DATA SECURITY AND PRIVACY STANDARDS
FOR NEW YORK STATE EDUCATIONAL AGENCIES
IMPLEMENTATION GUIDE

IDENTIFY

DEVELOPED BY:

RIC one
TWELVE REGIONAL INFORMATION CENTERS WORKING AS ONE

VERSION DATE:

January 2021

NYS RICS OVERVIEW:

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

RIC one

TWELVE REGIONAL INFORMATION CENTERS

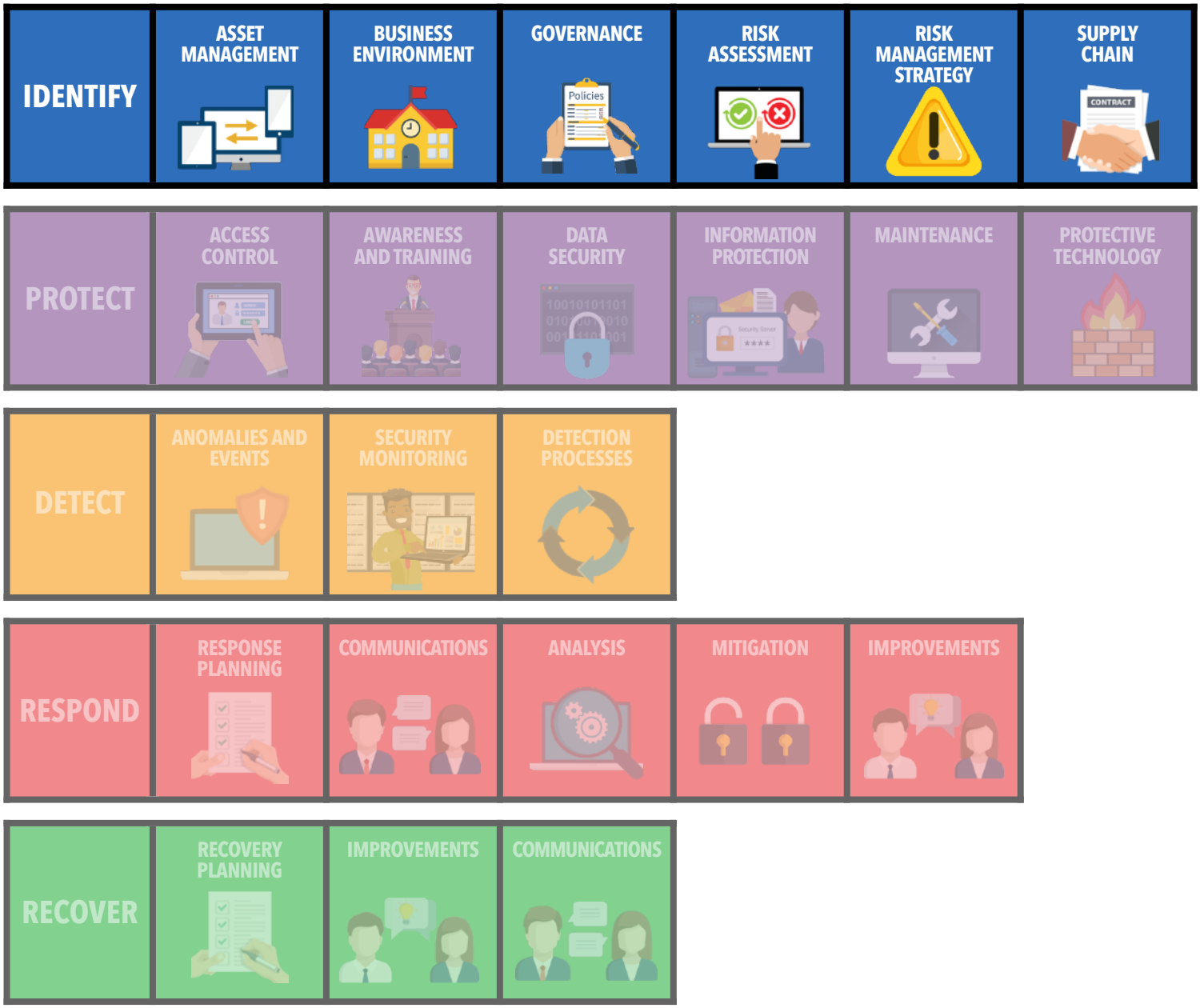
WORKING AS ONE

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



IDENTIFY

AGENCIES DEVELOP AN ORGANIZATIONAL UNDERSTANDING TO MANAGE CYBERSECURITY RISK TO SYSTEMS, PEOPLE, ASSETS, DATA, AND CAPABILITIES.

IDENTIFY CATEGORIES

Below are simplified descriptions of each of the Identify categories. An extended definition is included on the subsequent pages which provide information to assist educational agencies in understanding and applying practices aligned to the subcategories under each category.

ASSET MANAGEMENT
Managing assets consistent with their importance and the agency's risk strategy.

