

Cybersecurity Risk Management

Cybersecurity Awareness Month
October 2024




New York State Comptroller
THOMAS P. DiNAPOLI

1

Division of Local Government and School Accountability

Applied Technology Unit
Ariel Bethencourt
Nicole Cappiello



New York State Comptroller
THOMAS P. DiNAPOLI

2

Cybersecurity Risk Management

Part One Agenda

- Cybersecurity Risk Management
- Information Security
- Cybersecurity



New York State Comptroller
THOMAS P. DiNAPOLI

3


Cybersecurity Risk Management
What is it?

 New York State Comptroller
THOMAS P. DINAPOLI

4

Cybersecurity Risk Management
What is it?


- **Risk Management** is the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level.

 New York State Comptroller
THOMAS P. DINAPOLI

5

Cybersecurity Risk Management
What is it?

- **Risk management** is a complex, multifaceted activity that requires the involvement of the entire organization.
- There are multiple risk management frameworks and models available.

 New York State Comptroller
THOMAS P. DINAPOLI

6

Cybersecurity Risk Management

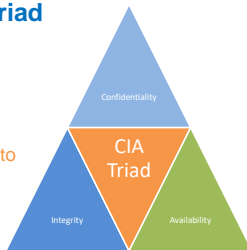
What is it?

- A major part of the **risk management** process is determining any adverse impact with respect to loss of confidentiality, integrity, and availability of systems and data.

Cybersecurity Risk Management

CIA Triad

- The **CIA triad** is a well-known model in information security development. It is applied in various situations to identify problems or weaknesses and to establish security solutions.



Cybersecurity Risk Management

CIA Triad

- The **CIA triad** is comprised of three main components: confidentiality, integrity and availability. Each component represents a fundamental objective of information security.

CIA Triad

Confidentiality

- **Confidentiality** is closely linked with privacy and relates to preventing or minimizing unauthorized access to and disclosure of data and information.
 - Securing online accounts with usernames and passwords is an example of helping to ensure confidentiality.

CIA Triad

Integrity


- **Integrity** is focused on ensuring that data is not tampered with during or after submission.
 - File permissions and user access controls are a way to help ensure the integrity of data.

CIA Triad

Availability

- **Availability** means that the information is available when it is needed. Data that cannot be accessed will prove to be of little value.
 - Maintaining hardware and software and updating and applying software patches as needed are examples of ways to help ensure availability.

Cybersecurity Risk Management
Risk Framing



13

Risk Framing
What is it?


- **Risk framing** is the set of assumptions, tolerances, constraints, priorities, and trade-offs that form an organization's approach to managing risk.
- The purpose of risk framing is to establish a foundation and produce a strategy.



14

Risk Framing
What is it?

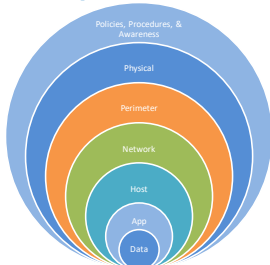
- **Risk framing** foundations include establishing current and necessary controls to protect the organization and system based on possible impact of risk.



15

Risk Framing Defense-in-Depth

- **Defense-in-depth** refers to the implementation of multiple layers of security to help protect data, networks and IT systems.



Risk Framing Defense-in-Depth

- A combination of controls helps ensure that your system does not become overly dependent on any one control or layer of security and provides added protection in case a layer of security fails to function properly or does not prevent or stop a threat to your data or system.

Risk Framing Defense-in-Depth

- Combining multiple preventive, detective and corrective internal controls will help keep your data and systems safe.

Internal Controls

Preventive

- **Preventive** controls are used to help avoid events. For example:
 - Policies and procedures
 - Software patching
 - User control access

Internal Controls

Detective

- **Detective** controls are designed to detect, log, and provide alerts after an event has occurred. For example:
 - Logging and monitoring tools
 - Anti-malware/Anti-virus tools
 - Intrusion Detection Systems (IDS)

Internal Controls

Corrective

- **Corrective** controls are designed to take corrective action on discovered incidents and minimize damage. For example:
 - Effective backups
 - Patching
 - Incident response plans


Cybersecurity Risk Management
Assessing Risk



22

Assessing Risk
What is it?


- A **cybersecurity risk assessment** is an assessment of an organization's ability to protect its information and information systems from cyber threats.



23

Assessing Risk
What is it?

- The purpose of a **cybersecurity risk assessment** is to identify, assess, and prioritize risks to systems and data.
- While risk management is an ongoing process, risk assessments focus on detecting and analyzing potential risks.



24

Assessing Risk

Vulnerability

- A **vulnerability** is a weakness or flaw in a system, process, or set of controls. For example:
 - Employees falling for phishing attempts
 - Unpatched software
 - Security misconfigurations

Assessing Risk

Threat

- A **threat** is anything that can exploit, or make use of, a vulnerability. For example:
 - Phishing attacks
 - Malware
 - Ransomware

Assessing Risk


Risk

- A **risk** is the probability of an incident occurring and the potential level of harm it could cause.



Cybersecurity Risk Management

Responding to Risk




28

Responding to Risk

What is it?

- **Risk response** is any action or response an organization takes towards an existing risk.
- Results from the risk assessment help determine the appropriate **risk response**.





29

Responding to Risk

Common Risk Response Strategies

- **Risk response** strategies are based in the probability of an incident occurring and the potential level of harm it could cause.





30

Responding to Risk

Avoidance

- Risk **avoidance** is when an action or process is deemed too risky and avoided completely. For example:
 - Stopping the use of a certain software due to it no longer being supported

Responding to Risk

Transfer

- Risk **transfer** is when the risk taken on is transferred to a third party. For example:
 - Purchasing cybersecurity insurance policies
 - Outsourcing cybersecurity tasks to external vendors or service providers

Responding to Risk

Mitigation

- Risk **mitigation** is the process of limiting risk exposure and reducing the likelihood of an incident occurring. For example:
 - Installing firewalls or other threat detection software
 - Installing security patches and updates

Responding to Risk

Acceptance

- Risk **acceptance** is when risk exposure has been considered an acceptable level. For example:
 - Keeping a legacy system active but separate from sensitive data environments
 - Allowing employees to connect their own devices if network access is segmented

Cybersecurity Risk Management

Risk Monitoring

Risk Monitoring

What is it?

- **Risk monitoring** is when an organization monitors implemented security controls to verify that they work as intended.

Risk Monitoring

Security Controls

- **Security controls** are the safeguards or countermeasures used to protect the confidentiality, integrity, and availability of a system and its information.

Security Controls

Administrative

- **Administrative** controls refer to an organization's policies, procedures, and guidelines. For example:
 - Incident response
 - Backup procedures
 - User education

Security Controls

Technical

- **Technical** controls are the hardware and software components that help protect a system. For example:
 - Firewalls
 - Encryption
 - Intrusion Detection Systems (IDS)

Security Controls

Physical

- **Physical** controls are used to help prevent or detect unauthorized access to physical assets. For example:
 - Access cards or security badges
 - Fences or gates
 - Surveillance cameras

Risk Monitoring

Dynamic Management

- **Risk monitoring** should include surveying the current threat landscape, emerging threats and technologies.
- Staying current allows organizations to continuously improve cybersecurity programs and cybersecurity risk management strategies.

Cybersecurity

Resources

Information Technology Governance


Local Government Management Guide

Information Technology Governance



Security Self-Assessment





New York State Comptroller
THOMAS P. DINAPOLI

43

Cyber Profile

Division of Local Government and School Accountability

Cyber Profile

October 2023




New York State Comptroller
THOMAS P. DINAPOLI

44

LGSA Resources

LGSA's Cybersecurity Resources	
Audit Reports	https://www.osc.state.ny.us/local-government/audits
Training	https://www.osc.state.ny.us/local-government/academy
Publications	https://www.osc.state.ny.us/local-government/publications
LGSA Help Line	localgov@osc.ny.gov or (866) 321-8503 or (518)-408-4934
ATU Cybersecurity Team	Muni-Cyber@osc.ny.gov or (518) 738-2639



New York State Comptroller
THOMAS P. DINAPOLI

45

Additional Resources

Additional Cybersecurity Resources	
NYS Association of Counties	https://www.nysac.org/cyber
NYS RIC One	https://riconedpss.org/
NYS Office of Information Technology Services (ITS)	https://www.its.ny.gov/
NYS Police Computer Crime Unit (CCU)	https://troopers.ny.gov/computer-crimes
Open-Source Web Application Security Project (OWASP)	https://owasp.org
United States Department of Justice Cybercrime	https://www.justice.gov/criminal-ccips

Additional Resources

Additional Cybersecurity Resources	
Center for Internet Security (CIS)	https://www.cisecurity.org/
Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/
Federal Bureau of Investigation (FBI)	https://www.fbi.gov/investigate/cyber
Multi-State Information Sharing and Analysis Center (MS-ISAC)	https://www.cisecurity.org/ms-isac
National Institute of Information Technology Services (NIST)	https://www.nist.gov/cybersecurity
NYS Division of Homeland Security and Emergency Services (DSHES)	https://www.dshes.ny.gov/cyber-incident-response-team

Cybersecurity Awareness Month

Part 2 Sneak Preview

Questions?

Contact us

- LGSA Applied Technology Unit's Cybersecurity Team
- Muni-Cyber@osc.ny.gov
- LGSA Help Line
 - 1-866-321-8503 or
 - 518-408-4934

Thank You