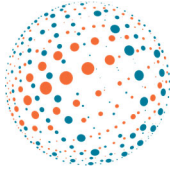


NETHOPE



NetHope Member CIS Controls Benchmarking Report

IMPLEMENTATION GROUP 1

NOVEMBER 2021

A young girl with dark hair and a pink shirt is holding up a piece of lined paper with a drawing of a person. She is in a crowd of people, and the background is slightly blurred. The image has a semi-transparent orange and white diagonal overlay.

NETHOPE

// In an age of digital identities, digital access to services, and digital targeting, cyberattacks can be life threatening for vulnerable and marginalized people that nonprofits serve. //

– Lance Pierce, NetHope CEO

TABLE OF CONTENT

I. Introduction.....	1
II. Executive Summary	3
III. Assessment Goals	5
IV. CIS Controls Definition.....	6
V. Maturity Model Definition	7
VI. Scope of Assessment	8
VII. Key Findings	9
VIII. Recommended Actions.....	21

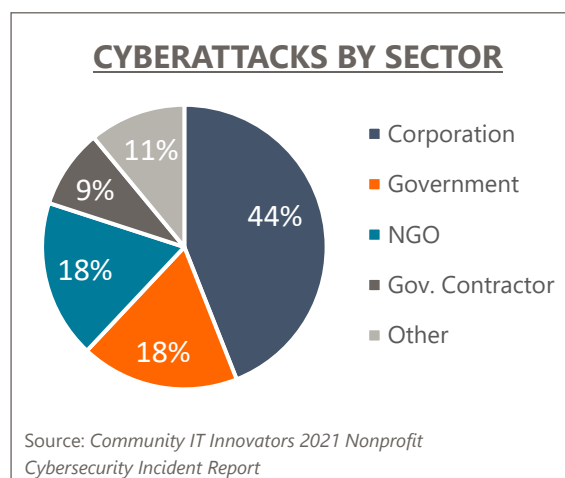
I. INTRODUCTION

[NetHope](#), a consortium of over 60 global NGOs, partnered with Okta to build the capacity of its [Members](#) to transform their digital operations starting by assessing their information security posture. This meta-analysis provides a common baseline understanding of the state of information security and the correlating scale of the risk across these nonprofits.

Information security is a growing concern for all, and especially for nonprofits.

Today, nonprofits are not 'just' on the sidelines of targeted attacks, they have become targets themselves. According to recent research by Microsoft, "31% of all nation-state notifications [of targeted attacks] that [Microsoft] sends out to organizations go to nonprofits. These are organizations that are human rights organizations, think-tanks, organizations with sensitive information that nation-states want to get their hands on. Cybersecurity threats are on the rise, and most nonprofit organizations do not have the same advanced network security protocols or resources or security models that a well-funded private corporation might have. 70% of nonprofit organizations haven't conducted a vulnerability assessment, 80%, based on [Microsoft's] research, don't have a cybersecurity strategy in place. And that just makes cybersecurity threats more of a reality each and every day. The attacks are becoming more sophisticated."¹

Today, nonprofits are not 'just' on the sidelines of targeted attacks – they have become targets themselves.



So, to protect against these exponentially growing threats, information security management professionals need to apply robust controls and measurement frameworks at various levels of infrastructure and management to gain visibility of their ecosystem to protect their networks, servers, and end-user devices. And, in the case of nonprofits, even more crucially they need to robustly protect the personal information of the people they work with – the people and communities that are the most vulnerable.

During this project, NetHope assessed its Members' security programs using a common framework to better identify common cybersecurity risks and provide a high-level overview of each organization's current state. Several NetHope Members utilize a variety of frameworks and standards with varying levels of detail to guide these efforts. For our criteria, we chose to use the [Center for Internet Security's CIS Controls](#) (Version 7), a prioritized list of 20 high-priority defensive measurements and actions that provide a starting point for organizations to improve their information security defense. The controls are divided

¹ <https://www.zdnet.com/article/microsoft-announces-security-programs-for-nonprofits-as-nation-state-attacks-increase/>

into three categories – [basic, foundational, and organizational](#). This assessment covers the Implementation Group 1 of the controls, which are defined as key controls that should be implemented in every organization for essential cyber defense readiness.

