

# DATA SECURITY AND PRIVACY STANDARDS

## FOR NEW YORK STATE EDUCATIONAL AGENCIES



## NIST CYBERSECURITY FRAMEWORK

DEVELOPED BY:



VERSION DATE:

**November 2019**

NYS RICS OVERVIEW:

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

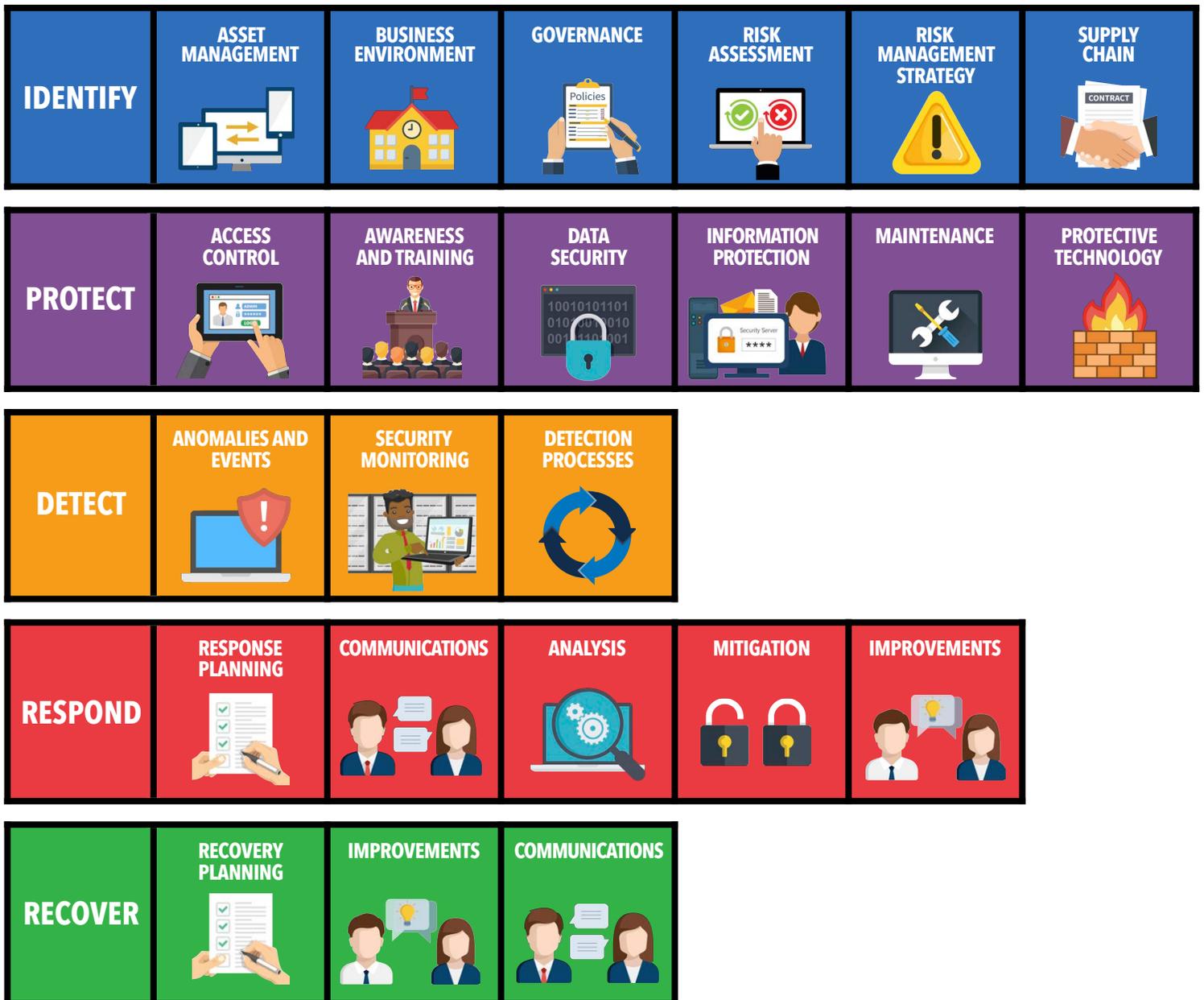
# INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK

## 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



# IDENTIFY FUNCTION

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

## ASSET MANAGEMENT



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

## BUSINESS ENVIRONMENT



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

## GOVERNANCE



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

# IDENTIFY FUNCTION

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

## RISK ASSESSMENT



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

## RISK MANAGEMENT



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

## SUPPLY CHAIN



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

# PROTECT FUNCTION

Develop and **IMPLEMENT APPROPRIATE SAFEGUARDS** to ensure delivery of critical services.

## ACCESS CONTROL



<b>PR.AC-1</b>	<b>Identities</b> and credentials are issued, <b>managed</b> , verified, revoked, and audited for authorized devices, users and processes
<b>PR.AC-2</b>	<b>Physical access to assets</b> is <b>managed</b> and protected
<b>PR.AC-3</b>	<b>Remote access</b> is <b>managed</b>
<b>PR.AC-4</b>	Access <b>permissions</b> and authorizations are <b>managed</b> , incorporating the principles of least privilege and separation of duties
<b>PR.AC-5</b>	<b>Network integrity</b> is <b>protected</b> (e.g., network segregation, network segmentation)
<b>PR.AC-6</b>	<b>Identities</b> are <b>proofed</b> and bound to credentials and asserted in interactions
<b>PR.AC-7</b>	Users, devices, and other assets are <b>authenticated</b> (e.g., single-factor, multi-factor) <b>commensurate with the risk of the transaction</b> (e.g., individuals' security and privacy risks and other organizational risks)

## AWARENESS AND TRAINING



<b>PR.AT-1</b>	All <b>users</b> are informed and <b>trained</b>
<b>PR.AT-2</b>	<b>Privileged users understand roles</b> and responsibilities
<b>PR.AT-3</b>	<b>Third-party stakeholders</b> (e.g., suppliers, customers, partners) <b>understand</b> their roles and <b>responsibilities</b>
<b>PR.AT-4</b>	<b>Senior executives understand</b> their <b>roles</b> and responsibilities
<b>PR.AT-5</b>	Physical and <b>cybersecurity personnel understand</b> their roles and <b>responsibilities</b>

## DATA SECURITY



<b>PR.DS-1</b>	<b>Data-at-rest</b> is <b>protected</b>
<b>PR.DS-2</b>	<b>Data-in-transit</b> is <b>protected</b>
<b>PR.DS-3</b>	<b>Assets</b> are formally <b>managed throughout removal, transfers, and disposition</b>
<b>PR.DS-4</b>	Adequate <b>capacity</b> to <b>ensure availability</b> is <b>maintained</b>
<b>PR.DS-5</b>	<b>Protections against data leaks</b> are implemented
<b>PR.DS-6</b>	<b>Integrity checking</b> mechanisms are used <b>to verify software, firmware, and information integrity</b>
<b>PR.DS-7</b>	The development and <b>testing environment(s)</b> are <b>separate from</b> the <b>production environment</b>
<b>PR.DS-8</b>	<b>Integrity checking</b> mechanisms are used <b>to verify hardware integrity</b>

# PROTECT FUNCTION

Develop and **IMPLEMENT APPROPRIATE SAFEGUARDS** to ensure delivery of critical services.

## INFORMATION PROTECTION



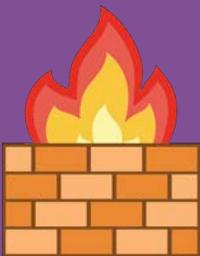
<b>PR.IP-1</b>	A <b>baseline configuration</b> of information technology/industrial control systems is <b>created and maintained</b> incorporating security principles (e.g. concept of least functionality)
<b>PR.IP-2</b>	A <b>System Development Life Cycle</b> to manage systems is <b>implemented</b>
<b>PR.IP-3</b>	<b>Configuration change</b> control <b>processes</b> are in place
<b>PR.IP-4</b>	<b>Backups</b> of information are <b>conducted, maintained, and tested</b>
<b>PR.IP-5</b>	Policy and regulations regarding the <b>physical operating environment</b> for organizational assets are <b>met</b>
<b>PR.IP-6</b>	<b>Data</b> is <b>destroyed according to policy</b>
<b>PR.IP-7</b>	<b>Protection processes</b> are <b>improved</b>
<b>PR.IP-8</b>	<b>Effectiveness of protection</b> technologies is <b>shared</b>
<b>PR.IP-9</b>	<b>Response plans</b> (Incident Response and Business Continuity) <b>and recovery plans</b> (Incident Recovery and Disaster Recovery) are <b>in place</b> and managed
<b>PR.IP-10</b>	<b>Response and recovery plans</b> are <b>tested</b>
<b>PR.IP-11</b>	Cybersecurity is included in <b>human resources practices</b> (e.g., deprovisioning, personnel screening)
<b>PR.IP-12</b>	A <b>vulnerability management plan</b> is developed and <b>implemented</b>

## MAINTENANCE



<b>PR.MA-1</b>	<b>Maintenance</b> and repair of organizational assets are <b>performed and logged</b> , with approved and controlled tools
<b>PR.MA-2</b>	<b>Remote maintenance</b> of organizational assets is <b>approved</b> , logged, and performed in a manner that prevents unauthorized access

## PROTECTIVE TECHNOLOGY



<b>PR.PT-1</b>	<b>Audit/log records</b> are determined, documented, implemented, and <b>reviewed</b> in accordance with policy
<b>PR.PT-2</b>	<b>Removable media</b> is <b>protected and</b> its use <b>restricted</b> according to policy
<b>PR.PT-3</b>	The <b>principle of least functionality</b> is incorporated by configuring systems to provide only essential capabilities
<b>PR.PT-4</b>	<b>Communications and control networks</b> are <b>protected</b>
<b>PR.PT-5</b>	<b>Mechanisms</b> (e.g., failsafe, load balancing, hot swap) are <b>implemented to achieve resilience</b> requirements in normal and adverse situations

# DETECT FUNCTION

Develop and implement appropriate activities to **IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT**.

## ANOMALIES AND EVENTS



- DE.AE-1** A baseline of **network operations and expected data flows** for users and systems is established and **managed**
- DE.AE-2** **Detected events** are **analyzed** to understand attack targets and methods
- DE.AE-3** **Event** data are collected and **correlated** from multiple sources and sensors
- DE.AE-4** **Impact of events** is **determined**
- DE.AE-5** Incident **alert thresholds** are **established**

## SECURITY MONITORING



- DE.CM-1** The **network** is **monitored** to detect potential cybersecurity events
- DE.CM-2** The **physical environment** is **monitored** to detect potential cybersecurity events
- DE.CM-3** **Personnel activity** is **monitored** to detect potential cybersecurity events
- DE.CM-4** **Malicious code** is **detected**
- DE.CM-5** **Unauthorized mobile code** is **detected**
- DE.CM-6** **External service provider activity** is **monitored** to detect potential cybersecurity events
- DE.CM-7** **Monitoring for unauthorized** personnel, **connections**, devices, and software is performed
- DE.CM-8** **Vulnerability scans** are **performed**

## DETECTION PROCESSES



- DE.DP-1** Roles and **responsibilities for detection** are well **defined** to ensure accountability
- DE.DP-2** **Detection activities comply with** all applicable **requirements**
- DE.DP-3** **Detection processes** are **tested**
- DE.DP-4** **Event detection information** is **communicated**
- DE.DP-5** Detection **processes** are **continuously improved**

# 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 event

## COMMUNICATION



**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**

**RS.MI-3** Newly identified **vulnerabilities** are **mitigated** or documented as accepted risks

## IMPROVEMENTS



**RS.IM-1** Response plans **incorporate lessons** learned

**RS.IM-2** Response **strategies** are **updated**

# 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

