

Cybersecurity for Local Governments and Schools: A 2-Part Live Webinar Series



New York State Comptroller
THOMAS P. DINAPOLI



1

Part 2 – Cybersecurity Standards: A Case Study



New York State Comptroller
THOMAS P. DINAPOLI



2

Division of Local Government and School Accountability (LGSA)

Applied Technology Unit (ATU)
Information Systems Auditors

John Martin
Nicholas De La Rosa

3

Part 2 Agenda

- Part 1 Recap
- Cybersecurity Standards Overview
- Common Cybersecurity Standards
- Choosing a Standard
- Relationships between Standards
- Case Study
- Cybersecurity Standards Summary
- Cybersecurity Resources

New York State Comptroller
THOMAS P. DINAPOLI



4

Part 1 Recap

Effective Cybersecurity Awareness Training

- Effective cybersecurity awareness training is crucial to help:
 - Prevent data breaches.
 - Protect information technology (IT) systems from unauthorized access and use.
 - Recognize and properly report cybersecurity incidents that may occur.
- A local government's or school's governing board and chief executive officer should ensure a culture and tone that encourages cybersecurity awareness.
- Assessments of training effectiveness should evaluate awareness and could measure for enhancements in cybersecurity knowledge, reinforcement of practices that help safeguard IT systems and data, and redirection from practices that may expose IT systems and data to cybersecurity risks and threats.

New York State Comptroller
THOMAS P. DINAPOLI

5

Cybersecurity Standards Overview

- IT systems, historically, were not always designed with security built in by default. IT system administrators generally need to evaluate, update and configure settings before a newly implemented IT system can be used securely.
- Cybersecurity standards provide a framework for consistently evaluating, securing, managing, and operating IT systems across a local government or school.
- Some cybersecurity standards are well-known and widely-adopted across a variety of organizations or within certain sectors (e.g., government, academia, water, emergency services).

New York State Comptroller
THOMAS P. DINAPOLI

6

Cybersecurity Standards Overview (continued)

- Local governments and schools operate interconnected IT systems, in some cases encompassing hundreds or thousands of components that may include network devices, applications, user accounts, and cloud services.
- Consistently following one or more applicable cybersecurity standards can help a local government or school to, for the myriad of components:
 - Establish minimum cybersecurity requirements.
 - Identify cybersecurity weaknesses.
 - Reduce cybersecurity risk.
 - Protect personal, private and sensitive information.
 - Measure cybersecurity performance.
 - Establish accountability.
 - Demonstrate regulatory compliance.
 - Establish criteria for cybersecurity audits and assessments.

New York State Comptroller
THOMAS P. DINAPOLI

7

Cybersecurity Standards Overview (continued)

Cybersecurity standards define industry best practices that can be used to help protect IT systems, networks, applications, and data. A cybersecurity standard may address one or more areas key to safeguarding from cybersecurity threats, such as:

- Access control
- Authentication
- Awareness and training
- Backup and recovery
- Data protection
- Incident response
- Governance
- Network security
- Risk management
- Security monitoring
- System configuration
- Vulnerability management

New York State Comptroller
THOMAS P. DINAPOLI

8

Cybersecurity Standards Overview (continued)

The term, cybersecurity standard, is used to refer to a variety of publications, many of which were intended to serve and are used for different purposes:

- **Frameworks** help organize cybersecurity activities and desired outcomes.
- **Control catalogs** provide structured lists of detailed cybersecurity controls.
- **Benchmarks** provide specific technical configuration recommendations.
- **Vendor guidance** describes how particular products should be configured.
- **Regulatory standards** establish requirements that a local government or school may be legally or contractually obligated to follow.

New York State Comptroller
THOMAS P. DINAPOLI

9

Common Cybersecurity Standards

Standard	Source
United States (US) National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF)	https://www.nist.gov/cyberframework
International Organization for Standardization (ISO)/International Electrotechnical Commission's (IEC) 27001: Information Security, Cybersecurity and Privacy Protection	https://www.iso.org/standard/27001
US NIST Special Publication (SP) 800-53: Security and Privacy Controls for Information Systems and Organizations	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
Multi-State Information Sharing and Analysis Center (MS-ISAC)/Center for Internet Security's (CIS) Critical Security Controls (CSC)	https://www.cisecurity.org/controls
MS-ISAC/CIS's Benchmarks	https://www.cisecurity.org/cis-benchmarks
Sector-specific regulatory frameworks/standards	https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
Vendor-developed software documentation/manuals	*Varies

New York State Comptroller
THOMAS P. DINAPOLI

10

Sector-Specific Regulatory Frameworks/Standards

Some local governments and schools must comply with certain cybersecurity-related requirements based on their industry, services, information, contracts, or jurisdiction. Examples include:

- | | |
|--|---|
| <ul style="list-style-type: none">• Federal requirements• State requirements• Critical infrastructure requirements | <ul style="list-style-type: none">• Educational requirements• Healthcare requirements• Payment card requirements• Contractual requirements |
|--|---|

New York State Comptroller
THOMAS P. DINAPOLI

11

11

Choosing a Standard

Finding the right balance

Security

- Protect data confidentiality
- Prevent threats
- Manage risk
- Comply with regulations
- Monitor and detect incidents

Access

- Available when needed
- Productive and efficient
- Innovative
- Collaborative
- User-friendly

New York State Comptroller
THOMAS P. DINAPOLI

12

Relationships between Standards

Multiple frameworks could also be used in coordination with each other, to help guide efforts towards different cybersecurity aspects. For example:

- **Why:** US NIST's CSF could be used when developing a high-level cybersecurity governance strategy.
- **When:** MS-ISAC/CIS's CSC could be used when prioritizing controls for implementation.
- **What/How:** Vendor-developed software manuals could be used when configuring IT systems' security settings.

New York State Comptroller
THOMAS P. DINAPOLI

13

Case Study | Background

Several tools are available to help IT system administrators assess and validate IT system cybersecurity in relation to one or more applicable standards:

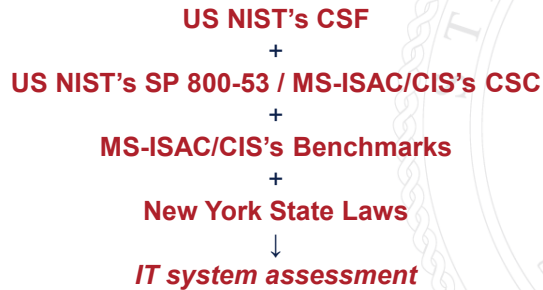
- Manual self-assessments
- Automated baseline analyzers/configuration assessors
- Dynamic network and web vulnerability scanners
- Continuous, real-time monitors

New York State Comptroller
THOMAS P. DINAPOLI

14

Case Study | Background (cont.)

IT system assessments should be driven by selected, applicable standards. For example:



New York State Comptroller
THOMAS P. DINAPOLI

15

Case Study | Background (cont.)

US NIST's CSF organizes recommended activities around six cybersecurity functions:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Source: US NIST, CSF
<https://www.nist.gov/cyberframework>

New York State Comptroller
THOMAS P. DINAPOLI

16

Case Study | Background (cont.)

US NIST's SP 800-53 organizes recommended controls into families:

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Assessment, Authorization and Monitoring (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Program Management (PM)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- Supply Chain Risk Management (SR)

Source: US NIST, SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
<https://www.nist.gov/cyberframework>

New York State Comptroller
THOMAS P. DINAPOLI

17

Case Study | Background (cont.)

MS-ISAC/CIS's CSC defines an industry agreed-upon collection of the top 18 cybersecurity best practices, categorized as:

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email and Web Browser Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

Source: MS-ISAC/CIS, CSC
<https://www.cisecurity.org/controls>

New York State Comptroller
THOMAS P. DINAPOLI

18

Case Study | Background (cont.)

MS-ISAC/CIS's Benchmarks provide detailed, step-by-step recommendations for securely configuring a variety of technology, including specific operating systems, applications, databases, network devices and cloud services.

- **Level 1 - Foundational:** Provides a strong baseline that protects against common threats with minimal impact to operations.
- **Level 2 - Enhanced:** Provides a higher level of cybersecurity with additional controls that reduce risk but may impact operational flexibility.
 - * The level that's appropriate for your local government or school will depend on a number of factors, including the nature of the operations and data involved, applicable statutory requirements, and cybersecurity governance strategy.

Source: MS-ISAC/CIS, Benchmarks
<https://www.cisecurity.org/cis-benchmarks>

New York State Comptroller
THOMAS P. DINAPOLI

19

Case Study | Background (cont.)

New York State laws require:

- Local governments to adopt a notification policy or local law that requires notification to be given to affected individuals when their private information is compromised or is reasonably believed to be compromised.

Source: New York State Technology Law Section 208

- Local government employees who use technology as a part of their official job duties to take annual cybersecurity awareness training.

Source: New York State Technology Law Section 103-f

- Local governments to report cybersecurity incidents and ransom demands to the New York State Division of Homeland Security and Emergency Services (DHSES) no later than 72 hours after the local government reasonably believes the incident occurred.

- * The cybersecurity incident report to DHSES must include whether the reporting local government is requesting or declining advice and/or technical assistance from DHSES.

Source: General Municipal Law Article 19-C

New York State Comptroller
THOMAS P. DINAPOLI

20

20

Case Study | Preparing to Run a Configuration Assessor

- Identifying IT systems to test.
- Selecting the appropriate baseline(s).
- Configuring test options (e.g., protocols, authentication).
- Scheduling the test run.
- Verifying successful test completion.

New York State Comptroller
THOMAS P. DINAPOLI

21

Case Study | Evaluating Configuration Assessor Results

- Eliminating false positives.
- Determining likely resulting impacts.
- Identifying highest risks.
- Prioritizing and assigning remediation efforts.
- Confirming and documenting corrective action.

New York State Comptroller
THOMAS P. DINAPOLI

22

Case Study | Weakness

Vulnerable Encryption Type Allowed

Security settings are not configured to prohibit vulnerable encryption types, including the Local Area Network (LAN) Manager (LM) authentication protocol and the New Technology LM authentication version 1 (NTLMv1) protocol, both of which have vulnerabilities that could allow encrypted passwords to be viewed in readable plaintext.

- * Whenever passwords are stored, they should be protected using strong encryption to minimize the risk that they could be stolen and used for unauthorized access, misuse or disruption.

Source: Microsoft, Security guidance for NTLMv1 and LM network authentication

<https://support.microsoft.com/en-us/servicing/os/windows-server/2017/01/security-guidance-for-ntlmv1-and-lm-network-authentication>

New York State Comptroller
THOMAS P. DINAPOLI

23

Case Study | Remediation

Prohibit Vulnerable Encryption Types

Configure the security setting,
Network security: LAN Manager authentication level
to

Send NTLMv2 response only. Refuse LM & NTLM

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:Lm
CompatibilityLevel

Computer Configuration\Policies\Windows Settings\Security
Settings\Local Policies\Security Options\Network security:
LAN Manager authentication level

Source: MS-ISAC/CIS, Microsoft Windows Server Benchmark

https://www.cisecurity.org/benchmark/microsoft_windows_server

New York State Comptroller
THOMAS P. DINAPOLI

24

Cybersecurity Standards Summary

- IT systems, historically, were not always designed with security built in by default.
- Cybersecurity standards provide a framework for consistently evaluating, securing, managing, and operating IT systems across a local government or school.
- Consistently following one or more applicable cybersecurity standards can help reduce risk, improve efficiency, and/or demonstrate due diligence to stakeholders
- Multiple frameworks could be used in coordination with each other, to help guide efforts towards different cybersecurity aspects.

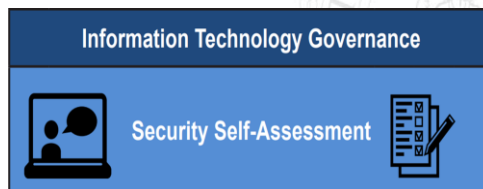
New York State Comptroller
THOMAS P. DINAPOLI

25

Information Technology Governance Local Government Management Guide

<https://www.osc.ny.gov/files/local-government/publications/pdf/IT-Governance-Self-Assessment-Form.pdf>

<https://www.osc.ny.gov/files/local-government/publications/pdf/information-technology-governance.pdf>



New York State Comptroller
THOMAS P. DINAPOLI

26

New York Local Government and School Cybersecurity: A Cyber Profile

<https://www.osc.ny.gov/files/local-government/publications/pdf/nys-local-gov-school-cyber-profile.pdf>



New York State Comptroller
THOMAS P. DINAPOLI

27

LGSA Resources

LGSA 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

28

Additional Resources

Additional Cybersecurity Resources

Center for Internet Security (CIS)	https://www.cisecurity.org/
Multi-State Information Sharing and Analysis Center (MS-ISAC)	https://www.cisecurity.org/ms-isac
NYS Division of Homeland Security and Emergency Services (DHSES)	https://www.dhSES.ny.gov/cyber-incident-response-team
NYS Office of Information Technology Services (ITS)	https://www.its.ny.gov/
NYS Police Computer Crime Unit (CCU)	https://troopers.ny.gov/computer-crimes

New York State Comptroller
THOMAS P. DINAPOLI

29

Additional Resources

Additional Cybersecurity Resources (continued)

United States Cybersecurity and Infrastructure Security Agency (CISA)	https://www.cisa.gov/
United States Department of Justice (DOJ) Cybercrime	https://www.justice.gov/criminal-ccips
United States Federal Bureau of Investigation (FBI)	https://www.fbi.gov/investigate/cyber
United States National Institute of Standards and Technology (NIST)	https://www.nist.gov/cybersecurity

New York State Comptroller
THOMAS P. DINAPOLI

30

Questions?

Contact Us

- LGSA Applied Technology Unit
Cybersecurity Team
 - Muni-Cyber@osc.ny.gov
 - (518) 738-2639
- LGSA Help Line
 - 1-866-321-8503 or
 - 518-408-4934

New York State Comptroller
THOMAS P. DINAPOLI



31

Thank you.



New York State Comptroller
THOMAS P. DINAPOLI



32