High	**6a. Identity Management** Verify that identities and credentials are managed for authorized devices and users,	1. Assess adequacy of user authentication policies and procedures including password parameters, default passwords, and periodic password changes.

	users, processes, or devices, and to authorized activities and transactions.	unauthorized access, data loss, financial and non-financial damages.		including timely deprovisioning of devices and accounts for terminated users.	2. Confirm that procedures and standards for user access administration (including additions and deletions) are in place, and user access is periodically reviewed to confirm appropriateness.
				6b. Access/Privilege Management Verify that access permissions are managed, incorporating the principles of least privilege and separation of duties, including administrative access to applications, operating systems, and databases.	1. Confirm that procedures and standards are in place to restrict and properly control the use of generic users.
					2. Confirm that administrative, super-user and privileged accounts to the network domain and applications are appropriate.
					3. Confirm that segregation of duties is controlled and monitored.
					4. Review the administrative, super-user and privileged accounts to the network domain and key applications to confirm effectiveness of access/privilege management.
				6c. Physical Access Management Verify that physical access to assets is managed and protected.	1. Confirm that physical access to assets including critical computer equipment facilities and office building is restricted to authorized personnel and is appropriately controlled.
				6d. Remote Access Management Verify that remote access is managed (e.g., multi-factor authentication for systems and applications).	1. Confirm that remote data access and wireless policy including multi-factor authentication for systems and applications are in place.
				6e. Network Integrity Verify that network integrity is protected, incorporating network segregation where appropriate.	1. Confirm that network integrity is addressed in the information security policies and procedures, and network segregation is incorporated where appropriate.
	7. Awareness and Training: The organization's personnel and partners	Failure to adequately train employees may compromise the quality of Information	High	**7. Awareness and Training** Evaluate that security awareness and training programs are established for	1. Confirm that security awareness and training programs are established for users, information security professionals, and other personnel.

	are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	Security's reviews, examinations and surveillance. This may result in human errors and lead to non-compliance with policies and regulations.		users, information security professionals, and other personnel.	2. Confirm that roles and responsibilities are established regarding information security and cybersecurity training programs. 3. Obtain training materials, logs (attendance sheets), and memos to confirm awareness and training compliance.
	8. Data Security: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Information and records may not be protected from intrusion. Critical data leaks may cause financial loss, reputation damage, and non-compliance with policies and regulations.	High	**8a. Data Security** Verify that protections against intrusion are in place (e.g., multi-factor or adaptive authentication, intrusion prevention systems (IPS), server and database configuration baseline changes).	1. Confirm that protections against intrusion are addressed in the information security program, including multi-factor or adaptive authentication, intrusion prevention systems (IPS), and server and database configuration baseline changes. 2. Confirm that intrusion prevention systems are in place. 3. Obtain firewall policy, management interface, and configuration to confirm the existence and functionality of firewall. 4. Obtain anti-virus software license and configuration to confirm that endpoints have the anti-virus client installed and properly configured.
				8b. Data Encryption Verify that encryption technologies are in place to protect data-in-transit and data-at-rest, including backups.	1. Confirm that encryption technologies are in place to protect data-in-transit and data-at-rest.
				8c. Protection against Data Leaks Verify that protections against data leaks are implemented.	1. Confirm that protections against data leaks are addressed in the information security program and implemented.

				8d. Privileged User Monitoring Verify that activities of privileged user accounts are logged and monitored for unusual activity.	1. Confirm that audit logs of privileged users on key applications are in place and periodically reviewed for unusual or suspicious activity.
				8e. Key Management Verify that cryptographic keys for required cryptography employed within the information system are managed.	1. Confirm that cryptographic keys and privileged passwords are adequately managed.
	9. Information Protection Processes and Procedures: 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.	Security and other IT policies, processes, and procedures may not be documented, current, or adequate to protect and manage information systems.	Medium	**9a. Business Continuity and Disaster Recovery (BC/DR) Plan** Assess whether information security is integrated into business continuity and disaster recovery (BC/DR) plan, the BC/DR plan is tested at least annually, and the BC/DR plan has been updated to address cyberattacks.	1. Confirm that Business Continuity / Disaster Recovery (BC/DR) policies and procedures are in place, and addresses information security. 2. Confirm that the BC/DR plan is tested at least annually, and has been reviewed/updated.
				9b. System Development Life Cycle (SDLC) Assess whether secure system development life cycle (S-SDLC) standards, including assessment and incorporation of security and privacy requirements into the SDLC process, are established.	1. Confirm that secure system development life cycle (S-SDLC) standards are in place, and the SDLC process incorporates security and privacy requirements.
				9c. Change Management Assess whether changes management policies and procedures are established and consider information security impact of changes.	1. Confirm that changes management policies and procedures are in place.

				9d. Patch Management Verify that a patch management program is established and includes how updates, patches, and fixes are obtained and disseminated, whether processes are manual or automated, and how often they occur.	1. Confirm that a patch management program including how updates, patches, and fixes are obtained and disseminated, whether processes are manual or automated, and how often they occur, is in place.
					2. Obtain the Microsoft Baseline Security Analyzer (MBSA) or equivalent report to confirm patch levels.
				9e. Back-ups Assess whether backups of information are conducted, maintained, and tested periodically.	1. Assess adequacy of backup and restoration strategies.
					2. Review the backups of key applications to confirm effectiveness of back-up management.
				9f. Decommission and Destruction Policies and Procedures Assess whether decommissioning and destruction policies and procedures exist to securely remove and destroy information based on sensitivity of data and type of various mediums (e.g., paper, tapes, disks, hard drives, mobile devices, etc.).	1. Confirm that decommission and destruction policies and procedures are in place to securely remove and destroy information based on sensitivity of data and type of various mediums (e.g., paper, tapes, disks, hard drives, mobile devices, etc.).

				9g. Cybersecurity in Human Resources Assess whether cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	1. Confirm that cybersecurity is included in human resources policies and procedures (e.g., deprovisioning and personnel screening). 2. Confirm whether the organization conducts a background investigation for new employees and employment is contingent on successfully completing the background check. This should include all locations and employees, such as the data center facility and all third-party personnel. The background checks must include at a minimum: criminal background check, education verification, employment verification. 3. Confirm whether the Code of Conduct and Employee Handbook are published and available to personnel on the company portal, outline how the company and its subsidiaries conduct business, describe the company's shared values, and describe responsibilities and expected behavior regarding system usage.
				9h. Removable Media Assess whether removable media is protected and its use restricted according to policy.	1. Confirm that protections and restricted usage of removable media are addressed in the information security policy.
	10. Maintenance: Maintenance and repairs of information system components is performed consistent with policies and procedures.	Failure to establish a vulnerability management plan, a patch management program, or maintenance of organizational assets may lead to unauthorized access and other security issues for the OS,	High	**10a. Change Management** Verify that changes to application programs, system software and infrastructure are subject to formal policies.	1. Confirm that a vulnerability management plan, as applicable to servers, endpoints, mobile devices, network devices, systems, and applications, is in place.
				10c. Maintenance and Repair Verify that requests for maintenance and repair of organizational assets (i.e., applications and infrastructure) are logged, tested, and	1. Review a sample of maintenance and repair requests of organizational assets along with the IT tickets/change management forms to confirm that they were logged, tested, and approved prior to migration into production.

		applications, network devices, hardware, etc.		approved prior to migration into production.	
				10d. Remote Maintenance Verify that remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	1. Confirm that policies and procedures are in place for remote maintenance of organizational assets.
					2. Select a sample of remote maintenance of organizational assets approvals/logs along with the IT tickets/change management forms to confirm that they were approved, logged, and performed in a manner that prevents unauthorized access.
Detect (DE)	**11. Detection:** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	Intrusion detection and monitoring processes and procedures may not provide effective parameters to detect intrusion, and penetration testing may not identify vulnerabilities in systems and applications.	High	**11a. Intrusion Detection Systems (IDS)** Verify that intrusion detection systems (IDS) are in place to monitor the network to detect potential cybersecurity events.	1. Confirm that intrusion detection systems (IDS) are in place to monitor the network.
					2. Inquire and verify whether a tool is available to analyze anomalous events to detect potential cybersecurity events.
				11b. Information Security Testing Verify that information security testing including periodic penetration testing and vulnerability assessment, is performed and monitored.	1. Confirm that policies and procedures are in place for periodic information security testing.
					2. Inquire and verify that Vulnerability/Penetration testing has been performed on the systems and key applications.
				11c. Security Events Verify that security events are logged, reviewed, and monitored for anomalous activity.	1. Inquire and verify that security events are logged, reviewed, and monitored for anomalous activity.

				11d. Security Event Data Assess whether security event data are aggregated and correlated from multiple sources and sensors.	1. Inquire and verify whether data aggregation and correlation is performed for security event data from multiple sources and sensors.
Respond (RS)	**12. Respond and Recover:** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	Incident response program may not provide clear instructions for employees to follow, or adequately address escalation and remediation procedures.	High	**12. Respond and Recover** Evaluate that an incident response program, including how incidents are detected, reported, escalated, and remediated, is in place and managed.	1. Confirm that an incident response program including how incidents are reported, escalated and remediated, is in place.
Recover (RC)					2. Inquire and assess the response procedures for the incidents occurred during the Covered Period against the incident response program.