Cybersecurity Framework

1st Edition

November 15, 2022

Overview

The New Jersey Cyber Risk Management Fund (Cyber JIF) was established to provide cyber insurance and risk management to local governments in New Jersey. At the core of the Cyber JIF is this cybersecurity framework, which is specifically designed for the local government members of the Cyber JIF. It provides a logical guide to achieving your cybersecurity goals taking into account the current cyber risk environment and cost and effectiveness of the security controls.

The Cyber JIF recognizes that much of the terminology and technical aspects of the framework might not make sense to everyone; therefore, it is critical this program be reviewed and enacted on with the assistant of a technology expert.

While all members are covered by cyber insurance, the per claim deductible as of January 1, 2023 is $50,000 plus 20% coinsurance of the next $300,000 (up to $110,000 out of pocket). Members become eligible for deductible reduction worth up to $110,000 by complying with the security controls outlined in this framework.

In order to qualify for the deductible reduction, follow these steps:

1. Submit the Certification checklist.
    - All items in the security group must be “Yes” to comply.
    - You may submit “No” or “Not Applicable” responses for consideration, but they must have detailed explanations.
2. At the time of a claim, submit the Deductible Reduction checklist and provide the supporting documentation requested.

Deductible Reductions Groups

1. **Minimum Security**: Deductible reduced to $25,000 (up to $85,000 in savings)
2. **Advanced Security**: Deductible reduced to $0 (up to $100,000 in savings)

Many of the security controls involve little or no cost (i.e., activating Microsoft Defender), while others will incur costs (i.e., subscription-based cloud backup). In all cases, the framework is designed considering the limited budgets of the members, and so the minimum standards will provide the most security for the lowest cost.

Keep in mind, these are only minimum standards, and they will not eliminate all technology risks.

These controls will provide a strong level of protection if effectively carried out but are only a minimum baseline. Also, cyber risks constantly evolve. This means you must constantly monitor your cybersecurity posture so your organization can respond to new threats and risks as warranted.

Table of Contents

Appendices

Getting Started!

1. GET A TECHNOLOGY EXPERT!

2. Review the Cybersecurity Framework with your technology expert.
3. Develop a plan, timetable, and budget to implement the standards.
4. Once implemented, complete the Certification checklist.
5. Establish a process to annually review your technology risks and ensure the program continues to be met.

Want to learn more about technology risks? See the work done by the Rutgers Bloustein Local Government Research Center on Technology Risk: http://blousteinlocal.rutgers.edu/managing-technology-risk/

Minimum Security

Control	CIS v8	Description	Comments
Asset Management	**Inventory and Control of Enterprise Assets (CIS 1)**	1. Inventory your technology ecosystem: Workstations, end-user devices, network devices, servers, etc.	Make sure cloud and IoT are also contemplated.
	Inventory and Control of Software Assets (CIS 2)	1. Inventory your technology ecosystem: Software: Operating systems and applications	
	Network Infrastructure Management (CIS 12)	1. Maintain network diagram. 2. Segment employee Wi-Fi from customer/public Wi-Fi.	
Data Management	**Data Protection (CIS 3)**	1. Create data management process that addresses data sensitivity, owner, retention and disposal. 2. Files with personally identifiable information (PII), protected health information (PHI) and other sensitive/confidential information are password protected or encrypted while being stored and shared. 3. Adhere to any additional cybersecurity practices required by applicable laws or regulations. 4. Inventory your data: Focus on Personally Identifiable Information (PII), Private Health Information (PHI) and other confidential information (police records, video, etc.)	
	Data Recovery (CIS 11)	1. Weekly, off-network, off-premises full backup of all data.	
Account Management	**Account Management (CIS 5)**	1. Maintain inventory of accounts: a. Users, b. Administrator / Elevated privileges, c. Service accounts, d. Shared accounts. 2. Separate administrative/elevated privilege accounts from user accounts and restrict privileges (such as web browsing and email) on admin accounts.	
	Access Control Management (CIS 6)	1. Must adopt a password policy that at least meets the standards set in the attached Cyber JIF Password Policy or meet the NIST Password Standards 800-63B (03/02/2020 Updates), and as further updated. 2. Utilize a Virtual Private Network (VPN) and Multi Factor Authentication (MFA) for all remote connections to your network. 3. Require MFA when accessing cloud-based applications (where capable). 4. Disable or delete accounts that are dormant or inactive for 45 days. 5. Users with administrator rights are limited to those who need them. 6. Non-administrator users are granted limited rights based on job function and responsibility. 7. Access rights are updated upon any personnel status change action. 8. Access rights for each individual are reviewed at least every six (6) months.	1. https://pages.nist.gov/800-63-3/sp800-63b.html
Vulnerability Management	**Continuous Vulnerability Management (CIS 7)**	1. Adopt a practice of installing all security and critical updates and patches as soon as practicable based on risk and operational impact, but no longer than a month for high and critical vulnerabilities as defined by CVSS. 2. Keep all operating software, application software and infrastructure equipment current with latest versions. 3. Annually review all non-standard applications for replacement/upgrade. 4. Scan your ecosystem with a vulnerability management tool on a monthly or more frequent basis.	1. For high and critical vulnerabilities that cannot be patched in a month, create an exception process that documents the vulnerability and plan to remediate or otherwise implement a compensating control for the risk. https://www.first.org/cvss/ https://nvd.nist.gov/vuln-metrics/cvss