NetHope employed the [CIS CSAT](#) (Control Self-Assessment Tool) to measure the information security maturity of each participating Member. In the following pages, we present our assessment results as tables and supporting graphics showing whether a particular control is implemented, partially implemented, or not implemented at all. Hopefully, this will provide Members with a quick snapshot of their areas of improvement. Note that the assessment does not consider an individual organization's risk appetite. So, while these controls are considered basic by many security practitioners, organizational leadership may choose not to fully implement a control to the highest level possible if they believe the cost of doing so outweighs the risk.

This assessment concluded that Members should update their security program to reflect recent statewide changes in governance structures, as well as address weaknesses in inventory management, vulnerability management, control of administrative accounts, configuration change management, and audit logging processes.

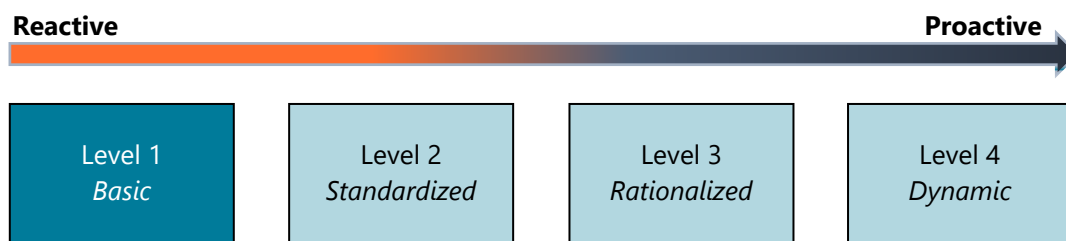
This report is not intended to be a detailed control analysis or a security audit, but merely a meta-analysis of the maturity of NetHope Members and a proxy for the wider global humanitarian and conservation nonprofit sector. Due to evolving threats and other changing variables, the accuracy of this report will likely diminish over time.

II. EXECUTIVE SUMMARY

This report is the result of an information security assessment that was executed for [NetHope Members](#) during April - October 2021. It is intended to provide an overall review of NetHope Member's information security posture and practices. The information security maturity of NetHope Members was measured through a [CIS \(Center for Internet Security\)](#) questionnaire/survey known as [CIS CSAT](#) (Control Self-Assessment Tool).

A. Organizational Ratings

After reviewing the [CIS controls \(v7.1\) Implementation Group 1](#) questionnaire (described in detail later), the assessment of NetHope Members' information security posture and practices shows a global maturity of **Basic (Level 1)**, based on the lowest maturity score of an organization.



The average score is also calculated and can be used to track progress in future security scans:



CIS Controls are not a standard by which organizations can become "compliant," but rather a series pragmatic controls that can be used to a greater or lesser degree. As the above score is not a measurement of compliance, Members should deep-dive into specific topics or start from the Security Profile and work on that foundation.

Based on our analysis, most NetHope Members are conscious of cyberthreats, but their information security activities are reactive, inconsistent, and ad-hoc in response to attacks. Member organizations recognize the business risks due to vulnerabilities but do not have adequately defined policies or procedures to protect themselves. Most of the implemented controls are reactive and not planned. Most Members are at the starting point of protecting their investment and ensuring continuity. Security awareness programs are being considered, but for key resources only. Some intrusion and detection testing is also being performed. While organizational size, industry, regulatory environment, location, and other risk factors might influence the final recommendations associated with this global rating, NetHope Members' information security positions share the following characteristics:



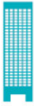
- The risks facing the organizations are generally understood although not managed in a proactive way.
- Organizations are generally aware of the security threats they face with poor threat intelligence integration.
- The governance of information security programs is structured but not fully integrated into other governance and compliance areas.

B. Organizational Recommendations

Based on the findings it is clear that organizations need to be more proactive in avoiding and preparing for information security risks and associated cyberthreats. A proactive approach, as opposed to reactive mitigation, entails proper risk management as a top-level strategic issue. This prioritization is key to identifying, protecting, detecting, and responding to risks and protecting digital environments, because the scale of the risks require senior management to be on board for support and accountability. It is recommended that Member organizations should make formal, conscious top-level decisions to incorporate CIS Controls (or a similar widely recognized and mappable information security control set) into their organization's standard for risk definition, measurement, and defense. For example, it is crucial to embed the definitions and progress towards the CIS Controls into each part of the organization's documented security policies and procedures for digital infrastructure.

III. ASSESSMENT GOALS

NetHope Members and the broader nonprofit sector are encountering a shifting threat landscape as major IT trends are changing, including the rapid adoption of cloud and privacy regulations, the accelerated growth of unstructured data, and the wider use of mobile devices. This assessment report provides a high-level review regarding NetHope Members' security programs based on the CIS Security Controls Implementation Group 1 across the three domains (Basic, Foundational, and Organizational) contained in the Version 7 framework.

	Implementation Group 1 Is the definition of basic cyber hygiene and represents a minimum standard of InfoSec for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.		Implementation Group 2 Assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.		Implementation Group 3 Assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.
---	--	---	--	---	--

The goals of this assessment were to:

- Initiate a baseline for promoting information security practices in a holistic, integrated way.
- Benchmark security “best practices” across a wide range of nonprofit organizations.
- Provide recommendations based on the key findings of the assessment.
- Identify urgent/critical information security issues.
- Develop a prioritized action list which can serve as a roadmap for improving the assessment participants' information security programs.

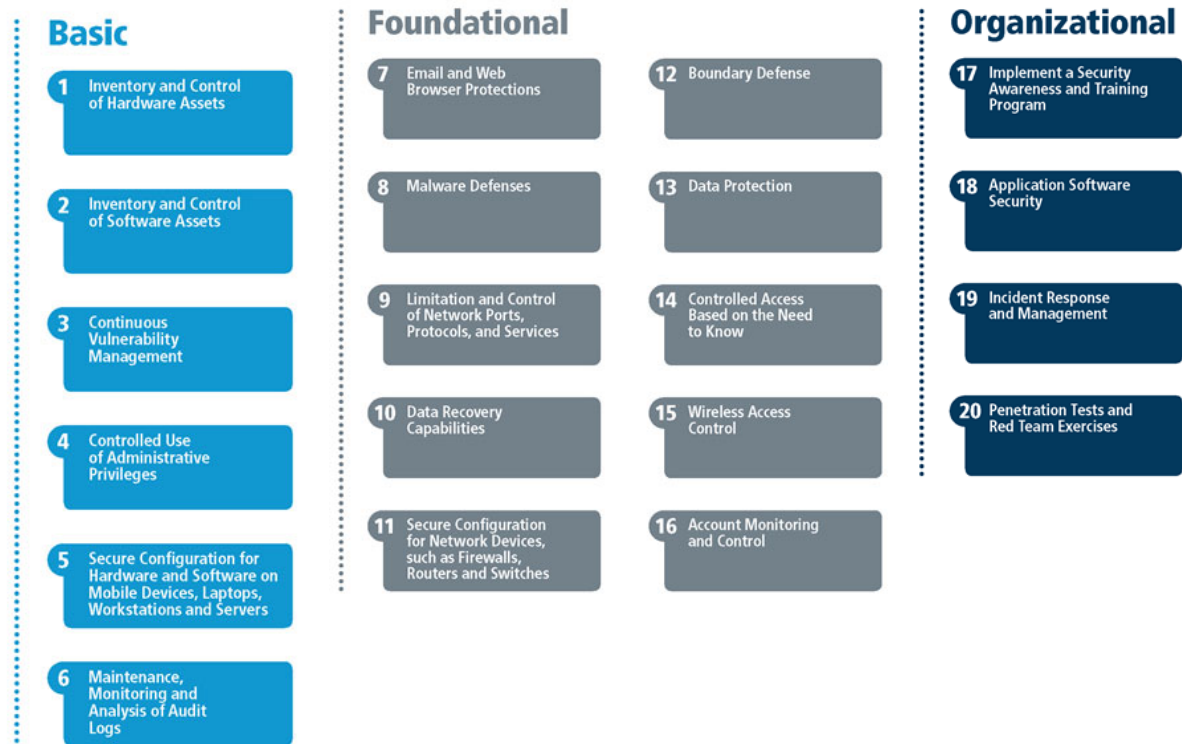
CIS Controls Self-Assessment Tool (CSAT)

The CIS Controls Self-Assessment Tool, also known as CIS CSAT, enables organizations to assess and track their implementation of the CIS Controls. It enables security teams to track and prioritize their implementation of the CIS Controls across their organization. CSAT enables assessors to:

- Collaborate across teams and assign user roles.
- Choose which specific safeguards to include in assessments.
- Upload documentation as supporting evidence.
- Track assessments over time and view graphs of progress.
- Monitor alignment to other security frameworks with CIS Controls mappings to frameworks including NIST CSF and NIST SP 800-53.
- Anonymously compare results to industry averages.

IV. CIS CONTROLS DEFINITION

The CIS Controls (Version 7) are segregated in domains to provide alignment and guidance throughout the implementation and afterwards in operation. These start with the Basic Controls, which define the scope and set a baseline for implementation, and are followed by the Foundational Controls, which cover the essential and important measures to protect IT assets. Finally, the Organizational Controls provide process and procedural guidance with proactive and mitigative controls to help protect the organization from threats.