RISK ASSESSMENT
Identifying the agency's cybersecurity risks to operations, assets, and individuals.

BUSINESS ENVIRONMENT
Understanding the agency's priorities to guide cybersecurity decisions.

RISK MANAGEMENT STRATEGY
Establishing the agency's priorities, constraints, and risk tolerances.

GOVERNANCE
Leveraging policies, procedures, and processes to manage and monitor the agency's risk.

SUPPLY CHAIN MANAGEMENT
Implementing processes to manage risk associated with partners and third-party contractors.

WHY IDENTIFY?

Understanding the business CONTEXT, the **RESOURCES that support critical functions, and** the related **cybersecurity RISKS enables an organization to** focus and **PRIORITIZE** its **EFFORTS**, consistent with its risk management strategy and business needs.

CONTEXT			RESOURCES		RISK
 **Priorities** Learning & Safety	 **Constraints** Funding	 **Policies** Ed Law 2-D	 **Assets** Data & Systems	 **Partners** Vendors & RICs	 **Risks** Ransomware

IDENTIFICATION AND PRIORITIZATION OF CYBERSECURITY ACTIONS

IDENTIFY

IMPLEMENTATION & PROGRESS MONITORING CHECKLIST

ASSET MANAGEMENT

Managing assets consistent with their importance and the agency's risk strategy.

☐	ID.AM-1	SERVERS AND INFRASTRUCTURE ARE INVENTORIED.
☐		STAFF DEVICES ARE INVENTORIED.
☐		STUDENT DEVICES ARE INVENTORIED.
☐	ID.AM-2 ID.AM-4 ID.AM-5	ADMINISTRATIVE SYSTEMS ARE INVENTORIED.
☐		INSTRUCTIONAL SYSTEMS ARE INVENTORIED.
☐		CLASSROOM (FREE) SYSTEMS ARE INVENTORIED.
☐		THE SYSTEM INVENTORIES NOTE CRITICALITY RATINGS AND UPTIME REQUIREMENTS.
☐	ID.AM-3	DATA FLOWS FOR CORE SYSTEMS ARE DOCUMENTED.
☐		DATA FLOWS FOR OTHER SYSTEMS ARE DOCUMENTED.
☐	ID.AM-6	IT/DATA STAFF RESPONSIBILITIES ARE DOCUMENTED.
☐		PARTNERS RESPONSIBILITIES ARE DOCUMENTED.
☐		ALL STAFF RESPONSIBILITIES ARE DOCUMENTED.

BUSINESS ENVIRONMENT

Understanding the agency's priorities to guide cybersecurity decisions.

☐	ID.BE-1 ID.BE-2 ID.BE-3 ID.BE-4 ID.BE-5	THE ORGANIZATION'S BUSINESS ENVIRONMENT IS DOCUMENTED.

IDENTIFY

NIST CSF FUNCTION

GOVERNANCE

Leveraging policies, procedures, and processes to manage and monitor the agency's risk.

☐	ID.GV-1	ED LAW 2-D POLICY IS ADOPTED AND POSTED.
☐	ID.GV-2	CYBER RESPONSIBILITIES ARE DOCUMENTED. (ALIGNED TO ID.AM.6 DELIVERABLES.)
☐	ID.GV-3	COMPLIANT PRACTICES, ALIGNED TO EACH LAW, ARE DOCUMENTED.
☐	ID.GV-4	RISK-RELATED SECURITY MEETINGS ARE IMPLEMENTED.

RISK ASSESSMENT

Identifying the agency's cybersecurity risks to operations, assets, and individuals.

☐	ID.RA-1	VULNERABILITIES ARE IDENTIFIED AND DOCUMENTED.
☐	ID.RA-2	THE AGENCY RECEIVES CYBER ALERTS.
☐	ID.RA-3	A RISK REGISTRY IS DEVELOPED AND MAINTAINED.

RISK MANAGEMENT STRATEGY

Establishing the agency's priorities, constraints, and risk tolerances.

☐	ID.RM-1	RISK MANAGEMENT PROCESSES ARE ESTABLISHED.
☐	ID.RM-2 ID.RM-3	THE AGENCY'S RISK TOLERANCE IS DOCUMENTED.

SUPPLY CHAIN MANAGEMENT

Implementing processes to manage risk associated with partners and third-party contractors.

☐	ID.SC-1 ID.SC-2 ID.SC-4 ID.SC-5	CYBER SUPPLY CHAIN RISK MANAGEMENT PROCESSES ARE DOCUMENTED.
☐	ID.SC-3	CONTRACTS ARE USED TO IMPLEMENT SAFEGUARDS.

IDENTIFY

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

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

THE DATA, PERSONNEL, DEVICES, SYSTEMS, AND FACILITIES THAT ENABLE THE ORGANIZATION TO ACHIEVE BUSINESS PURPOSES ARE IDENTIFIED AND MANAGED CONSISTENT WITH THEIR RELATIVE IMPORTANCE TO ORGANIZATIONAL OBJECTIVES AND THE ORGANIZATION'S RISK STRATEGY.

ID.AM-1 PHYSICAL DEVICES AND SYSTEMS WITHIN THE ORGANIZATION ARE INVENTORIED.

DEVICES TO INVENTORY

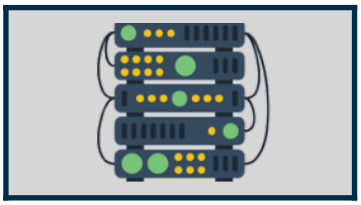
COMPUTERS AND LAPTOPS

TABLETS

CHROMEBOOKS

CELL PHONES

SERVERS



INFRASTRUCTURE

VOIP PHONES

OTHER (EXAMPLES: PRINTERS, USB)

INVENTORY ELEMENTS

1. Make
2. Model
3. Serial Number
4. Device Type
5. Asset Location
6. Assignee
7. Acquisition Date
8. Decommission Date

The inventory can also be used to document devices' operating system, antivirus, and other information relevant to security.

HELPFUL HINT

This category of work involves developing and maintaining a variety of inventories. Developing or performing significant updates to these inventories can be resource intensive. As a result, consider prioritizing the work. Always **START BY INVENTORYING THE** data, personnel, devices, **SYSTEMS**, and facilities **THAT HOUSE THE MOST SENSITIVE DATA AND/OR SUPPORT CRITICAL FUNCTIONS**.

ASSET MANAGEMENT

ID.AM-2 SOFTWARE PLATFORMS AND APPLICATIONS WITHIN THE ORGANIZATION ARE INVENTORIED.

ID.AM-4 EXTERNAL INFORMATION SYSTEMS ARE CATALOGUED.

ID.AM-5 RESOURCES (E.G., HARDWARE, DEVICES, DATA, TIME, PERSONNEL, AND SOFTWARE) ARE PRIORITIZED BASED ON THEIR CLASSIFICATION, CRITICALITY, AND BUSINESS VALUE.

SYSTEMS TO INVENTORY

PLATFORMS, APPLICATIONS, AND INFORMATION SYSTEMS	INTERNAL SYSTEMS	EXTERNAL SYSTEMS	INCLUDE "FREE" AND CLASSROOM BASED TOOLS
			

INVENTORY ELEMENTS

1. System Name
2. Vendor
3. System Type
4. Implementation Scope
5. Host Location
6. Data Type
7. Implementation Date
8. Termination Date
9. Criticality Rating
10. Required Uptime

RESOURCES PRIORITIZATION

RESOURCE PRIORITIZATION CONSIDERATIONS	CLASSIFICATION	CRITICALITY	BUSINESS VALUE
 ESSENTIAL RESOURCES AND RESOURCES HOUSING SENSITIVE INFORMATION	 **Sensitive Data** (Examples: Socio-Economic, Disability, Homeless, and Social-Emotional)	 **Essential Systems** (Examples: Financial, Facilities, Phones, Student, and E-mail)	 **Primary Learning Systems** (Examples: Core Programs and Local Assessments)

ASSET MANAGEMENT

ID.AM-3 ORGANIZATIONAL COMMUNICATION AND DATA FLOWS ARE MAPPED.

INVENTORY ELEMENTS

1. Source System
2. Destination System
3. Data Transferred
4. Method of Transfer
5. Purpose

SOURCE	DESTINATION	DATA	METHOD	PURPOSE
Mindex schooltool	Renaissance Star	Student Demographic	Renaissance Data Integrator (RDI)	Auto Uploaded and Updated Data

ID.AM-6 CYBERSECURITY ROLES AND RESPONSIBILITIES FOR THE ENTIRE WORKFORCE AND THIRD-PARTY STAKEHOLDERS (E.G., SUPPLIERS, CUSTOMERS, PARTNERS) ARE ESTABLISHED.

PARTNERSHIPS IN THE NYS EDUCATION SECTOR

DISTRICT
DPO, IT STAFF, ADMINISTRATION, AND ALL STAFF

EDUCATIONAL AGENCY PARTNERS
REGIONAL INFORMATION CENTERS AND BOCES

VENDOR PARTNERS
SOFTWARE COMPANIES
(INCLUDING "FREE" SOLUTION PROVIDERS)

OTHER PARTNERS
LEGAL, LAW ENFORCEMENT, COMMUNITY PARTNERS

CATEGORIES OF CYBERSECURITY ROLES AND RESPONSIBILITIES

DATA GOVERNANCE

COMPLIANCE WITH STATE AND FEDERAL LAW

TECHNICAL SAFEGUARDS

EMPLOYEE TRAINING

ACCESS CONTROLS

SUBCONTRACTORS OVERSIGHT

INCIDENT DETECTION AND RESPONSE

DATA TRANSFER AND DISPOSAL

NOT DISCLOSE PII TO ANY OTHER PARTY

ONLY USE PII AS AUTHORIZED

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.

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 (E.G. UNDER DURESS/ATTACK, DURING RECOVERY, NORMAL OPERATIONS).

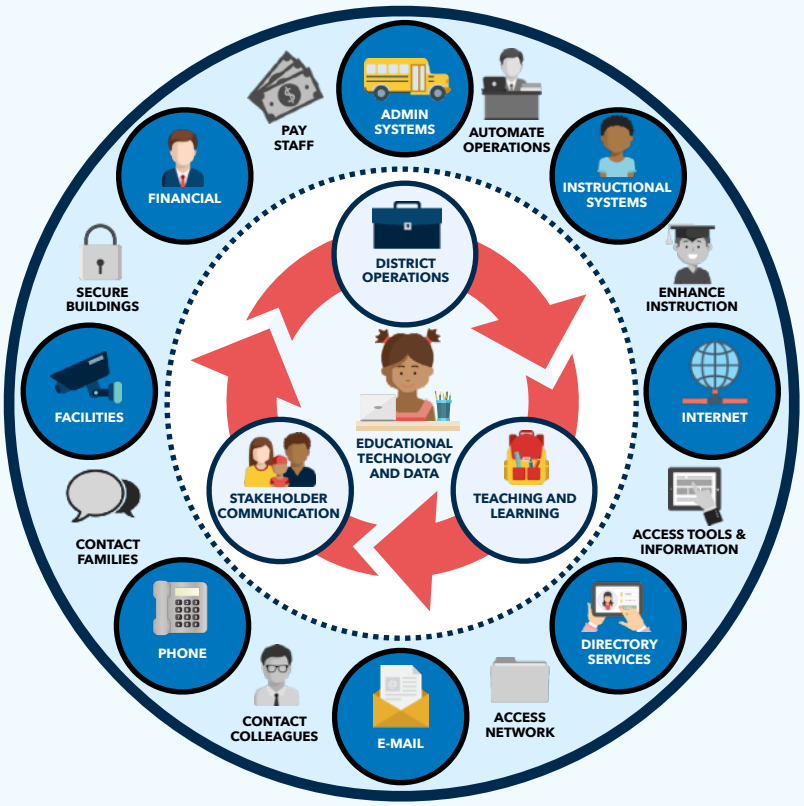
EXAMPLE DISTRICT BUSINESS ENVIRONMENT OVERVIEW

As a public school district in New York State, our core objective is to provide a high quality, modern education to students within our district from grades K-12. In order to accomplish this, our district utilizes many software applications that house valuable information for enhancing teaching and learning, providing targeted instruction, district administrative functions, and improving district operations.

These systems may reside on site or are hosted with outside partners. All systems and software titles are procured from outside vendors for our operations. Our district does not develop or resell software applications. These systems are utilized by district staff, students, and student families. As specific titles change from time to time, the district keeps a System Inventory outlining the products in use, and at what scope.

Our district is part of a wide-area network, along with 49 other school districts and 4 BOCES in central and northern NY, that is managed and maintained by the Regional Information Center. We rely on this connection, as well as our internal network infrastructure, for the 99.9+% uptime required for internet and system access necessary to successfully deliver a modern instructional experience, communicate with the families and guardians of our students, and interact with the NY State Education Department.

As some systems are more essential to daily operations than others, the criticality rating and required uptime may be found in our district's System Inventory.



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.

ID.GV-1 ORGANIZATIONAL CYBERSECURITY POLICY IS ESTABLISHED AND COMMUNICATED.

EDUCATION LAW 2-D DATA SECURITY AND PRIVACY POLICY

Education Law 2-D requires educational agencies to adopt a policy on data security and privacy by July 1, 2020. The chart below highlights some of the components that will be addressed in this policy.

NIST CSF ALIGNED PRACTICES

NIST Cybersecurity Framework aligned practices

DATA GOVERNANCE

Ensure using PII benefits students and the agency

DISCLOSURE AVOIDANCE

Protection of PII in public reports

STATE AND FEDERAL LAWS

FERPA, IDEA, and other laws

DATA PROTECTION OFFICER

Employee responsible for the implementation of Ed Law 2-d

ANNUAL EMPLOYEE TRAINING

Privacy and security awareness training

COMPLAINT PROCEDURES

Complaints about breaches or unauthorized releases of data

INCIDENT REPORTING

Reporting breach to the CPO and impacted stakeholders

ID.GV-2 CYBERSECURITY ROLES AND RESPONSIBILITIES ARE COORDINATED AND ALIGNED WITH INTERNAL ROLES AND EXTERNAL PARTNERS.

SAMPLE ROLES AND RESPONSIBILITIES

INTERNALLY/RIC HOSTED AND MANAGED SYSTEMS

The vendor is responsible for application level security, security patch development, and abiding by statutory, regulatory, and contractual requirements. The District or the RIC is responsible for all other cybersecurity activities based on service level.

EXTERNALLY HOSTED AND MANAGED SYSTEMS - DISTRICT RESPONSIBILITIES

The district is the data owner and responsible for data quality, defining privacy requirements, and business utilization of data entered into the system. Also, the district is responsible for application access privileges, system configurations, and security of devices accessing the system.