Minimum Security

Control	CIS v8	Description	Comments
Defensive Tools & Strategies	**Email and Web Browser Protections (CIS 9)**	1. Ensure only fully supported browsers and email clients are in use. 2. Add a clear and obvious automatic warning banner to all emails coming from outside of your organization.	
	Malware Defenses (CIS 10)	1. Microsoft Office applications open all downloaded files in "Protected Mode". 2. Antivirus enabled for all desktops and laptops / servers 3. Firewalls enabled for all desktops and laptops / servers 4. Antispam and antivirus filters enabled for the mail server 5. Firewall rules and policies need to be reviewed or reassessed at least twice per year 6. Disable autorun for all removable media. 7. Virus scan any removeable media before permitting connection. 8. Disable unused ports	
	Network Monitoring Defense (CIS 13)	1. Utilize endpoint detection and response (EDR) tool across entire network.	The Endpoint Detection and Response Solutions (EDR) market is defined as solutions that record and store endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems. EDR solutions must provide the following four primary capabilities: 1) Detect security incidents, 2) Contain the incident at the endpoint, 3) Investigate security incidents, 4) Provide remediation guidance. https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions
	Secure Configuration of Enterprise Assets and Software (CIS 4)	1. Ensure there are no default accounts or passwords on any organization devices.	
Cyber Hygiene	**Security Awareness and Skills Training (CIS 14)**	1. All computer, network or email users receive annual training of at least one hour, including these topics, with such training including phishing exercises: a. Malware Identification b. Password construction c. Identifying and responding to security incidents d. Social engineering attacks 2. Leadership briefed annually on state of security for the organization, including high impact incidents (breach/loss of PII, funds fraud, intrusion, etc.). 3. Register with Multi-State Information Sharing & Analysis Center (MS-ISAC) and New Jersey Cybersecurity Communication and Integration Cell (NJCCIC). If a Utility Authority, register with your respective ISAC, such as Water ISAC.	3. NJCCIC: https://cyber.nj.gov/members/ MS-ISAC: https://learn.cisecurity.org/ms-isac-registration
3rd Party Risk Management	**Service Provider Management (CIS 15)**	1. Maintain an inventory of third-party providers. 2. High Risk Vendors only (IT, Health, PII/PHI): a. Ensure contracts include security requirements, indemnification, and proper insurance. b. Utilize a 3rd Party Risk Assessment Tool for new/renewing contracts.	2.a. See the Cyber JIF's insurance recommendations. 2.b. See the Cyber JIF's 3rd Party Risk Assessment tool. https://www.vendorsecurityalliance.org/downloadQuestionaire https://cloudsecurityalliance.org/artifacts/star-level-1-security-questionnaire-caiq-v4/

Minimum Security

Control	CIS v8	Description	Comments
Policies & Procedures	**Incident Response Management (CIS 17)**	1. Management adopts a cybersecurity incident response plan to direct staff and guide technology management decision making when a cybersecurity incident takes place, which must include at a minimum the items in the Cyber JIF's Cybersecurity Incident Response Plan. 2. Management adopts a Technology Practices Policy, which must include at a minimum each of the subject items outlined in the Cyber JIF's Cyber Risk Management Program. 3. Establish procedures requiring multiple approvals for requests to change banking information. 4. Establish procedures requiring multiple approvals and source verification for financial transaction requests over a certain threshold.	

Advanced Security

Control	CIS v8	Description	Comments
Asset Management	Inventory and Control of Enterprise Assets (CIS 1)	1. Servers are physically protected from unauthorized access and environmental hazards. 2. Maintain ability to generate asset inventory on demand. 3. Use active discovery tool, including MDM that can install and updated programs on demand. 4. Address unauthorized devices.	3. Active discovery techniques send various types of network packets, such as Internet Control Message Protocol (ICMP) pings, to solicit responses from network hosts, generally through the use of an automated tool. Some examples include Nessus Vulnerability Scanner, NMAP, and Zenmap https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
	Inventory and Control of Software Assets (CIS 2)	1. Maintain ability to generate software inventory on demand. 2. Use an automated inventory tool. 3. Address unauthorized software. 4. Ensure a user without explicit admin privileges is prevented or unable to install software that is not on the approved software inventory.	
	Network Infrastructure Management (CIS 12)	1. Segment your network, separating key units, such as Finance, Human Resources, Police, Utilities, etc.	1. This control is very contingent on your organization's size, but even utilizing vLANs can be cost- and security-effective. Police are typically already separated. Utilities are critical to separate, particularly the Utility's ICS network.
Data Management	Data Protection (CIS 3)	1. Enforce data management process and ensure proper classification, retention, and disposal. 2. Encrypt all data on removable media.	
	Data Recovery (CIS 11)	1. Deploy a data loss prevention tool. 2. Move rarely-/un-used data off of the live network to off-network or segmented storage. 3. Use of standardized system images or virtualized desktops 4. Application, Operating System and Network Configuration Software: Back-up copy of current versions must always be available with a copy stored off-premises 5. Locally Stored Data (including MS 365, Google Workspace and similar): a. Daily incremental backups with minimum of 14 days of versioning on off-network device. b. All backups are spot-checked monthly. 6. Cloud-Based Applications and Data: Must meet the same standards as the Locally Stored Data. 7. Third-Party Application Data: Vendor must meet the same standards as the Locally Stored Data.	
Account Management	Account Management (CIS 5)	1. Must be able to generate inventory on demand.	
	Access Control Management (CIS 6)	1. Use an enterprise password management solution. 2. Use password manager or specialized PAM tool 3. Periodically test all email addresses with an email breach service to determine if any emails have been compromised and take necessary action to ensure integrity.	2. A password manager is a type of software that can store and create complex passwords for various applications and websites. The user will only need to memorize a master password for this type of solution. Some examples include LastPass and 1Password, A Privileged Access Management (PAM) tool manages execution of privileges, but especially important for elevated privileges. This extends beyond storage of passwords. PAM tools are able apply granular control of privilege execution beyond what exists in applications and remove privileges after execution is complete. PAM tools can manage accounts with username and passwords or stored secrets. Some examples of PAM are CyberArk, and Thycotic
Vulnerability Management	Continuous Vulnerability Management (CIS 7)	1. Use automatic updating where practicable, particularly as related to security patches.	

Advanced Security

Control	CIS v8	Description	Comments
Logging	**Audit Log Management (CIS 8)**	1. Logging must be setup for entire network/all devices, such as System, Application and Security logs. 2. Spot check logs monthly. 3. Centralize log collection and build detections off collected logs.	
Defensive Tools & Strategies	**Email and Web Browser Protections (CIS 9)**	1. Ensure only fully supported plug-ins for browsers and email clients are in use. 2. Deploy protective DNS for the ecosystem	MS-ISAC offers a Protective DNS service. See here for details: https://www.cisecurity.org/ms-isac/services/mdbr
	Malware Defenses (CIS 10)	1. Use anti-exploitation and behavior-based anti-malware tools.	
	Network Monitoring Defense (CIS 13)	1. 24x7 support by phone or email in case of incident. 2. Maintain automated robust alerting and reporting that can prompt human interdiction on a 24x7 basis.	
Cyber Hygiene	**Security Awareness and Skills Training (CIS 14)**	1. Administrators and privileged users receive specialized training. 2. Organization leadership has access to expertise that supports technology decision making (i.e., risk assessment, planning, and budgeting).	
3rd Party Risk Management	**Service Provider Management (CIS 15)**	1. For all vendors, ensure contracts include security requirements, indemnification and proper insurance. 2. For all vendors, utilize a 3rd Party Risk Assessment Tool for all contracts. 3. Risk rank third party providers based on accesses and service provided. 4. Use monitoring solution with continuous monitoring and assessment of third party (high risk).	See the 3rd Party Risk Assessment comments in Minimum Security.
Policies & Procedures	**Incident Response Management (CIS 17)**	1. Develop a Business Continuity Plan for everything technology related.	1. Consider utilizing your Continuity of Government (CoG) plans as a starting point, but now addressing technology assets.
Penetration Testing	**Penetration Testing (CIS 18)**	1. Perform Penetration Testing on an annual basis.	A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources. https://csrc.nist.gov/glossary/term/penetration_testing