The controls were derived from the most common cyberattack patterns and vetted across a broad community of governments and industries, with very strong consensus on the resulting set of controls. They serve as a strong basis for high-value actions. The Controls are aligned to several common cybersecurity frameworks to help organizations document their compliance with whichever larger framework they have adopted. Ideally, the CIS Controls provide focus and priority to a smaller number of actionable controls with high leverage and high payoff.

V. MATURITY MODEL DEFINITION

This information security assessment utilizes a Maturity Model to communicate its findings and recommendations. This model is based on a similar model developed by Microsoft (Security Maturity Model). The below reflects the levels:



Level 1 <i>Basic</i>	Level 2 <i>Standardized</i>	Level 3 <i>Rationalized</i>	Level 4 <i>Dynamic</i>
The program is tactical at best and the risks of an information security issue are severe.	The program is proactive, and the risks of an information security issue are significant.	The program is holistic, and fully operational and the risks of an information security issue are moderate.	The program is strategic and optimal, and the risks of an information security issue are minor

VI. SCOPE OF ASSESSMENT & PARTICIPANTS

This assessment was executed in partnership with 27 nonprofit organizations who are Members of the NetHope community. The timeline of the project was as follows:

ACTIVITY	DATE
Kickoff Call	21 April 2021
Complete Interview Series	23 August 2021
Data Analysis/Review	16 August 2021
Executive Report	01 October 2021

Interviews were conducted with key Members' stakeholders to gather information in addition to employing the automated CIS CSAT self-assessment tool. Below are the 27 Members:



VII. KEY FINDINGS

Specific ratings associated with each CIS control are more illuminating about the state of specific activities towards information security by the Member organizations, than the overall/all organization rating. These ratings can be used as a current state benchmark, as well as a way to drive realistic targets for the teams that seek to improve these practices and thereby reduce risks (both at the organization level, as well as the harm that may befall the people and communities they work with).

The individual scoring of some Members was close to “1” with a very Basic Information Security posture and reactive in most controls’ implementation. Other Members, with ratings above “3”, have a strategic program that is fully operational which proactively identifies cyberthreats and optimizes cyber defense. Below is a comparison of the average of participant member organizations (in blue) with an example of one organization’s scores (in orange).



Dashboard for Policy, Reporting, Implementation and Automation of Controls Maturity

In the illustration above, presenting CIS controls (1-20) rating for an example organization compared to the average benchmark for 4 different maturities: Policy approved, Control Implementation, Control Automation and the Reporting Maturity. The Policy Approved Maturity determines whether or not the organization has a policy defined that indicates that they should be implementing the defined sub control. The Control Implementation Maturity determines whether or not the organization currently has implemented this sub control and to what degree the control has been implemented. The Automation Maturity determines whether or not the organization currently has automated the implementation of this

sub control and to what degree the control has been automated. The Reporting Maturity determines whether the organization is reporting this sub control to business representatives and to what degree the control has been reported.

The above maturity ratings are the result of the average calculation of the control scores related to each organization. It's worth to mention that all names were anonymized protecting the identity of the Members and the results of their information security postures.

A. CIS Basic Controls – Definition

The CIS Basic Controls are related to inventory, scoping and control of the IT environment to its full extent. The six CIS Basic Controls and their objectives are:

CONTROL	OBJECTIVE
1. Inventory and Control of Hardware Assets	Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from access.
2. Inventory and Control of Software Assets	Actively manage (inventory, track, and correct) all software in the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from the installation or execution.
3. Continuous Vulnerability Management	Continuously acquire, assess, and act on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.
4. Controlled Use of Administrative Privileges	The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
5. Secure Configuration for HW/SW on Mobile Devices, Laptops, Workstations, and Servers	Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, and workstations using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.
6. Maintenance, Monitoring and Analysis of Audit Logs	Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

B. CIS Basic Controls – Average Member Rating

As per the above objectives, the average organizations current rating on each CIS Basic Control as follows:

	1	2	3	4
1. Inventory and Control of Hardware Assets	Lowest 0.8 ↓	Average 2.0 ↓	Highest 3.4 ↓	
2. Inventory and Control of Software Assets	Lowest 0.8 ↓	Average 2.0 ↓	Highest 3.4 ↓	
3. Continuous Vulnerability Management	Lowest 1.2 ↓	Average 2.5 ↓		Highest 4.0 ↓
4. Controlled Use of Administrative Privileges	Lowest 0.8 ↓	Average 2.4 ↓	Highest 3.6 ↓	
5. Secure Configuration for Hardware/Software on Mobile Devices, Laptops, Workstations, and Servers	Lowest 1.0 ↓	Average 2.3 ↓		Highest 3.8 ↓
6. Maintenance, Monitoring and Analysis of Audit Logs	Lowest 1.0 ↓	Average 2.3 ↓		Highest 3.8 ↓

The common shortcomings in most organizations that affects these ratings include the failure to patch known vulnerabilities, poor configuration management, and poor management of administrative privileges. This doesn't mean "Poor Hygiene." The low scores in this area are likely due to the under-resourced information security functions in most nonprofits that in turn amplifies the effects of the complex environments that many global humanitarian and conservation nonprofits work in. Examples include:

- 1) Many NetHope Members cite the porous organizational boundaries that are associated with consortia and the highly collaborative working environments that span complex locations, multiple agencies, implementers, funders, as well as users who are an ever-changing mix of staff, clients/beneficiaries, and volunteers, for their struggle to manage inventory and assets.
- 2) Many NetHope Members report that the problem is not that they don't know what is occurring or what needs to be addressed. But rather they point out that they do not have the resources to triage the items raised by the audit logs in the audit platforms, let alone action the fixes necessary for the issues raised by those audit logs.

C. CIS Basic Controls – Findings & Recommendations

Below are organizational recommendations for the detailed findings of the six CIS Basic Controls:

URGENT			
CONTROL	QUESTION	RATING	SUGGESTION
2. Inventory and Control of Software Assets	Are discovery tools implemented to identify all software applications throughout the organization's infrastructure?	Basic (1) Not Implemented	Embed a discovery tool for software asset management.
3. Continuous Vulnerability Management	Are discovery tools implemented to identify software vulnerabilities on systems within the organization's infrastructure?	Basic (1) Not Implemented	Implement vulnerability scan software. Scan for vulnerabilities regularly, especially on systems contain sensitive information.
	Has an automated patch management solution been implemented to continuously update all of the organization's systems?	Basic (1) Not Implemented	Implement a patch management process and solution. Gain insights on the patch status of all systems.
4. Controlled Use of Administrative Privileges	Does every administrator have a dedicated personal admin account, separated from their normal user account? Has the organization implemented MFA for all administrative access?	Basic (1) Not Implemented	Setup personal admin accounts and enable MFA for all external admin access.
	Does the organization have an entitlement review process to validate that each person with admin privileges on servers, desktops and laptops is authorized by a senior executive on a repeating schedule?	Basic (1) Not Implemented	Implement an entitlement and approval review process for all accounts with admin privileges for regular check. Clean up old unused accounts.
5. Secure Configuration for HW/SW on Mobiles, devices, Laptops, Workstations, and Servers	Are discovery tools implemented to identify any misconfigured security settings on the of the organization's systems within the infrastructure?	Basic (1) Not Implemented	Implement a configuration management tool to check all systems for a minimal set of security settings.

HIGH PRIORITY			
CONTROL	QUESTION	RATING	SUGGESTION
1. Inventory and Control of Hardware Assets	Are discovery tools (active and passive) implemented to identify all devices attached to the organization's infrastructure?	Standardized (2) Implemented with limited scope	Extend the scope of the discovery solution(s) to the entire infrastructure.
2. Inventory and Control of Software Assets	Are software whitelisting solutions implemented that only authorized software programs to be executed on all the organization's systems?	Basic (1) Not Implemented	Configure whitelisting to restrict the usage of unwanted and malicious software.
5. Secure Configuration for HW/SW on mobiles, devices laptops, workstations, and servers	Does the organization have an implemented secure hardening baseline for all new systems, disabling old NTLM and SMB and more security registry keys?	Basic (1) Not Implemented	Define a secure hardening baseline for all systems, to lock down all systems by default.
6. Maintenance, Monitoring and Analysis of Audit Logs	Have all devices and servers, including Domain Controllers, Firewalls, Networks-based Intrusion Prevention Systems, and inbound and outbound proxies, been implemented and configured to verbosely log all traffic and failed login attempts?	Standardized (2) Implemented with limited scope	Point the logging configuration of all devices to the central logging platform.

D. CIS Foundational Controls – Definition

The CIS Foundational Controls are mostly focused on technically securing IT assets to the full extent of the environment and the detection of threats. The ten CIS Foundational Controls and their objectives are:

CONTROL	OBJECTIVE
7. Email and Web Browser Protections	Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.
8. Malware Defenses	Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action.

9. Limitation and Control of Network Ports, Protocols, and Services	Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices to minimize windows of vulnerability available to attackers.
10. Data Recovery Capabilities	The processes and tools used to properly backup critical information with a proven methodology for timely recovery of it.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process to prevent attackers of exploiting vulnerable services and settings.
12. Boundary Defense	Detect/prevent/correct the information transferring networks of different trust levels with a focus on security-damaging data.
13. Data Protection	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.
14. Controlled Access Based on the Need to Know	The processed and tools used to track/control/prevent/correct secure access to critical assets according to formal determination of which persons, computers and applications have a need and right to access the critical assets based on an approved classification.
15. Wireless Access Control	The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANS), access points and wireless client systems.
16. Account Monitoring and Control	Actively manage the life cycle of system and application accounts – their creation, use, dormancy, deletion – to minimize opportunities for attackers to leverage them.

E. CIS Foundational Controls – Average Member Rating

The assessment has taken a measurement based on the above objectives of the CIS Foundational Controls and projected these to all organizations' current position and resulting in a rating of:

	1	2	3	4
7. Email and Web Browser Protections	Lowest 0.0	Average 2.0		Highest 3.6
8. Malware Defenses	Lowest 1.0	Average 2.5		Highest 3.4
9. Limitation and Control of Network Ports, Protocols and Services	Lowest 0.8	Average 2.5		Highest 3.4

	1	2	3	4
10. Data Recovery Capabilities	Lowest 0.0	Average 2.5		Highest 3.8
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Lowest 0.8	Average 2.3	Highest 3.4	
12. Boundary Defense	Lowest 0.4	Average 2.3		Highest 3.8
13. Data Protection	Lowest 0.0	Average 1.6	Highest 2.8	
14. Controlled Access Based on the Need to Know	Lowest 0.4	Average 2.5		Highest 3.8
15. Wireless Access Control	Lowest 0.8	Average 2.5		Highest 4.0
16. Account Monitoring and Control	Lowest 0.0	Average 2.2		Highest 3.8

F. CIS Foundational Controls – Findings & Recommendations

Malicious software is a common component of cyberattacks and a huge threat. Organizations should use a combination of barrier and detection technologies to identify and block malware as it attempts to enter the network. In addition, they should use automated scanning solutions to keep track of active ports, services, and protocols to ensure that only those with legitimate business need are enabled.

Successful attacks against digital assets often result in substantial changes to the availability of systems and the confidentiality and integrity of data. This can be obvious, as in the case of ransomware, or it can be more subtle, with attacks quietly advancing over time. While most Members have created and stored data backups, many don't have strong processes to test and recover from an attack. The CIS Foundational Controls implementation outlines an iron-clad process for creating, maintaining, protecting, testing, and restoring from data backups.

Most Members have data stored in several locations, so the first step in protecting data is to maintain an up-to-date inventory of all sensitive information that is stored, processed, or transmitted. Beyond this, strict policies must be in place to control the movement of data via mobile devices, laptops, USB drives, and other transportable data storage devices. Encryption is critical to keep data secure in transit. Moreover, network segmentation and disabling workstation-to-workstation communication help minimize the risk of data being transmitted between user accounts of different access levels. In

addition, Members must have control over the full life cycle of user accounts. There must be a process in place to immediately disable/terminate accounts that are no longer required (for example, when a user leaves the organization), and all accounts should have an expiration date that is closely monitored and enforced.

Below are recommendations per the detailed findings of the ten CIS Foundational Controls:

URGENT			
CONTROL	QUESTION	RATING	SUGGESTION
8. Malware Defenses	Are there centrally managed tools implemented to continuously scan for anti-malware and to remove malware and keep ant-malware and signature files on workstations, servers, and mobile devices up to date and properly configured?	Basic (1) Not Implemented	Enable the default tools for antivirus, anti-malware and Data Execution Prevention on the organization's systems.
	Are logs of antivirus events stored centrally with alerting activated so that IT departments can take actions?	Basic (1) Not Implemented	Store antivirus logs centrally and apply alerting for additional insights.
12. Boundary Defense	Do all remote login access require encryption of data in transit and multi-factor authentication?	Basic (1) Not Implemented	Identify sensitive information on the organization's main data sources. Apply labeling and data classification.
13. Data Protection	Has device and disk encryption software been applied to mobile devices and all systems that hold sensitive data?	Basic (1) Not Implemented	Enable encryption on the organizations' main data source.
17. Account Monitoring and Control	Are account and password policies enforced with MFA for all users on all systems?	Basic (1) Not Implemented	Define a standard password policy definition for all applications and infrastructure services. Increase password length.

HIGH PRIORITY			
CONTROL	QUESTION	RATING	SUGGESTION
7. Email and Web Browser Protection	Are network-based URL filters implemented that limit a system's ability to connect to websites not approved by the organization?	Standardized (2) Implemented for some systems	Ensure the use of proxy server/IPS solution by all systems.

	Is email protected with SPF, DKIM and DMARK?	Standardized (2) on some domains	Create the appropriate SPF and DKIM record for all email domains. Setup and enable DMARK for your domains.
	Are email attachments scanned and blocked in a sandbox solution?	Basic (1) Not Implemented	Implement an email antivirus, antimalware solution that proactively scans attachments.
9. Limitation and Control of Network Ports, Protocols, and Services	Are web application firewalls implemented in front of critical servers to verify and validate the traffic going to the server?	Standardized (2) implemented on some systems	Setup Web Application Firewalls (WAF) in front of any critical server.
10. Data Recover Capabilities	Does organizations have a backup process in place where each system is automatically backed up? Is a restore tested and verified at least once every three months?	Standardized (2) Backup implemented for main systems, restore incidentally tested	Extend the backup process to include all systems.
11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches	Are automated tools implemented to verify approved organizational standards for network device configurations and detect bias?	Standardized (2) Implemented for some network devices	Extend the network device management solution to include all the organizations' network devices.
	Is a process implemented to install the latest version of any security related updates on all network devices?	Standardized (2) A process is in place but is not scheduled or based on risks	Schedule the execution of the update process for network devices.
12. Boundary Defense	Is network segmentation applied to separate systems with different roles?	Standardized (2) Only servers and endpoints	Separate systems based on roles and restriction levels.
	Are firewalls and network-based IDS/IPSs implemented to detect and block attacks and malicious traffic at each of the organization's boundaries?	Standardized (2) Basic Firewalls are implemented	Enable the deep packet inspection (DPI) and IDS/IPS functionality of the firewall, if possible.
14. Controlled Access Based on the Need to Know	Is encryption in transit (SSL/TLS) implemented for all communication of sensitive information over less-trusted networks?	Standardized (2) Implemented on for some communication	Enable encryption for all external/public network communication and internal network communication related to sensitive data.

	Is network segmentation applied based on the label or classification level of the information stored?	Standardized (2) Implemented for some systems	Apply network segmentation for all the organization's data sources.
	Are Access Control Lists implemented to limit the access of individuals to sensitive information based on need?	Standardized (2) Basic security Groups have been implemented	Create security groups based on the business role matrix.
15. Wireless Access Control	Have wireless networks been implemented with Advanced Encryption Standard (AES) encryption for data in transit?	Standardized (2) Wireless networks have been implemented with WPA2 (TKIP)	Switch from WPA2-TKIP to WPA2-AES authentication /encryption.
	Are Wi-Fi guest networks separated from the corporate network?	Standardized (2) Implemented but not separated from the organization network boundary	Assign a separate VLAN to guest networks.
16. Account Monitoring and Control	Is a centralized authentication platform available and used for every application, device, and cloud storage platform?	Standardized (2) Implemented for the core applications and infrastructure services	Configure a single authentication source directory for all applications and systems.
	Is account management performed by the business unit with ownership of each account? Are dormant accounts automatically deactivated after a set period?	Standardized (2) Some accounts are checked, by business owner, but old accounts are still lingering around	Implement business ownership of all accounts, including checks by the business/ functional owner of each account, and establish a process to cleanup old accounts.

G. CIS Organizational Controls – Definition

The CIS Organizational Controls are related to processes and procedures of the organization. Mainly, related to Awareness and Training, Incident Response and Red Team Exercises. The two Implementation Group 1 CIS Organizational Controls and their objectives are:

CONTROL	OBJECTIVE
18. Implement a Security Awareness and Training Program	Develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness program.
19. Incident Response and Management	Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure for quickly discovering an attack and effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

H. CIS Organization Controls – Average Member Rating

The assessment has taken a measurement based on the above objectives of the CIS Organizational Controls and projected these to all organizations' current position and resulting in a rating of:

	1	2	3	4
17. Implement a Security Awareness and Training Program	Lowest 0.4	Average 2.4		Highest 4.0
19. Incident Response and Management		Lowest 0.8	Average 2.2	Highest 3.0

I. CIS Organizational Controls – Findings & Recommendations

Nonprofit organizations have a **phish-prone percentage** (number of employees who clicked a simulated phishing email link or opened an infected attachment during a testing campaign) of **31.2%**.² Without the commitment of senior management to support cybersecurity goals, most Members will not be able to implement adequate information security tools and solutions. Members should identify all functional roles within their organizations with a focus on those who are most central to the organization's success. Competent team members with the specific technical Information Security knowledge and expertise are required to build a robust cyber defense. Develop a plan which identifies skill and knowledge gaps and how training and security awareness will be managed. It is critical for Members to have established processes in place to respond quickly and

² <https://info.knowbe4.com/phishing-by-industry-benchmarking-report>

effectively to any cyberthreat. Organizations should have an incident response infrastructure in place with written plans defining the roles of each employee and the different steps necessary to address incidents.

Below are organizational recommendations for the detailed findings of the ten CIS Foundational Controls:

URGENT			
CONTROL	QUESTION	RATING	SUGGESTION
17. Implement a Security Awareness and Training Program	Is a security & privacy program established?	Basic (1) No security and privacy awareness program available	Establish a security and privacy awareness program.
	Is there a security awareness training program in place addressing secure logins, social engineering, sensitive data handling, unintentional data exposure, and identifying and reporting incidents?	Basic (1) No Training program available	Setup a basic training program for the core roles within the organization.

HIGH PRIORITY			
CONTROL	QUESTION	RATING	SUGGESTION
19. Incident Response and Management	Is an incident response procedure in place with the right reporting techniques and escalation processes, data collection, management responsibilities, legal protocols, and communication strategy?	Standardized (2) A basic incident repines procedure is in place	Provide more details to the procedure and include staff roles and management responsibilities. Regularly test this.

VIII. RECOMMENDED ACTIONS

A. Urgent Priority Actions

These are the urgent and pressing priority actions that surfaced from the collective assessment, and they are further detailed below in this report. We recommend that the items below are urgently assessed and acted upon as a matter of urgency by each individual organization.

PRIORITY	ACTION
1. Inventory and Control of Hardware Assets	Embed a discovery tool for hardware asset management including personal computers, servers, storage spaces, multi-channeled networks, etc. Asset discovery involves keeping a check on the active and inactive assets present in your network.
2. Inventory and Control of Software Assets	Embed a discovery tool for software asset management. Asset discovery not only maximizes the value of existing assets, but also optimizes the network especially in enhancing the level of security.
3. Continuous Vulnerability Management	Implement vulnerability scan tool. Scan for vulnerabilities periodically, especially on systems contain sensitive information.
	A patch management process and tooling used to ensure that the components of an organization's software stack and IT infrastructure are up to date. Gaining insights on the patch status of all systems.
4. Administrative Privileges	Setup admin accounts and MFA (multi factor authentication) enabled for all external admin access.
7. Email and Web Browser Protections	Ensure fully supported web browsers and email clients can execute. Use Domain Name System (DNS) filtering services to help block access to known malicious domains.
8. Malware Defenses	Enable the default tools for Antivirus, anti-malware on the organization's systems.
13. Data Protection	Add an extra security layer to data by enabling encryption on the main data sources including data at rest and in transit.
16. Account Monitoring and Control	Define standard password policy definition for the systems in addition to enabling MFA on all systems, increase password length if MFA is not yet available.

B. Quick Wins

With the actions below, security enhancements are evident and can quickly be deployed in organizations.

PRIORITY	CONTROL	ACTION
Operating Systems	2. Inventory and Control of Software Assets	Replace and migrate all end-of-life Operating Systems as it will no longer have technical support, and more importantly, will no longer have updates to it.

Patching	3. Continuous Vulnerability Management	Expedite available security updates on all endpoints especially the critical updates.
Admin Access	4. Controlled use of Administrative Privileges	Review Administrator accounts and disable/remove old/unused users.
Data Encryption	13. Data Protection	To effectively secure digital data, it should be encrypted so that it is accessible only for authorized users. Enable BitLocker on all endpoints including mobile devices.
AD Accounts	16. Account Monitoring and Control	Add a security layer to the account level by implementing MFA – Multi Factor Authentication. Also, by disabling old/unused accounts Review external accounts.

NETHOPE MEMBERS



NETHOPE PARTNERS