EXTERNALLY HOSTED AND MANAGED SYSTEMS - VENDOR RESPONSIBILITIES

The vendor is responsible for infrastructure security, uptime, patching, application level security, patch development, patch deployment, and abiding by statutory, regulatory, and contractual requirements.

GOVERNANCE

ID.GV-3 LEGAL AND REGULATORY REQUIREMENTS REGARDING CYBERSECURITY, INCLUDING PRIVACY AND CIVIL LIBERTIES OBLIGATIONS, ARE UNDERSTOOD AND MANAGED.

NYS EDUCATION SECTOR AND CYBERSECURITY LAWS AND REGULATIONS

The diagram below highlights the primary laws and regulatory requirements regarding cybersecurity and the NYS education sector. Additionally, sample evidence of a district's compliance with each law is included. By clicking on the name of the law in the chart, you can access websites that provide more information about each requirement. In addition to these laws and regulations, other laws such as Children's Internet Protection Act (CIPA), and NYS Technology Law impact cybersecurity practices.

ED LAW 2-D	FERPA	COPPA	PPRA	ED-1
This law protects the privacy and security of personally identifiable information (PII) of students, and certain APPR data. The law outlines requirements for educational agencies and their contractors.	This is the foundational federal law related to the privacy of students' educational records. FERPA limits access to student records and details rules to follow when accessing the data.	COPPA imposes requirements on operators of websites, games, apps or online services directed to children under 13, and on online service providers that collect personal information online from a child under 13.	PPRA defines the rules states and districts must follow when administering surveys, analysis, and evaluations funded by the US Department of Education. It requires parental approval to administer many tools.	The ED-1 Records Retention and Disposition Schedule indicates the minimum length of time that officials of school districts and BOCES must retain their records before they may be disposed of legally.
District Data Privacy and Security Policy and Compliant Third-Party Contracts	District Education Records Policy	District Attains Parental Consent to Use Tools, As Required via Terms of Service	District Parental Access Instructional Materials Policy	District Records Management Policy

ID.GV-4 GOVERNANCE AND RISK MANAGEMENT PROCESSES ADDRESS CYBERSECURITY RISKS.

OVERVIEW AND SAMPLE TOOL

The risk landscape changes overtime as the district environment and external landscape change. District security staff, technology staff, and administration should meet monthly to prioritize individual risks, develop mitigation strategies, and ensure past projects remain on task.

INHERENT RISK LEVEL FORMULA								
IMPACT			**x**	**LIKELIHOOD**			**=**	**RISK LEVEL**
1	2	3	x	1	2	3	=	<4 4-6 >6

REVIEW ID.RM.1 IN ORDER TO LEARN MORE ABOUT THIS FORMULA.

Based on risk assessment, districts should focus their efforts on their highest risks. In other words, the risks to the organization that will have the greatest impact on the objectives of the district that have the greatest likelihood of occurring should be prioritized when developing policies, defining practices, and implementing controls.

RISK ASSESSMENT

THE ORGANIZATION UNDERSTANDS THE CYBERSECURITY RISK TO ORGANIZATIONAL OPERATIONS (INCLUDING MISSION, FUNCTIONS, IMAGE, OR REPUTATION), ORGANIZATIONAL ASSETS, AND INDIVIDUALS.

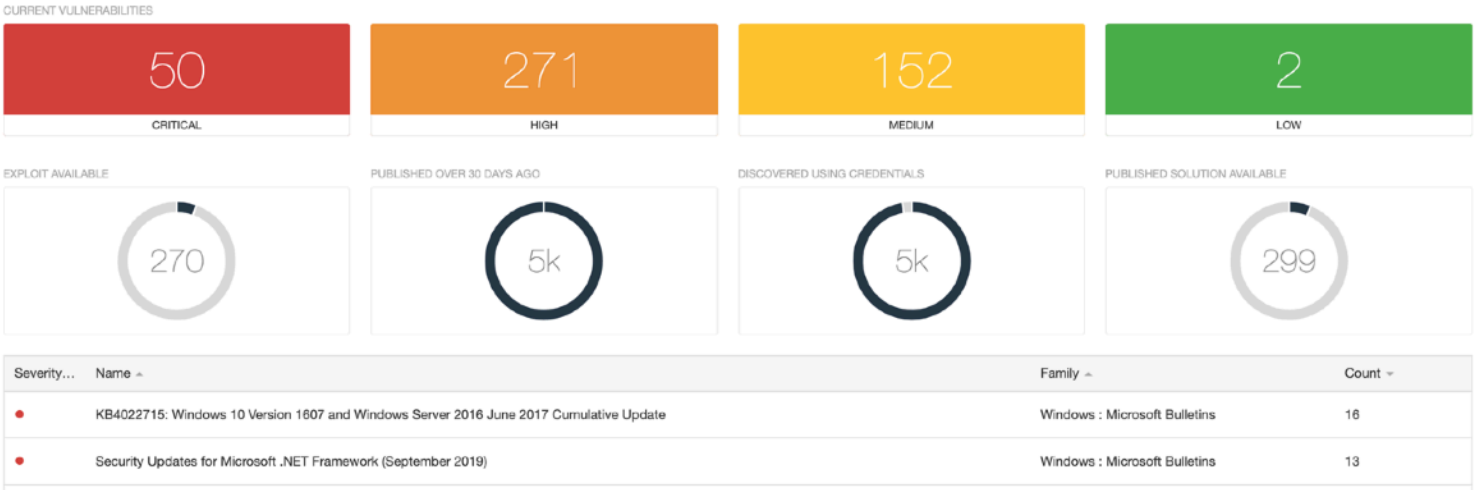
ID.RA-1 ASSET VULNERABILITIES ARE IDENTIFIED AND DOCUMENTED.

SAMPLE VULNERABILITY MANAGEMENT PROCEDURE

Our district conducts vulnerability scans on critical systems on a monthly basis. High severity vulnerabilities as well as those vulnerabilities that cause a particular risk to exceed our risk appetite, are mitigated as quickly as possible.

Should a particular vulnerability exist that is unable to be patched either because it would disrupt a particular system or a patch does not yet exist, additional controls will be put in place to lower the risk below the appropriate threshold.

Additionally, we review critical operational processes on an annual basis to ensure no vulnerabilities exist in our manual processes



ID.RA-2 CYBER THREAT INTELLIGENCE IS RECEIVED FROM INFORMATION SHARING FORUMS AND SOURCES.

CYBER INCIDENT NOTIFICATIONS & ALERTS

Educational agencies should receive alerts from the following organizations regarding critical data security and privacy threats that have the potential to impact agency operations. Click on the entities' names in the chart, to access websites associated with each entity.

LOCAL REGIONAL INFORMATION CENTER	NYSED DATA PRIVACY AND SECURITY DEPARTMENT	NATIONAL CYBER AWARENESS SYSTEM	MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER
RIC one – TWELVE REGIONAL INFORMATION CENTERS WORKING AS ONE	NYSED.gov	U.S. DEPARTMENT OF HOMELAND SECURITY	MS-ISAC® Multi-State Information Sharing & Analysis Center®

RISK ASSESSMENT

ID.RA-3 THREATS, BOTH INTERNAL AND EXTERNAL, ARE IDENTIFIED AND DOCUMENTED.

ID.RA-4 POTENTIAL BUSINESS 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.

THE EDUCATION SECTOR AND THE THREAT LANDSCAPE

The chart below identifies some of the most common, internal and external, threats.

SYSTEM AVAILABILITY	SYSTEM AND DATA INTEGRITY	UNAUTHORIZED PII DISCLOSURE	MONETARY LOSS	NON-COMPLIANCE
				
Access to systems or infrastructure is disrupted or denied	Unauthorized data modification causing inaccuracy of information	PII viewed by unauthorized persons	Monetary loss due to cyber incident	Agency practices not compliant with laws, regulations and policies
• Denial of Service Attack • Hardware Failure • Malicious Insider • Malware Infection • Misconfiguration	• Credential Theft • Data Loss • Malicious Insider • Malware Infection	• Accidental Leakage • Device Theft • Malicious Insider • Theft (External Systems) • Theft (Internal Systems)	• Device Theft • Digital Theft • Extortion • Malicious Insider • Social Engineering	• Laws and Regulations

RISK REGISTER

Using a risk register, educational agencies will determine risk. Then, the risks will be prioritized and response plans will be documented and managed. To learn more about Inherent Risk, Residual Risk, and Risk Tolerance, review ID.RM.1, ID.RM.2, and ID.RM.3. Additionally, ask your local RIC for an excel Risk Register tool.

Risk	Description of Risk and Impact	Inherent Risk	Existing Mitigating Controls	Residual Risk	Risk Tolerance	Residual Gap	Mangement Plan
MONETARY LOSS - DEVICE THEFT	A piece of hardware is stolen from the district that is necessary to conduct educational or district operational functions. The device will need to be replaced in order to continue normal activities.	Medium	Physical Asset Inventory Asset Management Procedures Mechanisms Insurance Physical Protections Employee On/Off Boarding Practices	Low	Medium	Cannot track missing devices.	Implement geolocation tracking software for portable devices.

RISK MANAGEMENT STRATEGY

THE ORGANIZATION'S PRIORITIES, CONSTRAINTS, RISK TOLERANCES, AND ASSUMPTIONS ARE ESTABLISHED AND USED TO SUPPORT OPERATIONAL RISK DECISIONS.

ID.RM-1 RISK MANAGEMENT PROCESSES ARE ESTABLISHED, MANAGED, AND AGREED TO BY ORGANIZATIONAL STAKEHOLDERS.

SAMPLE RISK MANAGEMENT PROCESSES

As new risks are identified and existing risks move beyond levels that are acceptable to our district, risk management and mitigation plans will be established to lower risks to acceptable levels. Plans will be established by district administration with input from appropriate stakeholders and roles will be assigned as required in order to implement the plan in a defined timeframe. The tools below will support our district in managing risk.

INHERENT RISK

Inherent Risk is the fundamental risk an organization experiences for a given threat, irrespective of the controls and preventative measures in place.

INHERENT RISK LEVEL								
Impact			x	Likelihood			=	Risk Level
1	2	3	x	1	2	3	=	<4 4-6 >6

CONTROL EFFECTIVENESS

Control Effectiveness measures the level of implementation of security strategies and protections designed to mitigate the risk an organization experiences for a given threat.

CONTROL EFFECTIVENESS													
Procedural Controls				x	Technical Controls				=	Overall Effectiveness			
1	2	3	4	x	1	2	3	4	=	<4	5-7	8-12	>12

RESIDUAL RISK

Residual Risk is the actual risk an organization experiences for a given threat after taking into account controls put in place to mitigate the Inherent Risk.

RESIDUAL RISK LEVEL		INHERENT RISK LEVEL		
		Low	Medium	High
CONTROL EFFECTIVENESS	Highly Effective	Low	Low	Medium-Low
	Effective	Low	Medium-Low	Medium
	Partially Effective	Low	Medium-Low	Medium-High
	Ineffective	Low	Medium	High

RISK MANAGEMENT STRATEGY

THE ORGANIZATION'S PRIORITIES, CONSTRAINTS, RISK TOLERANCES, AND ASSUMPTIONS ARE ESTABLISHED AND USED TO SUPPORT OPERATIONAL RISK DECISIONS.

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.

SAMPLE ORGANIZATIONAL RISK TOLERANCE STATEMENT

In order to achieve our objectives of providing a high quality education to our students, in a way that is meaningful in the modern environment, with the resources available to us, and with the openness expected by our community, **our district understands it must accept some risk** in various areas of our operations.

Our district has little to no appetite for assuming risk that may cause harm to our students, the **unauthorized disclosure of highly sensitive** personally identifiable **information** of students or staff, **negatively impact learning, or result** in the **loss of substantial funds.**

Our district has a moderate appetite for risks that will cause minor impacts to daily activities, but not substantially disrupt the core functions of our district for extended periods.

EDUCATION LAW 2-D AND RISK MANAGEMENT

Educational Law 2-D requires educational agencies to ensure every use and disclosure of PII by the agency benefits students and the educational agency. This can be determined during the system or project analysis / evaluation phase using a tool similar to the sample below. Agencies should balance the educational value and security and privacy considerations.

OVERVIEW	
Describe the instructional or administrative tool and the purpose for which it will be used.	
EDUCATIONAL VALUE	**TRAINING** NEEDS
• State the educational value of the solution. • Is there a solution currently deployed within the district that addresses the stated need? If yes, specify the solution.	• Outline expected staff professional development needs.
FINANCIAL DETAILS	**SECURITY AND PRIVACY** CONSIDERATIONS
• What is the true product cost, including hardware, software, implementation, ongoing support, and other expenses? • How can the agency procure the tool in compliance with laws/ policies?	• Is there an Educational Law 2-D compliant agreement in place? • List data elements that are collected, stored and/or utilized by the system. Identify protected and sensitive data elements. • Identify potential risks (e.g. student harm, data disclosure).
TECHNICAL NEEDS	**DATA INTEGRATION** NEEDS
• Does the district have appropriate technical expertise to support and maintain this product?	• State data entry and/or transmission element requirements. • Identify data transmission options.

SUPPLY CHAIN MANAGEMENT

THE ORGANIZATION'S PRIORITIES, CONSTRAINTS, RISK TOLERANCES, AND ASSUMPTIONS ARE ESTABLISHED AND USED TO SUPPORT RISK DECISIONS ASSOCIATED WITH MANAGING SUPPLY CHAIN RISK. THE ORGANIZATION HAS ESTABLISHED AND IMPLEMENTED THE PROCESSES TO IDENTIFY, ASSESS AND MANAGE SUPPLY CHAIN RISKS.

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-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.

EXAMPLE SUPPLY CHAIN RISK MANAGEMENT STRATEGY

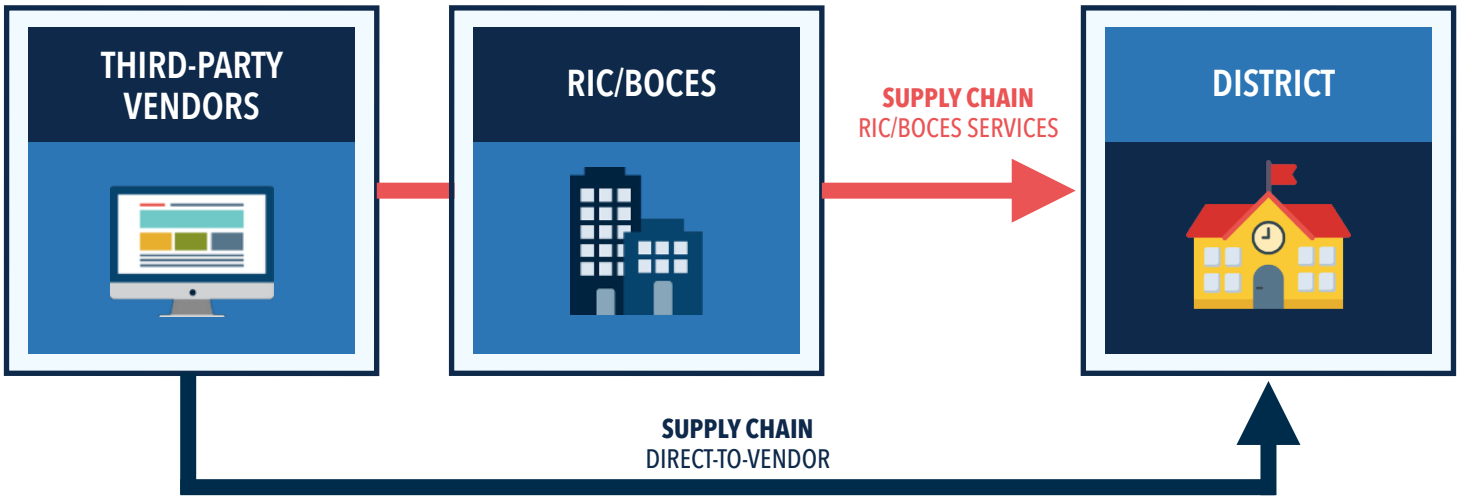
As part of our risk management strategy, our district will only utilize systems designated as Criticality Level 1 that are hosted and managed internally or with an outside entity who is able to demonstrate the ability to protect the information in a fashion that fits within the acceptable risk profile developed by our district. The district will still retain responsibilities related to cybersecurity as outlined in the Governance Category.

Should our district utilize an outside entity to host and/or manage a Level 1 Critical System, our district will transfer risk to that entity through contractual agreements that outline terms for the protection and utilization of district information.

As part of those terms, the third party will be bound by all applicable statutes and regulations, and will make available resources that confirm audits, test results, or other assessments related to their security posture.

Additionally, the third party must provide reasonable assurances related to resiliency and their ability to respond to a cybersecurity incident, and recover from that incident with minimal to no data loss. This should include a plan to regularly test recovery procedures as well as define data backup and retention periods.

Should the district require any material changes to these types of systems, such as changing vendors or migrating host location, the district will evaluate any associated risks prior to implementing those changes.



SUPPLY CHAIN MANAGEMENT

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.

OVERVIEW OF REQUIREMENTS RELATED TO THIRD-PARTY CONTRACTORS

Education law 2-D and Part 121 of the Commissioner's Regulations define several requirements related to third-party contractors. Educational agencies must ensure provisions are in contracts with third party contractors. The diagram below highlights these required elements. Additionally, other statutory and regulatory obligations are noted. While not required, educational agencies should strive to ensure the additional obligations are also noted in agreements. In order to learn more about these obligations, leverage Education Law 2-D and Part 121 resources.

DATA SECURITY AND PRIVACY PLAN

- IMPLEMENTATION OF ALL REQUIREMENTS
- SECURITY PROTECTIONS
- SUPPLEMENTAL INFO COMPLIANCE
- CONTRACTOR TRAINING
- SUBCONTRACTOR TRAINING
- SUBCONTRACTORS MANAGEMENT
- CYBER INCIDENT PLAN
- DATA TRANSFER AND DISPOSAL
- SIGNED COPY OF THE BILL OF RIGHTS

ADDITIONAL STATUTORY AND REGULATORY OBLIGATIONS

- NIST CSF SAFEGUARDS
- COMPLY WITH AGENCY POLICY AND LAW 2-D
- LIMIT ACCESS TO PII
- ONLY USE PII AS AUTHORIZED
- NOT DISCLOSE PII TO ANY OTHER PARTY
- SAFEGUARD THE PII IN CUSTODY
- ENCRYPTION PRACTICES APPLIED
- PROHIBITIONS ON PII COMMERCIAL USE
- OVERSIGHT OF SUBCONTRACTOR

OBLIGATIONS RELATED TO THE SUPPLEMENTAL INFORMATION FOR THE BILL OF RIGHTS

- EXCLUSIVE PURPOSES FOR DATA USE
- OVERSIGHT OF SUBCONTRACTORS
- CONTRACT DURATION AND DATA DISPOSAL
- DATA ACCURACY / CORRECTION PRACTICES
- SECURITY PROTECTIONS AND DATA LOCATION
- ENCRYPTION PRACTICES APPLIED

CONFIDENTIALITY MAINTAINED

- IN ACCORDANCE WITH LAWS
- IN ACCORDANCE WITH AGENCY POLICY

Contractual Obligations

Additional Statutory and Regulatory Obligations

RIC one

TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE