DATA SECURITY AND PRIVACY STANDARDS

FOR NEW YORK STATE EDUCATIONAL AGENCIES

RIC ONE TARGET PROFILE FOR EDUCATIONAL AGENCIES

RESPOND

DEVELOPED BY:

RIC one
TWELVE REGIONAL INFORMATION CENTERS WORKING AS ONE

VERSION DATE:

March 2021

NYS RICS OVERVIEW:

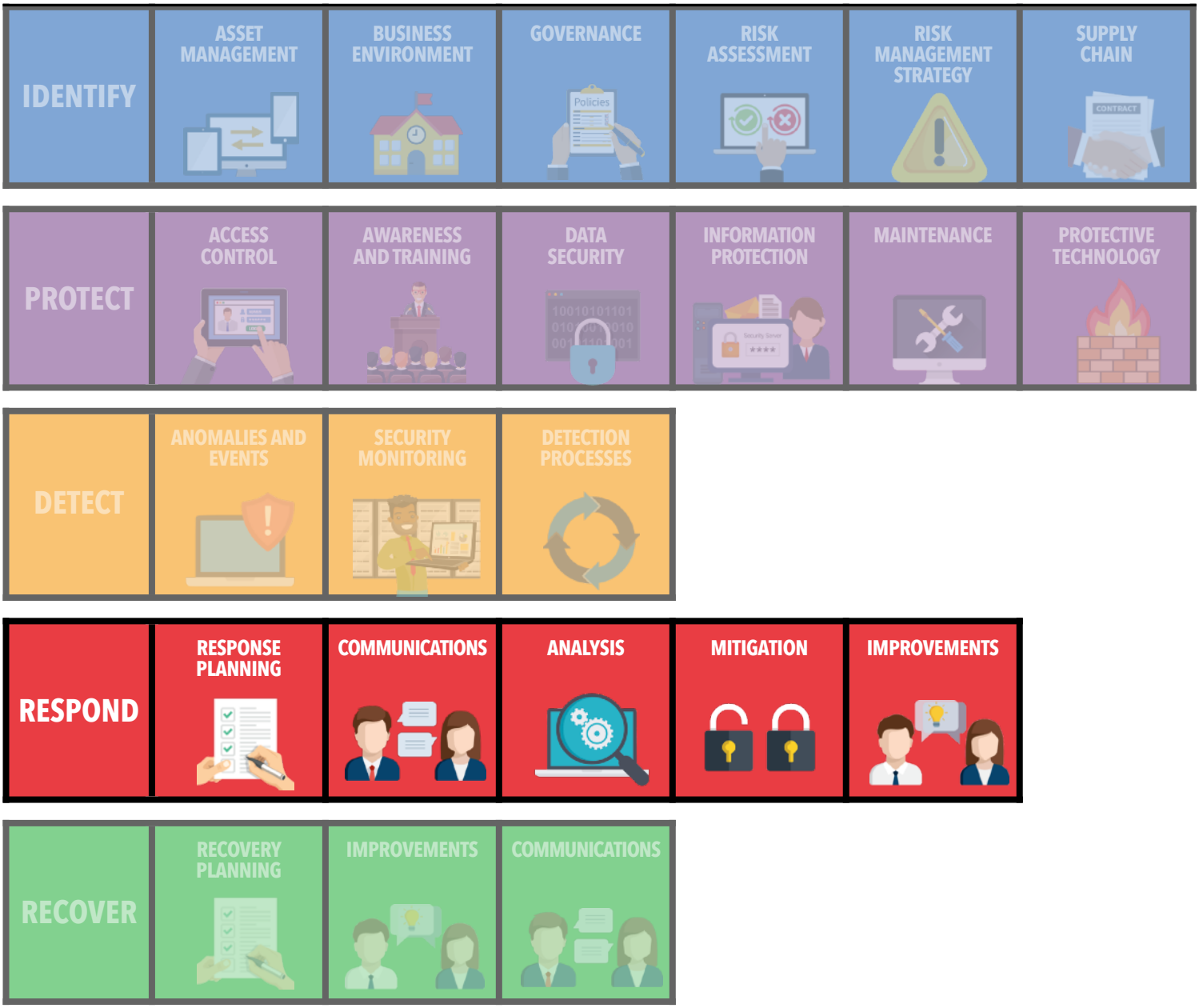
12 NYS centers organized under and supporting the 37 BOCES to provide shared technology services.

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.

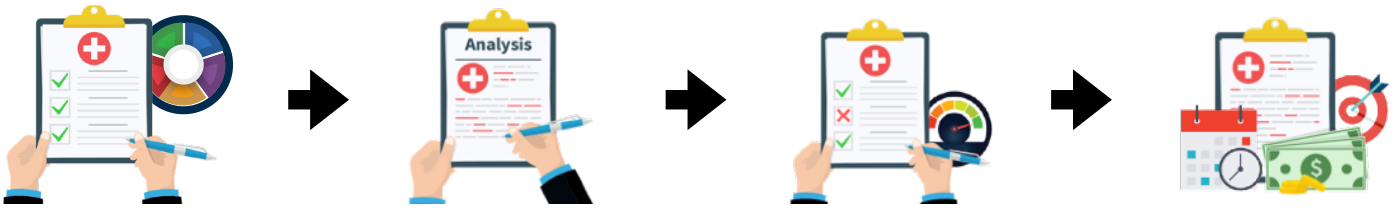
TARGET PROFILE OVERVIEW

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
RESPONSE PLAN EXECUTED DURING AN INCIDENT	**NO** FORMAL **RESPONSE PLAN** EXISTS	**RESPONSE PLAN** IS FORMALLY **DEFINED**	**RESPONSE PLANS** ARE **REGULARLY TESTED**	**RESPONSE PLANS** ARE **REGULARLY TESTED** **METRICS** DEVELOPED TO JUDGE SUCCESS

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

RESPOND FUNCTION

DEVELOP AND **IMPLEMENT** APPROPRIATE **ACTIVITIES TO TAKE ACTION** REGARDING A DETECTED **CYBERSECURITY INCIDENT**.

RESPONSE PLANNING	**RS.RP-1**	**Response plan is executed** during or after an incident
COMMUNICATIONS	**RS.CO-1**	**Personnel know their roles and order of operations** when a response is needed
	RS.CO-2	**Incidents are reported** consistent with established criteria
	RS.CO-3	**Information is shared** consistent with response plans
	RS.CO-4	**Coordination with stakeholders** occurs consistent with response plans
	RS.CO-5	**Voluntary information sharing occurs with external stakeholders** to achieve broader cybersecurity situational awareness
ANALYSIS	**RS.AN-1**	**Notifications** from detection systems are **investigated**
	RS.AN-2	The **impact** of the incident is **understood**
	RS.AN-3	**Forensics** are performed
	RS.AN-4	**Incidents are categorized** consistent with response plans
	RS.AN-5	**Processes** are established to **receive, analyze and respond to vulnerabilities** disclosed to the organization from **internal and external sources** (e.g. internal testing, security bulletins, or security researchers)
MITIGATION	**RS.MI-1**	**Incidents are contained**
	RS.MI-2	**Incidents are mitigated**
IMPROVEMENT	**RS.IM-1**	Response plans incorporate **lessons learned**
	RS.IM-2	Response **strategies are updated**

RESPONSE PLANNING CATEGORY

RS.RP-1	**Response plan is executed** during or after an incident
LEVEL 1	Response plans are defined but processes, procedures, and supporting technology are not tested to ensure the plan can function as intended.
LEVEL 2	Response 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	**Response 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	Response 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.

COMMUNICATIONS CATEGORY

RS.CO-1	**Personnel know their roles and order of operations** when a response is needed
LEVEL 1	Personnel are unaware of their roles and responsibilities related to incident response.
LEVEL 2	Personnel are given copies of organizational response plans that contain their roles and responsibilities related to incident response.
LEVEL 3	Personnel are given copies of organizational response plans that contain their roles and responsibilities related to incident response. The lead of the incident response team periodically examines roles and responsibilities, and makes any updates as the environment or requirements change. Updates and reminders are distributed to all organizational staff with a role in incident response.
LEVEL 4	**Personnel** are given copies of organizational response plans that contain their **roles and responsibilities** related to incident response. **Meetings of core members of the incident response team** occur periodically to examine roles and responsibilities, and make any **updates** as the environment or requirements change. Updates and reminders are distributed to all organizational staff with a role in incident response.

COMMUNICATIONS CATEGORY (CONTINUED)

RS.CO-2	**Incidents are reported** consistent with established criteria
LEVEL 1	No defined criteria for information sharing related to security incidents exists.
LEVEL 2	A defined process for reporting potential security incidents for analysis. That process and associated reporting requirements are communicated to appropriate staff at the time of development, but not continuously reinforced.
LEVEL 3	A **defined process** for r**eporting potential security incidents for analysis**. That process and associated reporting requirements are **communicated** to appropriate staff at the time of development, and are continuously reinforced.
LEVEL 4	Automated mechanisms are utilized to make reporting, tracking and escalating incidents more efficient. That process and associated reporting requirements are communicated to appropriate staff at the time of development, and are continuously reinforced.

RS.CO-3	**Information is shared** consistent with response plans
LEVEL 1	No defined criteria for information sharing related to security incidents exists.
LEVEL 2	The organization has a process to meet defined statutory and regulatory requirements for sharing information related to security incidents. However, no process exists for sharing security incident information with other primary stakeholders.
LEVEL 3	The organization has a **process to meet defined statutory and regulatory information sharing requirements**. Additionally, the organization has **defined criteria** for information that may be shared related to security incidents, including what **types of information may be shared** and with which primary stakeholders, outside of statutory and regulatory requirements.
LEVEL 4	The organization has a process to meet defined statutory and regulatory information sharing requirements. Additionally, the organization has defined criteria for information that may be shared related to security incidents, including what types of information may be shared and with which primary stakeholders, outside of statutory and regulatory requirements. Automated mechanisms are utilized to disseminate the appropriate security incident information to the appropriate primary stakeholders more efficiently.

COMMUNICATIONS CATEGORY (CONTINUED)

RS.CO-4	**Coordination with stakeholders** occurs consistent with response plans
LEVEL 1	Coordination with stakeholders related to security incidents does not occur.
LEVEL 2	Organizational staff are aware of how and when to coordinate with internal stakeholders in the event of a security incident; however, external entities may be unaware of their role in incident response ahead of time.
LEVEL 3	Organizational staff are aware of **how and when to coordinate** with both **internal** and **external stakeholders** in the event of a security incident. **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.
LEVEL 4	Organizational staff are aware of how and when to coordinate with both internal and external stakeholders in the event of a security incident. 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 are developed and collected related to frequency, success, and efficiency.

RS.CO-5	**Voluntary information sharing occurs with external stakeholders** to achieve broader cybersecurity situational awareness
LEVEL 1	No defined criteria for information sharing focused on the development of awareness of the cybersecurity landscape among outside stakeholders exists.
LEVEL 2	The organization has defined criteria for information that may be shared related to security incidents, including what types of information may be shared and with which outside stakeholders.
LEVEL 3	The organization has **defined criteria for information that may be shared** related to security incidents, including **what types of information** may be shared and **with which outside stakeholders**. Additionally, those stakeholders are aware of what the organization considers appropriate use of that information.
LEVEL 4	The organization has automated mechanisms in place to more efficiently disseminate the appropriate security incident information to the appropriate outside stakeholders. Additionally, those stakeholders are aware of what the organization considers appropriate use of that information.

ANALYSIS CATEGORY

RS.AN-1	**Notifications** from detection systems are **investigated**
LEVEL 1	The organization does not have a defined process to investigate notifications from detection systems.
LEVEL 2	Staff members are aware of the detection systems alerts they are responsible for investigating, however investigation requirements do not exist related to the severity of the alert.
LEVEL 3	Staff members are aware of the detection systems alerts they are responsible for investigating and alerts are **investigated** appropriately **based on the type and severity** of the alert.
LEVEL 4	The organization utilizes automated mechanisms to aggregate, correlate and analyze security notifications from detection systems.

RS.AN-2	The **impact** of the incident is **understood**
LEVEL 1	The organization does not have a process to determine the impact of an incident.
LEVEL 2	The organization is able to determine the systems impacted by an incident, but does not have the visibility to determine the full scope of the incident (e.g. data, users, system performance, etc.).
LEVEL 3	The organization is able to determine the scope (e.g. systems, data, users, system performance, etc.) affected by the incident, but not quantify the impact the incident had on the organization holistically.
LEVEL 4	The organization is able to **determine the scope** (e.g. systems, data, users, system performance, etc.) affected by the incident and **quantify the impact** the incident had on the organization holistically.

RS.AN-3	**Forensics are performed**
LEVEL 1	No process for performing forensics exists.
LEVEL 2	The organization takes steps to preserve systems, logs, and other sources of evidence related to an incident, in the event they are needed for forensic investigation.
LEVEL 3	The organization takes steps to **preserve systems, logs, and other sources of evidence** related to an incident, in the event they are needed for forensic investigation. Additionally, the organization **defines incident types and situations** where forensic investigation is required. In those situations, the investigation is conducted by forensic experts.
LEVEL 4	Automated mechanisms are in place to preserve systems, logs, and other sources of evidence related to an incident, in the event they are needed for forensic investigation. Additionally, the organization defines incident types and situations where forensic investigation is required. In those situations, the investigation is conducted by forensic experts.

ANALYSIS CATEGORY (CONTINUED)

RS.AN-4	**Incidents are categorized** consistent with response plans
LEVEL 1	The organization has not defined categories of incidents to be utilized for identifying incident response actions.
LEVEL 2	The organization has defined categories of incidents to be utilized for identifying incident response actions and appropriately categorizes incidents. Categories of incidents may include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. However, the organization has not assigned appropriate incident response reactions to the defined categories.
LEVEL 3	The organization has **defined categories** of incidents to be utilized for identifying incident response actions and appropriately categorizes incidents. Categories of incidents may include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Additionally, the organization has **assigned appropriate incident response reactions** to the defined categories.
LEVEL 4	The organization has defined categories of incidents to be utilized for identifying incident response actions. Automated mechanisms are used to appropriately categorize incidents, and apply the appropriate incident response actions.

RS.AN-5	**Processes** are established to **receive, analyze and respond to vulnerabilities** disclosed to the organization from **internal** and **external** sources (e.g. internal testing, security bulletins, or security researchers)
LEVEL 1	No processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization.
LEVEL 2	The organization receives vulnerability alerts from internal and external sources, but does not have a process to categorize the severity of the vulnerabilities and respond accordingly.
LEVEL 3	The organization receives **vulnerability alerts from internal and external sources**, and has a manual process to categorize the severity of vulnerabilities and respond accordingly.
LEVEL 4	The organization receives vulnerability alerts from internal and external sources, and has automated processes to categorize the severity of vulnerabilities and implement the appropriate responses.

MITIGATION CATEGORY

RS.MI-1	Incidents are contained
LEVEL 1	The organization has not defined appropriate incident containment strategies for use in its environment.
LEVEL 2	The organization has identified various containment strategies that are appropriate for their environment, such as system shutdown, limiting access, rerouting traffic, network disconnection, disabling functions, etc. However, specific incident types are not mapped to the appropriate containment strategies.
LEVEL 3	The organization has identified various **containment strategies** that are appropriate for their environment, such as system shutdown, limiting access, rerouting traffic, network disconnection, disabling functions, etc. Additionally, **incident types are mapped to the appropriate containment strategies.**
LEVEL 4	The organization has identified various containment strategies that are appropriate for their environment, such as system shutdown, limiting access, rerouting traffic, network disconnection, disabling functions, etc. Additionally, automated mechanisms exist to apply the appropriate containment strategies to the appropriate incident types.

RS.MI-2	Incidents are mitigated
LEVEL 1	The organization has not defined appropriate incident mitigation strategies for use in its environment.
LEVEL 2	The organization has identified various mitigation strategies that are appropriate for their environment, such as malware removal, changing of credentials, removal of accounts, patching vulnerabilities, etc.
LEVEL 3	The organization has identified various **mitigation strategies** that are appropriate for their environment, such as malware removal, changing of credentials, removal of accounts, patching vulnerabilities, etc. Additionally, **incident types are mapped** to the appropriate **mitigation strategies.**
LEVEL 4	The organization has identified various mitigation strategies that are appropriate for their environment, such as malware removal, changing of credentials, removal of accounts, patching vulnerabilities, etc. Additionally, automated mechanisms exist to apply the appropriate mitigation strategies to the appropriate incident types.

IMPROVEMENTS CATEGORY

RS.IM-1	Response plans incorporate **lessons learned**
LEVEL 1	No process to incorporate lessons learned into response plans exists.
LEVEL 2	The organization reviews incidents and how the response process was applied to determine any enhancements that are necessary for the plan. Some factors to consider are: efficiency, communication, incident identification, containment strategy, mitigation strategy, prevention strategy, etc.
LEVEL 3	The organization **reviews incidents** and how the response process was applied to **determine any enhancements that are necessary** for the plan. Some factors to consider are: efficiency, communication, incident identification, containment strategy, mitigation strategy, prevention strategy, etc. Additionally, **during the incident** response process, the organization **keeps records of key events, process activities** applied, and **potential enhancements** to better inform the response improvement discussion.
LEVEL 4	The organization reviews incidents and how the response process was applied to determine any enhancements that are necessary for the plan. Some factors to consider are: efficiency, communication, incident identification, containment strategy, mitigation strategy, prevention strategy, etc. Additionally, during the incident response process, the organization keeps records of key events, process activities applied, and potential enhancements to better inform the response improvement discussion. The organization then uses the information collected and discussed to develop incident response metrics to quantify improvement.

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

TWELVE REGIONAL INFORMATION CENTERS
WORKING AS ONE