

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.

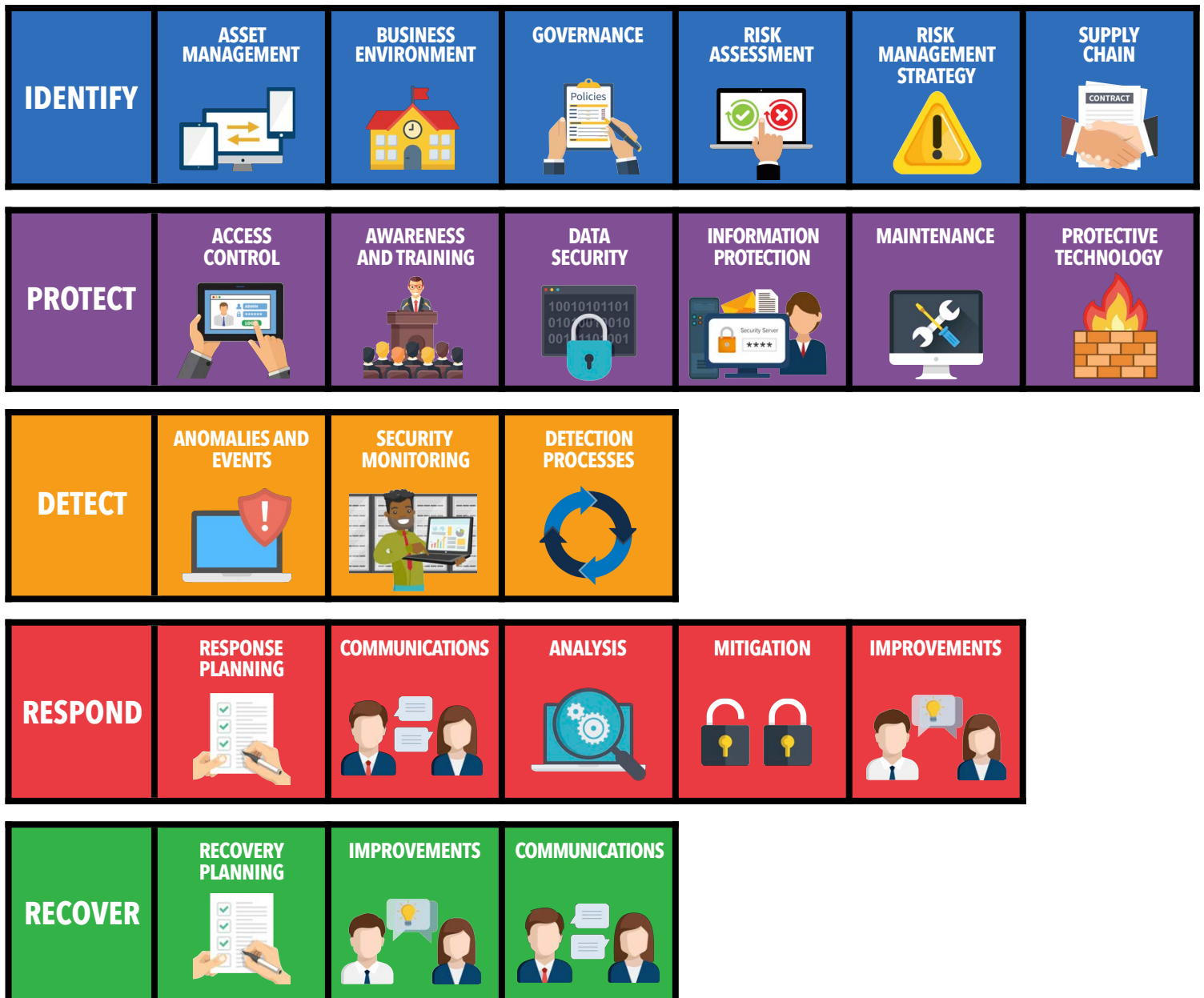
INTRODUCTION TO THE NIST CYBERSECURITY FRAMEWORK



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



- | | |
|---------|---|
| 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

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 |

PROTECT FUNCTION

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

ACCESS CONTROL



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

AWARENESS AND TRAINING



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

DATA SECURITY



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

PROTECT FUNCTION

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

INFORMATION PROTECTION



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

MAINTENANCE



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

PROTECTIVE TECHNOLOGY



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

