DATA SECURITY AND PRIVACY STANDARDS

FOR NEW YORK STATE EDUCATIONAL AGENCIES

RIC ONE TARGET PROFILE FOR EDUCATIONAL AGENCIES

RECOVER

DEVELOPED BY:

RIC one
TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE

VERSION DATE:

April 2021

NYS RICS OVERVIEW:

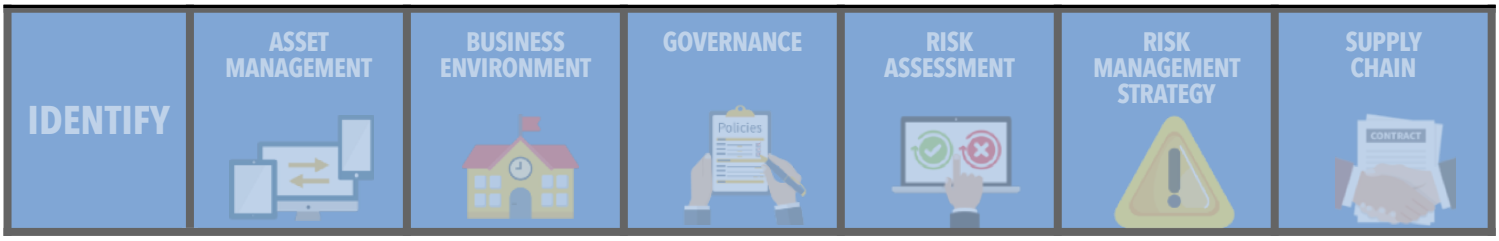
12 NYS centers organized under and supporting the 37 BOCES to provide shared technology services.

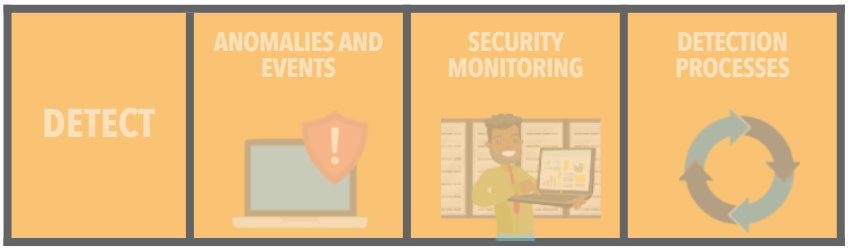
INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK

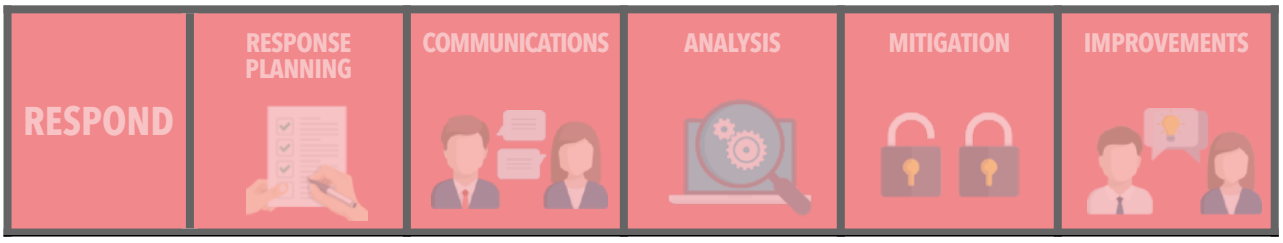
NATIONAL DATA SECURITY FRAMEWORK OVERVIEW

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
RECOVERY PLAN IS EXECUTED DURING OR AFTER A CYBERSECURITY INCIDENT	**RECOVERY PROCESSES** ARE **DEFINED** BUT **NOT ABLE TO BE EXECUTED**	**RECOVERY PROCESSES** ARE **DEFINED** BUT **NOT** REGULARLY **TESTED**	**RECOVERY PLANS** ARE **DEFINED, TESTED** AND ABLE TO BE **EXECUTED** DURING AN INCIDENT	**RECOVERY PLANS** ARE **DEFINED, TESTED** AND ABLE TO BE **EXECUTED** DURING AN INCIDENT. **METRICS** EXIST TO **QUANTIFY** RESPONSE AND IMPROVEMENT.

USING THE TARGET PROFILE TO DEVELOP AN ACTION PLAN

TARGET **PROFILE**

RIC ONE K-12 TARGET PROFILE DEVELOPED

common desired cybersecurity outcomes are identified in the Target Profile for Educational Agencies

CURRENT **PROFILE**

AGENCIES DETERMINE THEIR CURRENT PROFILE

educational agencies identify the current state of their cybersecurity activities in the Current Profile

GAP **ANALYSIS**

AGENCIES ANALYZE AND PRIORITIZE GAPS

agencies identify gaps by comparing the profiles and then prioritizing the mitigation of those gaps

ACTION **PLAN**

AGENCIES DEVELOP AND IMPLEMENT ACTION PLANS

educational agencies develop plans to address gaps and adjusts practices in order to achieve the Target Profile

RECOVER FUNCTION

DEVELOP AND **IMPLEMENT** APPROPRIATE **ACTIVITIES** TO MAINTAIN PLANS FOR **RESILIENCE** AND TO **RESTORE ANY CAPABILITIES OR SERVICES** THAT WERE IMPAIRED DUE TO A **CYBERSECURITY INCIDENT**.

RECOVERY PLANNING	**RC.RP-1**	**Recovery plan is executed** during or after a cybersecurity incident
IMPROVEMENTS	**RC.IM-1**	**Recovery plans** incorporate **lessons learned**
	RC.IM-2	**Recovery strategies** are **updated**
COMMUNICATIONS	**RC.CO-1**	**Public relations** are **managed**
	RC.CO-2	**Reputation** is **repaired** after an incident
	RC.CO-3	**Recovery activities are communicated** to internal and external **stakeholders** as well as executive and **management teams**

RECOVERY PLANNING CATEGORY

RC.RP-1	**Recovery plan is executed** during or after a cybersecurity incident
LEVEL 1	Recovery plans are defined but processes, procedures, and supporting technology are not tested to ensure the plan can function as intended.
LEVEL 2	Recovery plans are defined and processes, procedures, and supporting technology are tested at the time of plan development to ensure the plan can function as intended. However, continuous testing does not occur.
LEVEL 3	**Recovery plans** are **defined** and processes, procedures, and supporting technology are **tested** at least annually to ensure the plan can function as intended. **Processes, procedures, and supporting technology are updated** as the environment or requirements change, or failures occur during plan execution.
LEVEL 4	Recovery plans are defined and processes, procedures, and supporting technology are regularly tested to ensure the plan can function as intended. Processes, procedures, and supporting technology are updated as the environment or requirements change, or failures occur during plan execution. Metrics are developed and collected related to frequency, success, and efficiency.

IMPROVEMENTS CATEGORY

RC.IM-1	**Recovery plans** incorporate **lessons learned**
LEVEL 1	No process to incorporate lessons learned into recovery plans exists.
LEVEL 2	The organization reviews incidents and how the recovery process was applied to determine any plan enhancements that are necessary. Some processes to consider include: restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security.
LEVEL 3	The organization **reviews incidents** and how the recovery process was applied to **determine any plan enhancements that are necessary**. Some processes to consider include: restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. Additionally, **during the incident recovery process**, the organization **documents** and maintains records of **key events, process activities applied, and potential enhancements** to better inform the recovery improvement discussion.
LEVEL 4	The organization reviews incidents and how the recovery process was applied to determine any plan enhancements that are necessary. Some processes to consider include: restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. Additionally, during the incident recovery process, the organization documents and maintains records of key events, process activities applied, and potential enhancements to better inform the recovery improvement discussion. The organization then uses the information collected and discussed to develop incident recovery metrics to quantify improvement.

IMPROVEMENTS CATEGORY (CONTINUED)

RC.IM-2	Recovery strategies are updated
LEVEL 1	No process exists to update incident recovery strategies.
LEVEL 2	The organization annually updates recovery strategies based on the collective results of incidents that occurred that year.
LEVEL 3	The organization **updates recovery strategies based on outcomes** from incident reviews that occur immediately following an incident.
LEVEL 4	The organization updates recovery strategies based on outcomes from incident reviews that occur immediately following an incident. Additionally, the organization develops and utilizes incident recovery metrics to quantify improvement.

COMMUNICATIONS CATEGORY

RC.CO-1	Public relations are managed
LEVEL 1	No process exists to manage public relations during incident recovery.
LEVEL 2	The organization has identified staff focused on the management of public relations, including defining messaging related to an incident.
LEVEL 3	The organization has **identified staff** focused on the **management of public relations and defining messaging** related to an incident. Additionally, **roles and responsibilities are assigned** to team members, for example, media communication, community outreach, and staff messaging.
LEVEL 4	The organization has identified staff focused on the management of public relations, including defining messaging related to an incident. Additionally, roles and responsibilities are assigned to team members, for example, media communication, community outreach, and staff messaging. To assist with communication efficiency, the organization has pre-drafted scripts, memos, letters, and other communications.

COMMUNICATIONS CATEGORY

RC.CO-2	**Reputation** after an event is **repaired**
LEVEL 1	No process exists to manage organizational reputation after an incident.
LEVEL 2	The organization has identified staff focused on the management of organizational reputation, including defining messaging related to improvements and enhancements, and a commitment to prevention.
LEVEL 3	The organization has **identified staff** focused on the **management of public relations**, including defining **messaging related to improvements and enhancements**, and a **commitment to prevention**. Additionally, roles and **responsibilities are assigned** to team members, for example, media communication, community outreach, and staff messaging.
LEVEL 4	The organization has identified staff focused on the management of public relations, including defining messaging related to improvements, enhancements, and a commitment to prevention. Additionally, roles and responsibilities are assigned to team members, for example, media communication, community outreach, and staff messaging. To assist with communication efficiency, the organization has pre-drafted scripts, memos, letters, and other communications.

RC.CO-3	**Recovery activities are communicated** to internal and external **stakeholders** as well as executive and **management teams**
LEVEL 1	Communication with internal stakeholders related to incident recovery does not occur.
LEVEL 2	The organization has defined criteria for information that may be shared related to security incident recovery, including what types of information may be shared and with which stakeholders.
LEVEL 3	The organization has **defined criteria** for information that may be shared related to security incident recovery, including what **types of information may be shared and with which stakeholders**. **Administrative teams receive information** that can guide decision making related to management and communication of future incidents.
LEVEL 4	External entities required for incident response are involved with determining roles and responsibilities. Those roles and responsibilities are updated as the environment or requirements change. Additionally, metrics related to the recovery process are communicated to administrative teams to guide decision making related to management and communication of future incidents.

TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE