DATA SECURITY AND PRIVACY STANDARDS

FOR NEW YORK STATE EDUCATIONAL AGENCIES

RIC ONE TARGET PROFILE FOR EDUCATIONAL AGENCIES

IDENTIFY

DEVELOPED BY:

RIC one
TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE

VERSION DATE:

September 2020

NYS RICS OVERVIEW:

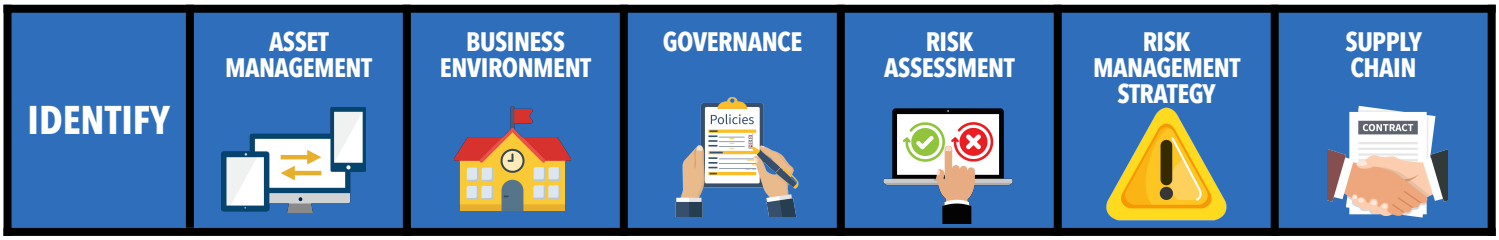
12 NYS centers organized under and supporting the 37 BOCES to provide shared technology services.

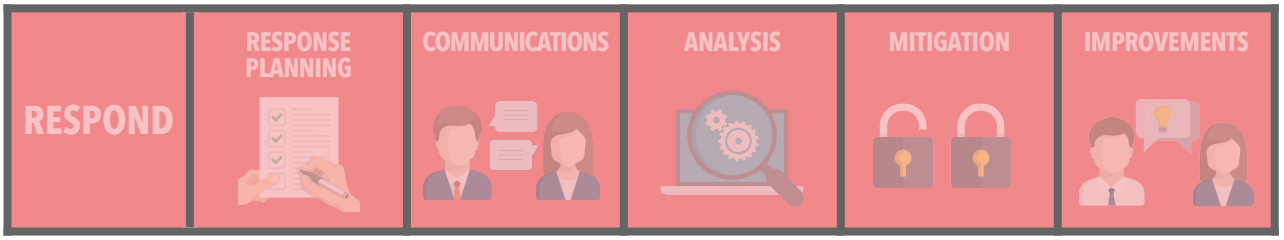
INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK

NATIONAL DATA SECURITY FRAMEWORK OVERVIEW

Education Law 2-d requires educational agencies to adopt a policy on data security and privacy that aligns with the state's data security and privacy standard. The Department adopted the National Institute for Standards and Technology Cybersecurity Framework (NIST CSF) as the standard for educational agencies. **At the center of the framework is the Core, which is a set of activities and desired outcomes designed to help organizations manage data security and privacy risk**. The Core is organized into functions, categories, and subcategories.

FRAMEWORK CORE 5 FUNCTIONS AND 23 CATEGORIES





IMPLEMENTATION OF THE CYBERSECURITY FRAMEWORK

PROGRESSION TOWARD STATEWIDE OBJECTIVES

As educational agencies apply the NIST Cybersecurity Framework, the goal is to continuously evaluate current practices and progress toward a defined objective, or Target Profile. Using the RIC One Target Profile, educational **agencies will evaluate their current environment, identify where deficiencies or inefficiencies exist, and design an action plan** to enhance the security posture.

TARGET PROFILE OVERVIEW

School districts and BOCES will use the Target Profile to support the development of a district-specific data security and privacy strategic action plan. The Target Profile identifies common desired cybersecurity outcomes. The Target Profile was developed to address our sector's needs and risk environment. Specifically, the tool includes a four-level rubric and desired level for each subcategory. As many agencies do not employ a cybersecurity expert, the related rubrics incorporate education-specific explanatory language. Below is a simplified version of one rubric with the associated NYS target highlighted.

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
PHYSICAL DEVICES AND SYSTEMS WITHIN THE ORGANIZATION **ARE INVENTORIED**	AN **INVENTORY** OF PHYSICAL ASSETS **DOES NOT EXIS**T OR EXISTS IN A LIMITED STATE.	INVENTORY **EXISTS**, BUT IS **NOT MAINTAINED**	**INVENTORY INCLUDES CERTAIN ELEMENTS** MAKE, MODEL, SERIAL NUMBER, DEVICE TYPE, ASSET LOCATION, ASSIGNEE, ACQUISITION DATE, AND DECOMMISSION DATE	**AUTOMATED MECHANISMS** EXIST **TO UPDATE** INVENTORY

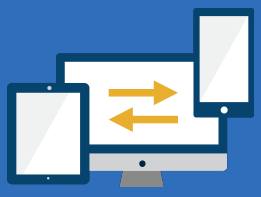
USING THE TARGET PROFILE TO DEVELOP AN ACTION PLAN

TARGET **PROFILE**	CURRENT **PROFILE**	GAP **ANALYSIS**	ACTION **PLAN**
			
RIC ONE K-12 TARGET PROFILE DEVELOPED common desired cybersecurity outcomes are identified in the Target Profile for Educational Agencies	**AGENCIES DETERMINE THEIR CURRENT PROFILE** educational agencies identify the current state of their cybersecurity activities in the Current Profile	**AGENCIES ANALYZE AND PRIORITIZE GAPS** agencies identify gaps by comparing the profiles and then prioritizing the mitigation of those gaps	**AGENCIES DEVELOP AND IMPLEMENT ACTION PLANS** educational agencies develop plans to address gaps and adjusts practices in order to achieve the Target Profile

IDENTIFY FUNCTION

Agencies develop an **ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK** to systems, people, assets, data, and capabilities.

ASSET MANAGEMENT



ID.AM-1	**Physical devices** and systems within the organization are **inventoried**
ID.AM-2	**Software platforms** and applications within the organization are **inventoried**
ID.AM-3	Organizational **communication and data flows** are **mapped**
ID.AM-4	**External** information **systems** are **catalogued**
ID.AM-5	**Resources** are **prioritized based on** their **classification, criticality, and business value**
ID.AM-6	**Cybersecurity** roles and **responsibilities** for the entire workforce and third-party stakeholders **are established**

BUSINESS ENVIRONMENT

ID.BE-1	The organization's **role in the supply chain** is **identified** and communicated
ID.BE-2	The organization's **place in** critical infrastructure and its **industry sector** is **identified** and communicated
ID.BE-3	Priorities for **organizational** mission, **objectives**, and activities are **established** and communicated
ID.BE-4	Dependencies and **critical functions** for delivery of critical services are **established**
ID.BE-5	**Resilience requirements** to support delivery of critical services are **established** for all operating states

GOVERNANCE

ID.GV-1	Organizational **cybersecurity policy** is **established** and communicated
ID.GV-2	Cybersecurity roles and **responsibilities** are **coordinated** and aligned with **internal roles and external partners**
ID.GV-3	**Legal and regulatory requirements** regarding cybersecurity, including privacy and civil liberties obligations, are understood and **managed**
ID.GV-4	Governance and **risk management processes address** cybersecurity **risks**

IDENTIFY FUNCTION

Agencies develop an **ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK** to systems, people, assets, data, and capabilities.

RISK ASSESSMENT

ID.RA-1	Asset **vulnerabilities** are identified and **documented**
ID.RA-2	**Cyber threat intelligence** is **received** from information sharing forums and sources
ID.RA-3	**Threats**, both internal and external, are **identified and documented**
ID.RA-4	Potential **organizational impacts** and likelihoods are **identified**
ID.RA-5	**Threats, vulnerabilities, likelihoods, and impacts** are **used** to **determine risk**
ID.RA-6	**Risk responses are identified** and prioritized

RISK MANAGEMENT

ID.RM-1	**Risk management processes** are **established**, managed, and agreed to by organizational stakeholders
ID.RM-2	Organizational **risk tolerance** is **determined** and clearly expressed
ID.RM-3	The organization's determination of **risk tolerance** is **informed by** its role in critical infrastructure and **sector specific risk analysis**

SUPPLY CHAIN

ID.SC-1	Cyber **supply chain risk management processes** are identified, **established**, assessed, managed, and agreed to by organizational stakeholders
ID.SC-2	Suppliers and **third party partners** of information systems, components, and services **are identified, prioritized, and assessed** using a cyber supply chain risk assessment process
ID.SC-3	**Contracts** with suppliers and third-party partners are **used to implement** appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber **Supply Chain Risk Management Plan**
ID.SC-4	Suppliers and **third-party partners** are **routinely assessed** using audits, test results, or other forms of evaluations **to confirm** they are **meeting** their **contractual obligations**
ID.SC-5	**Response and recovery** planning and **testing** are conducted **with** suppliers and **third-party providers**

ASSET MANAGEMENT CATEGORY

ID.AM-1	**PHYSICAL DEVICES** and systems within the organization are **INVENTORIED**
LEVEL 1	An inventory of physical assets does not exist or exists in a limited state.
LEVEL 2	An inventory of physical assets exists, but is not frequently maintained, or does not contain all of the following information: make, model, serial number, device type, asset location, assignee, acquisition date, and decommission date.
LEVEL 3	An accurate, documented **inventory exists and is updated** as assets are acquired or removed from service. The **asset inventory includes: make, model, serial number, device type, asset location, assignee, acquisition date, and decommission date**.
LEVEL 4	An accurate, documented inventory exists and automated mechanisms exist to update inventory, detect unauthorized assets, verify inventory accuracy, and track assets by geographic location. The asset inventory includes: make, model, serial number, device type, asset location, assignee, acquisition date, and decommission date.

ID.AM-2	**SOFTWARE PLATFORMS** and applications within the organization are **INVENTORIED**
LEVEL 1	An inventory of software does not exist or exists in a limited state.
LEVEL 2	An accurate inventory of administrative and prominent instructional software and applications exists. However, software systems containing PII, of which administration do not have knowledge, are in use. The inventory may not contain all the following elements: system name, vendor, system type, scope of implementation, host location, type of data stored, implementation date, and termination date.
LEVEL 3	An accurate, documented **inventory of all** software and **applications containing PII exists** and a process is in place to ensure the district is aware of new products and products that are no longer in use. The **inventory contains: system name, vendor, system type, scope of implementation, host location, type of data stored, implementation date, and termination date**.
LEVEL 4	An accurate, documented inventory of all software and applications exists and a process is in place to ensure the district is aware of new products and products that are no longer in use. The inventory contains: system name, vendor, system type, scope of implementation, host location, type of data stored, implementation date, and termination date. Additionally, automated mechanisms exist to identify software installed and prevent the utilization of unauthorized systems.

ASSET MANAGEMENT CATEGORY (CONTINUED)

ID.AM-3	Organizational **COMMUNICATION AND DATA FLOWS** are **MAPPED**
LEVEL 1	The organization is not aware of the system interoperability information flows necessary to carry out its objectives. Examples of information flow include, but are not limited to: transmission of information across internal or external networks, traffic origin, internet access, and system interoperability.
LEVEL 2	An informal awareness of the system interoperability information flows necessary to carry out organizational objectives exists; however, no documented listing of appropriate information flows exists. Interoperability information should include: source system, destination system, data transferred, method of transfer, and purpose.
LEVEL 3	System **interoperability information flows** necessary to carry out organizational objectives are defined and **documented**. **Interoperability information includes: source system, destination system, data transferred, method of transfer, and purpose**.
LEVEL 4	Information flows necessary to carry out organizational objectives are defined and documented. Additionally, automated mechanisms to control and monitor information flow are in place. System interoperability information includes: source system, destination system, data transferred, method of transfer, and purpose.

ID.AM-4	**EXTERNAL** information **SYSTEMS** are **CATALOGUED**
LEVEL 1	An inventory of software does not exist or exists in a limited state.
LEVEL 2	An accurate inventory of externally hosted administrative and prominent instructional information systems exists. However, systems containing PII, of which administration do not have knowledge, are in use. The inventory may not contain all the following elements: system name, vendor, system type, scope of implementation, host location, type of data stored, implementation date, and termination date.
LEVEL 3	An accurate, documented **inventory of externally hosted information systems containing PII exists**, and a process is in place to ensure the district is aware of new products and products that are no longer in use. The **inventory contains: system name, vendor, system type, scope of implementation, host location, type of data stored, implementation date, and termination date**.
LEVEL 4	An accurate, documented inventory of externally hosted information systems exists, and a process is in place to ensure the district is aware of new systems and systems that are no longer in use. The inventory contains: system name, vendor, system type, scope of implementation, host location, type of data stored, implementation date, and termination date. Additionally, automated mechanisms exist to prevent the utilization of unauthorized systems.

ASSET MANAGEMENT CATEGORY (CONTINUED)

ID.AM-5	RESOURCES are PRIORITIZED BASED ON their CLASSIFICATION, CRITICALITY, AND BUSINESS VALUE
LEVEL 1	Information systems and technology resources do not have a defined classification and criticality.
LEVEL 2	A general awareness of high priority information systems exists; however, no documented classification and criticality exists.
LEVEL 3	A documented listing of information system classification and criticality exists, and the characteristics of the levels within those scales are clearly defined and documented.
LEVEL 4	A documented **listing of information system classification and criticality exists**, and the characteristics of the levels within those scales are clearly defined and documented. **Resource prioritization is regularly re-evaluated** with the addition or subtraction of new systems, data elements or technologies.

ID.AM-6	CYBERSECURITY roles and RESPONSIBILITIES for the entire workforce and third-party stakeholders ARE ESTABLISHED
LEVEL 1	Cybersecurity roles and responsibilities for all stakeholder groups are not clearly defined and documented.
LEVEL 2	Cybersecurity roles and responsibilities are defined, documented, and communicated for internal stakeholders, but not external stakeholder groups.
LEVEL 3	Cybersecurity **roles and responsibilities for all stakeholder groups**, both internal and external, **are** clearly defined, **documented, and communicated**.
LEVEL 4	Cybersecurity roles and responsibilities for all stakeholder groups, both internal and external, are clearly defined, documented, and communicated. Additionally, the organization integrates the establishment or modification of cybersecurity roles into the process of planning for critical changes to their environment.

BUSINESS ENVIRONMENT CATEGORY

ID.BE-1	The organization's **ROLE IN THE SUPPLY CHAIN** is **IDENTIFIED** and communicated
LEVEL 1	The organization is unaware of its role in the supply chain.
LEVEL 2	The organization is aware of its role in the supply chain, but has not formally defined that role.
LEVEL 3	The organization has formally defined its role in the supply chain, but has not had discussions to relate that role to security operations.
LEVEL 4	The organization has formally **defined its role in the supply chain, and utilizes its understanding** of that role **to inform security operations**.

ID.BE-2	The organization's **PLACE IN** critical infrastructure and its **INDUSTRY SECTOR** is **IDENTIFIED** and communicated
LEVEL 1	The organization is unaware of its role in critical infrastructure and its industry sector.
LEVEL 2	The organization is aware of its role in critical infrastructure and its industry sector, but has not formally defined its environment.
LEVEL 3	The organization has formally defined its role in critical infrastructure and its industry sector, but has not had discussions to relate its environment security operations.
LEVEL 4	The organization has formally **defined its role in** critical infrastructure and its **industry sector, and utilizes its understanding** of its environment **to inform security operations**.

ID.BE-3	Priorities for organizational mission, **OBJECTIVES**, and activities are **ESTABLISHED AND COMMUNICATED**
LEVEL 1	Organization mission and objectives are not established.
LEVEL 2	Organization mission and objectives are established, but not communicated to all staff.
LEVEL 3	Organization mission and objectives are established and communicated to all staff. Activities supporting the organizational mission and objectives are not clearly established and communicated.
LEVEL 4	Organization **mission, objectives, and activities** are **established and communicated** to all staff.

BUSINESS ENVIRONMENT CATEGORY (CONTINUED)

ID.BE-4	Dependencies and **CRITICAL FUNCTIONS** for delivery of critical services are **ESTABLISHED**
LEVEL 1	Critical services are not clearly defined and documented.
LEVEL 2	Critical services are clearly defined and documented, but critical supporting systems and processes, are not identified and documented.
LEVEL 3	Critical services, and their supporting systems and processes, are identified and documented.
LEVEL 4	**Critical services**, **and** their **supporting systems** and processes, are identified and **documented**. As changes are made to critical systems, or their supporting systems and processes, documentation is **updated** to reflect the modifications.

ID.BE-5	**RESILIENCE REQUIREMENTS** to support delivery of critical services are **ESTABLISHED** for all operating states (e.g. under duress/attack, during recovery, normal operations)
LEVEL 1	Resilience requirements of critical services are not clearly defined and documented.
LEVEL 2	Resilience requirements of critical services are identified, but not placed into clear and defined categories.
LEVEL 3	**Resilience requirements of critical services are identified through the use of** clear and defined **categories**.
LEVEL 4	Resilience requirements of critical services are identified through the use of clear and defined categories. Categories are reviewed and updated consistently as the organizational environment, requirements, or technology change.

GOVERNANCE CATEGORY

ID.GV-1	Organizational information **SECURITY POLICY** is **ESTABLISHED** and communicated
LEVEL 1	No organizational information security policy exists.
LEVEL 2	An outdated or incomprehensive organizational information security policy exists, but does not reflect all appropriate laws, regulations, and policies.
LEVEL 3	An organizational information security policy reflecting appropriate laws, regulations, and policies is in place, documented, and communicated.
LEVEL 4	An organizational information security **policy reflecting appropriate laws, regulations, and policies is in place**, documented, and communicated. The policy is **updated consistently** as the organizational environment, requirements, or technology change.

ID.GV-2	Cybersecurity roles and **RESPONSIBILITIES** are **COORDINATED** and aligned with **INTERNAL ROLES AND EXTERNAL PARTNERS**
LEVEL 1	Cybersecurity roles and responsibilities are not clearly defined and documented.
LEVEL 2	Cybersecurity roles and responsibilities are defined and documented; however, those responsibilities are not aligned with the roles of the appropriate staff members or external partners.
LEVEL 3	Cybersecurity roles and responsibilities are defined and documented, and those responsibilities are aligned with the roles of the appropriate staff members or external partners.
LEVEL 4	Cybersecurity roles and **responsibilities are** defined and **documented**, and those responsibilities are aligned with the roles of the appropriate staff members or external partners. Additionally, **the organization integrates the allocation of cybersecurity roles into the process of planning for critical changes** to their environment.

ID.GV-3	**LEGAL AND REGULATORY REQUIREMENTS** regarding cybersecurity, including privacy and civil liberties obligations, are understood and **MANAGED**
LEVEL 1	Legal and regulatory requirements are not identified or well understood.
LEVEL 2	Legal and regulatory requirements are identified, but the understanding of these requirements is not sufficient to adequately shape district practices for data security.
LEVEL 3	**Legal and regulatory requirements** are identified and **well understood at upper administrative levels and are used to define district practices** for data security. However, gaps in the understanding of requirements exist in other areas of the organization.
LEVEL 4	Legal and regulatory requirements are identified and well understood at all levels of the organization and are used to define district data security practices.

GOVERNANCE CATEGORY (CONTINUED)

ID.GV-4	Governance and **RISK MANAGEMENT STRATEGIES** are **IN PLACE** to address cybersecurity risk
LEVEL 1	No cybersecurity risk management process exists.
LEVEL 2	The organization has identified where cybersecurity risks lie but does not have a comprehensive understanding of the severity of specific risks in order to prioritize decision making.
LEVEL 3	The organization has identified where cybersecurity risks lie and understands the severity of specific risks but does not consistently take action to mitigate the highest severity risks to acceptable levels.
LEVEL 4	The **organization understands its appetite** for risk, has identified **where cybersecurity risks lie**, understands **the severity of those risks**, **and uses that knowledge to inform** prioritized **action plans** related to risk mitigation.

RISK ASSESSMENT CATEGORY

ID.RA-1	Asset **VULNERABILITIES** are identified and **DOCUMENTED**
LEVEL 1	Asset vulnerabilities are not identified and documented.
LEVEL 2	Asset vulnerabilities are defined by internal staff through the use of manual processes assessment and automated vulnerability scanning tools, but regular assessments are not conducted and reviewed.
LEVEL 3	Asset **vulnerabilities are defined and regularly updated by** internal staff through the use of **manual processes assessment and** automated vulnerability **scanning tools**.
LEVEL 4	Asset vulnerabilities are defined by internal staff through the use of manual processes and automated vulnerability scanning tools. Additionally, results are verified through the use of external vulnerability assessments.

ID.RA-2	**CYBER THREAT INTELLIGENCE** is **RECEIVED** from information sharing forums and sources
LEVEL 1	The organization does not receive threat and vulnerability updates from reputable organizations.
LEVEL 2	The organization receives threat and vulnerability updates from reputable organizations, but does not consistently use the information to enhance their security practices.
LEVEL 3	The organization **receives threat and vulnerability updates** from reputable organizations **and consistently uses the information** to enhance their security practices.
LEVEL 4	The organization receives threat and vulnerability updates from reputable organizations, and actively participates in threat and vulnerability sharing forums and discussions with colleagues.

ID.RA-3	**THREATS**, both internal and external, are identified and **DOCUMENTED**
LEVEL 1	Cybersecurity threats are not identified and documented.
LEVEL 2	Cybersecurity threats to the organization are generally known, but not well-defined.
LEVEL 3	Cybersecurity **threats** to the organization **are identified, documented, and understood**.
LEVEL 4	Cybersecurity threats to the organization are identified, documented, and understood, and are verified via external threat assessments.

RISK ASSESSMENT CATEGORY (CONTINUED)

ID.RA-4	Potential **ORGANIZATIONAL IMPACTS** and likelihoods are **IDENTIFIED**
LEVEL 1	The impact and likelihood of vulnerability exploitations to the organization are not identified.
LEVEL 2	The impact and likelihood of vulnerability exploitations to the organization are generally known, but not defined.
LEVEL 3	The **impact and likelihood of vulnerability exploitations** to the organization are identified and **documented**.
LEVEL 4	The impact and likelihood of vulnerability exploitations to the organization are identified and documented, and are verified via external impact assessments.

ID.RA-5	Threats, vulnerabilities, likelihoods, and impacts are used to **DETERMINE RISK**
LEVEL 1	The organization does not keep a risk registry that identifies the severity of its risks based on their likelihood and impact.
LEVEL 2	The organization keeps a risk registry that identifies risks to its environment, but the severity of those risks is not fully informed by threats, vulnerabilities, likelihoods, and impacts.
LEVEL 3	**Threats, vulnerabilities, likelihoods, and impacts inform a** comprehensive **risk registry** which, in turn, is **used to guide decision-making.**
LEVEL 4	Threats, vulnerabilities, likelihoods, and impacts inform a formal risk determination process which, in turn, is used to guide decision-making. Additionally, these risk determinations are compared to formal, external risk assessments.

ID.RA-6	**RISK RESPONSES ARE IDENTIFIED** and prioritized
LEVEL 1	No cybersecurity risk response process exists.
LEVEL 2	The organization has identified where cybersecurity risks lie but does not develop action plans to mitigate those risks to acceptable levels based on their defined risk appetite and the severity of each risk.
LEVEL 3	The organization has **identified where** cybersecurity **risks lie** and **develops action plans to mitigate those risks** to acceptable levels **based on their defined risk appetite and the severity of each risk**.
LEVEL 4	The organization has identified where cybersecurity risks lie and develops action plans to mitigate those risks to acceptable levels based on their defined risk appetite and the severity of each risk. Additionally, these risk determinations are compared to formal, external risk assessments.

RISK MANAGEMENT CATEGORY

ID.RM-1	**RISK MANAGEMENT PROCESSES** are **ESTABLISHED**, managed, and agreed to by organizational stakeholders
LEVEL 1	Information security risk management processes are not formally established and documented.
LEVEL 2	Information risks are identified, evaluated, and managed exclusively by technology staff.
LEVEL 3	A **committee** is established **to** define and **manage** organizational **information security risks**. **Committee members represent all critical areas of organizational operations** in order to accurately identify risks and their effects on the organization as a whole.
LEVEL 4	A committee is established to define and manage organizational information security risks. Committee members represent all critical areas of organizational operations in order to accurately identify risks and their effects on the organization as a whole. Those findings are regularly assessed via external risk assessment experts.

ID.RM-2	Organizational **RISK TOLERANCE** is **DETERMINED** and clearly expressed
LEVEL 1	Organizational information security risk tolerance levels are not formally established and documented.
LEVEL 2	Tolerance for information security risks are determined exclusively by technology staff.
LEVEL 3	A **committee** is **established** to define the organizations **tolerance for** information **security risks**. **Committee members represent all critical areas of organizational operations** in order to accurately reflect all areas of the organization.
LEVEL 4	A committee is established to define the organization's tolerance for information security risks. Committee members represent all critical areas of organizational operations in order to accurately reflect all areas of the organization. Those findings are regularly assessed via external risk assessment experts.

ID.RM-3	The organization's determination of **RISK TOLERANCE** is **INFORMED BY** its role in critical infrastructure and **SECTOR SPECIFIC RISK ANALYSIS**
LEVEL 1	Organizational information security risk tolerance levels are not are not aligned to the organization's role in critical infrastructure.
LEVEL 2	Technology staff exclusively determines whether the organization's tolerance for information security risk aligns with the organization's role in critical infrastructure.
LEVEL 3	A **committee,** that represents all critical areas of organizational operations, is **established** to ensure the organization's **tolerance for information security risks aligns with** its role in **critical infrastructure**.
LEVEL 4	A committee, that represents all critical areas of organizational operations, is established to ensure the organization's tolerance for information security risks aligns with its role in critical infrastructure. Those findings are regularly assessed via external risk assessment experts.

SUPPLY CHAIN CATEGORY

ID.SC-1	Cyber **SUPPLY CHAIN RISK MANAGEMENT PROCESSES** are identified, **ESTABLISHED**, assessed, managed, and agreed to by organizational stakeholders
LEVEL 1	Cyber supply chain risk management processes are not formally established and documented.
LEVEL 2	Risks incurred by utilizing information systems designed or hosted by external entities, are identified, evaluated, and managed exclusively by technical staff.
LEVEL 3	A **committee** is **established to** define and **manage organizational information security risks**. **Committee members represent all critical areas of organizational operations** in order to accurately identify risks and their effects on the organization as a whole. **Risks incurred by utilizing information systems designed or hosted by external entities are included in those discussions**.
LEVEL 4	A committee is established to define and manage organizational information security risks. Committee members represent all critical areas of organizational operations in order to accurately identify risks and their effects on the organization as a whole. Risks incurred by utilizing information systems designed or hosted by external entities, are included in those discussions. Those findings are regularly assessed via external risk assessment experts.

ID.SC-2	Suppliers and **THIRD PARTY PARTNERS** of information systems, components, and services **ARE IDENTIFIED, PRIORITIZED, AND ASSESSED** using a cyber supply chain risk assessment process
LEVEL 1	No process exists for the identification and evaluation of third-party information systems in use by the organization.
LEVEL 2	The organization has a process to identify and evaluate risks associated with third-party information systems and services, prior to their use by the organization, that is managed exclusively by technical staff.
LEVEL 3	The organization has a **process to identify and evaluate risks associated with third-party information systems** and service, **prior to their use** by the organization, that includes input from all critical areas of the organization.
LEVEL 4	The organization has a process to identify and evaluate risks associated with third-party information systems and service, prior to their use by the organization, that includes input from all critical areas of the organization. That process is regularly assessed via external risk assessment experts.

SUPPLY CHAIN CATEGORY (CONTINUED)

ID.SC-3	**CONTRACTS** with suppliers and third-party partners are **USED TO IMPLEMENT** appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber **SUPPLY CHAIN RISK MANAGEMENT PLAN**
LEVEL 1	The organization has no process to ensure contracts with third-party partners meet organizational security and privacy requirements.
LEVEL 2	The organization has a process to ensure contracts that meet organizational security and privacy requirements are in place with third-party partners who access highly sensitive information, including administrative and prominent instructional information systems.
LEVEL 3	The organization has a **process to ensure contracts** that meet organizational security and privacy **requirements are in place** with third-party partners who access any organizational personally identifiable information.
LEVEL 4	The organization has a process to ensure all contracts with third-party partners meet organizational security and privacy requirements.

ID.SC-4	Suppliers and **THIRD-PARTY PARTNERS** are **ROUTINELY ASSESSED** using audits, test results, or other forms of evaluations **TO CONFIRM** they are **MEETING** their **CONTRACTUAL OBLIGATIONS**
LEVEL 1	The organization has no process to evaluate third-party partners to ensure they meet organizational security and privacy requirements.
LEVEL 2	The organization has a process in place to periodically evaluate contracts with third-party partners who access highly sensitive information, including administrative and prominent instructional information systems, to ensure they continue to meet organizational security and privacy requirements.
LEVEL 3	The organization has a process in place to **periodically evaluate contracts with third-party partners** who access any organizational personally identifiable information, **to ensure they continue to meet** organizational **security and privacy requirements.**
LEVEL 4	The organization has a process that requires all third-party partners to demonstrate that they are meeting their contractual obligations by regularly providing the results of audits, assessments, or other testing agreed upon by both entities.

SUPPLY CHAIN CATEGORY (CONTINUED)

ID.SC-5	**RESPONSE AND RECOVERY** planning and **TESTING** are conducted **WITH** suppliers and **THIRD-PARTY PROVIDERS**
LEVEL 1	The organization has no process to ensure response and recovery processes involving third-party partners are functional and effective.
LEVEL 2	The organization and third-party providers of administrative and prominent instructional information systems have a plan in place that outlines roles and responsibilities related to response and recovery. However, those plans are not regularly tested.
LEVEL 3	The organization receives **annual assurances** that **response and recovery processes related to administrative and prominent instructional information systems**, managed by third-party partners, **are functional and effective**.
LEVEL 4	The organization regularly participates in simulated response and recovery exercises related to administrative and prominent instructional information systems that are managed by third-party providers.

TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE