LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HEALTH SECTOR CYBERSECURITY COORDINATION CENTER
HC3

CIS Controls and the HPH

09/03/2020

Report #: 202009031030

Agenda

- Introduction
- Center for Internet Security (CIS)
- CIS Communities
- CIS Controls
- Conclusion
- Reference Materials
- Questions

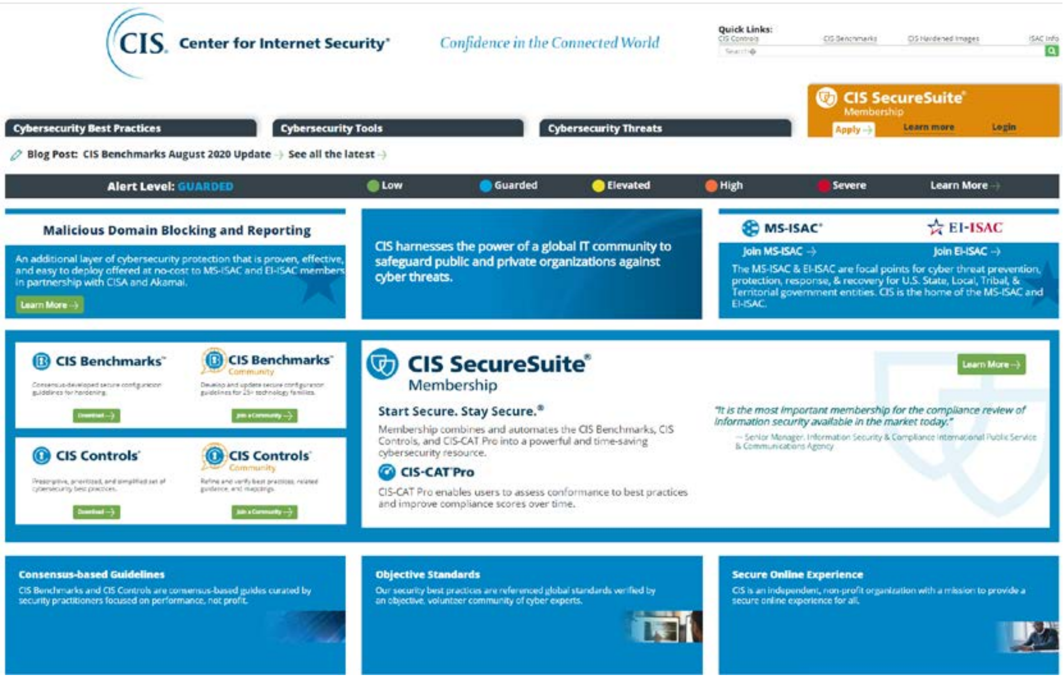
Slides Key:

👤	Non-Technical: managerial, strategic and high-level (general audience)
⚙	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Introduction

CIS Controls:

- Provide a quick security win for the Healthcare and Public Health (HPH) Sector
- They offer an initial starting point for execution of a cyber security strategy
- They are scalable to meet the needs of the smallest to largest organizations
- Execution of the initial 43 sub-controls can defend against the five major cyber attacks and mitigates 62% of Mitre ATT&CK Techniques



Blog Post: CIS Benchmarks August 2020 Update → See all the latest →

Malicious Domain Blocking and Reporting

An additional layer of cybersecurity protection that is proven, effective, and easy to deploy offered at no-cost to MS-ISAC and EI-ISAC members in partnership with CISA and Akamai.

CIS harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.

The MS-ISAC & EI-ISAC are focal points for cyber threat prevention, protection, response, & recovery for U.S. State, Local, Tribal, & Territorial government entities. CIS is the home of the MS-ISAC and EI-ISAC.

CIS Benchmarks™: Consensus-developed secure configuration guidelines for hardening.

CIS Benchmarks™ Community: Develop and update secure configuration guidelines for 25+ technology families.

CIS Controls®: Prescriptive, prioritized, and simplified set of cybersecurity best practices.

CIS Controls® Community: Refine and verify best practices, related guidance, and mappings.

CIS SecureSuite® Membership

Start Secure. Stay Secure.®

Membership combines and automates the CIS Benchmarks, CIS Controls, and CIS-CAT Pro into a powerful and time-saving cybersecurity resource.

CIS-CAT® Pro

CIS-CAT Pro enables users to assess conformance to best practices and improve compliance scores over time.

"It is the most important membership for the compliance review of information security available in the market today."

— Senior Manager, Information Security & Compliance International Public Service & Communications Agency

Consensus-based Guidelines

CIS Benchmarks and CIS Controls are consensus-based guides curated by security practitioners focused on performance, not profit.

Objective Standards

Our security best practices are referenced global standards verified by an objective, volunteer community of cyber experts.

Secure Online Experience

CIS is an independent, non-profit organization with a mission to provide a secure online experience for all.

Figure source: Center for Internet Security

Center for Internet Security

Center for Internet Security (CIS)

- Community-driven nonprofit
- Maintains the CIS Controls and CIS Benchmarks
- Provides cloud-based CIS Hardened Images
- Home to MS-ISAC and EI-ISAC

The CIS Vision:

- “Leading the global community to secure our ever-changing connected world.”

The CIS Mission:

- “Our mission is to make the connected world a safer place by developing, validating, and promoting timely best practice solutions that help people, businesses, and governments protect themselves against pervasive cyber threats.”

Figure source: Center for Internet Security

CIS Communities

CIS Benchmarks™ Community

- Over 100 configuration guidelines
  - Operating Systems
  - Server Software
  - Cloud Providers
  - Mobile Devices
  - Network Devices
  - Desktop Software
  - Multi-function Print Devices
- Across 25+ vendor product families
- Maintained by community volunteers

CIS Controls® Community

- 20 Security Controls
  - Six Basic Controls
  - Ten Foundational Controls
  - Four Organizational Controls
  - 171 sub-controls
- Initial application recommended according to organization's Implementation Group (IG)
  - IG1, IG2, and IG3
- Maintained by community volunteers

Figure source: Center for Internet Security

CIS Communities

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Elections
Infrastructure
ISAC™

Mission:

- “The mission of the MS-ISAC is to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.”

Mission:

- “The mission of the EI-ISAC is to improve the overall cybersecurity posture of state, local, territorial, and tribal election offices, through collaboration and information sharing among members, the U.S. Department of Homeland Security and other federal partners, and private sector partners are the keys to success.”

Figure source: Center for Internet Security

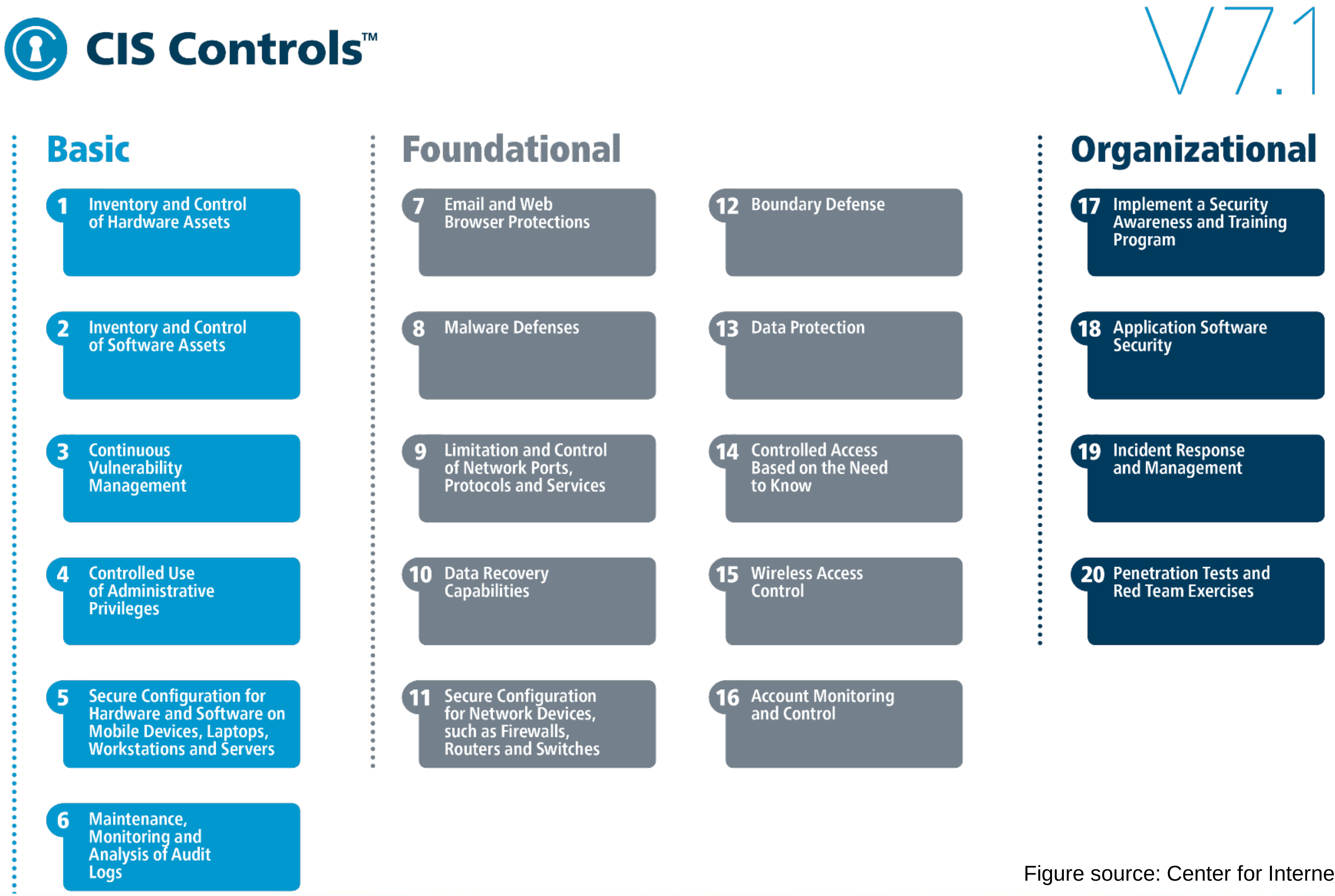
CIS Controls

Figure source: Center for Internet Security

CIS Controls (cont.)

2001	• Tony Sager led release of NSA security guidance to public
2008	• Sager led small group at NSA to determine where to get started with security
2009	• Picked up the Center for Strategic and International Studies and SANS Institute • Originally “The Consensus Audit Guidelines” => “SANS Top 20”
2012	• Sager retires from NSA – Takes over SANS Top 20 at SANS
2013	• Maintenance of Controls transferred to the Council on Cyber Security
2015	• Maintenance of Controls transferred to the Center for Internet Security
2019	• Current version 7.1 of Controls released in April 2019

CIS Controls (cont.)



CIS Controls™ V7.1

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

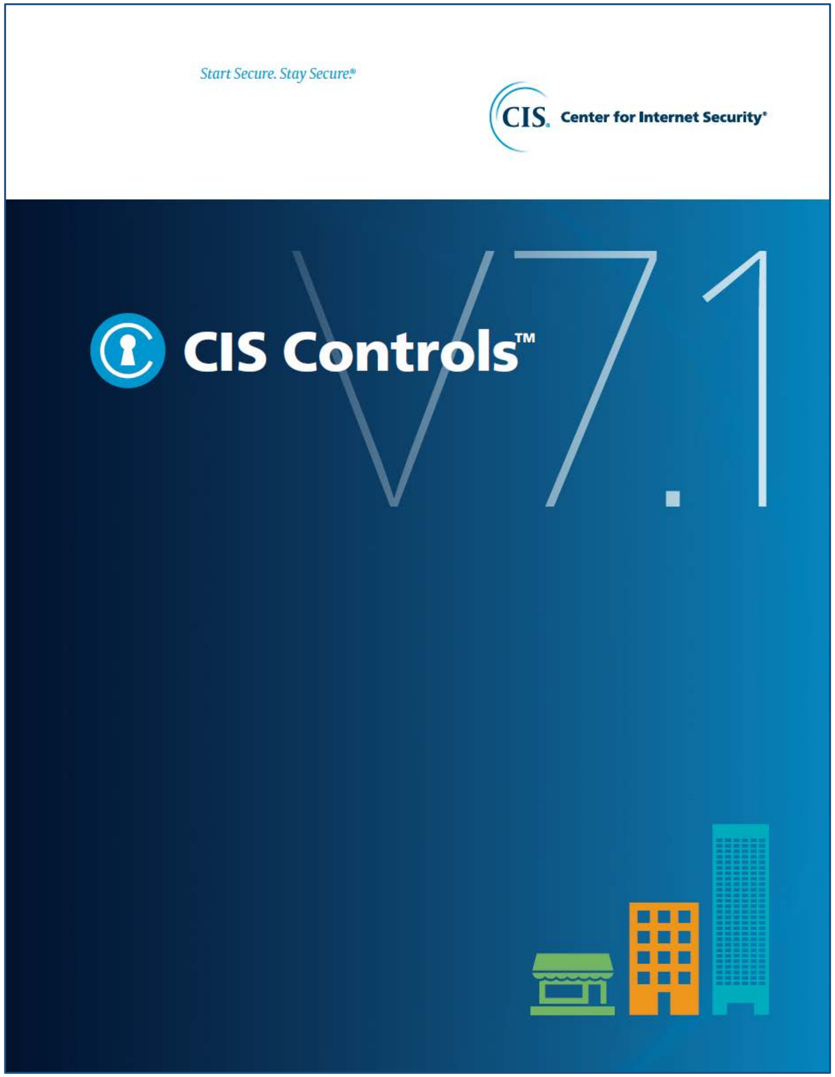
18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Figure source: Center for Internet Security

CIS Controls (cont.)



Start Secure. Stay Secure.®

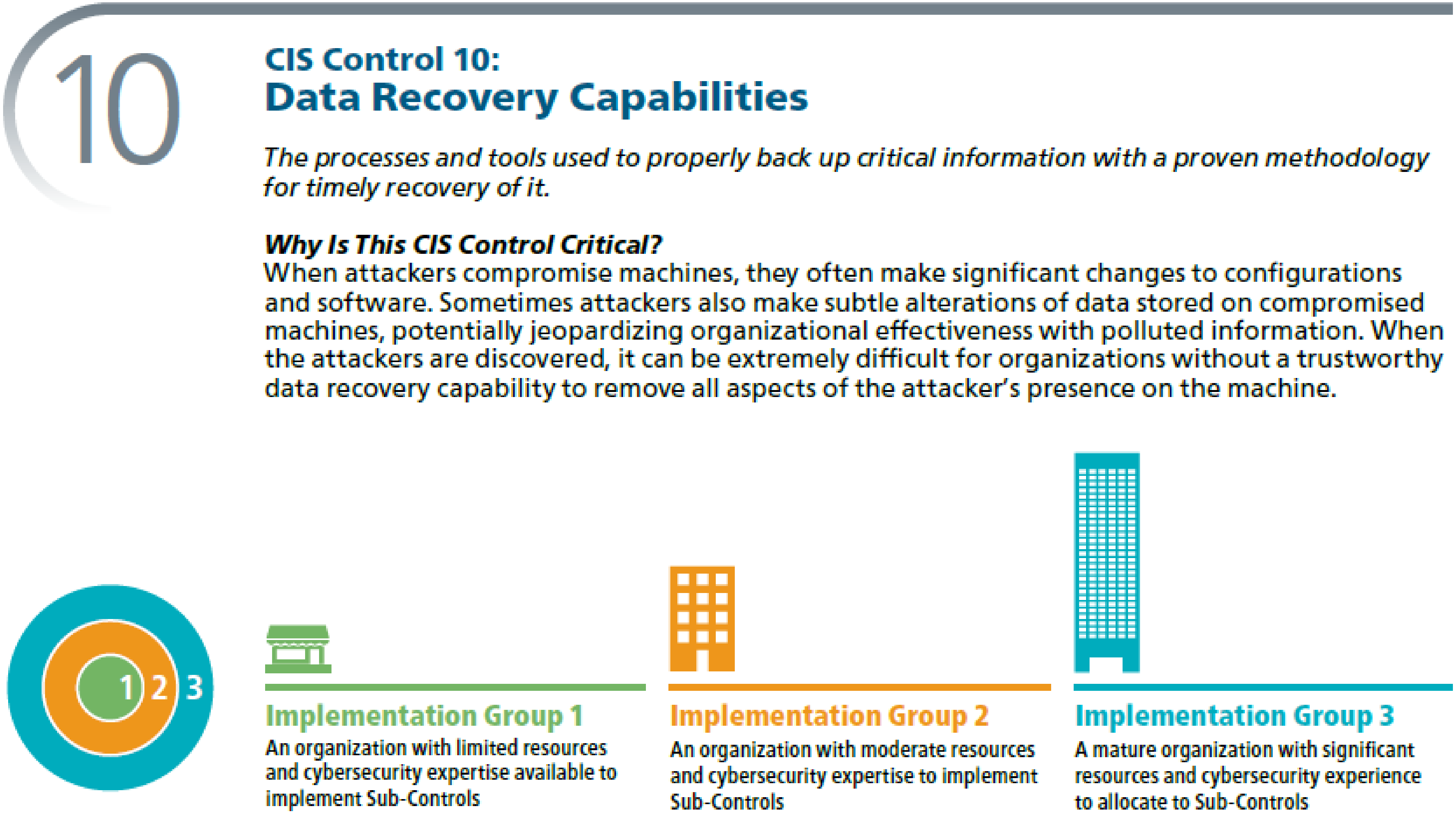
CIS. Center for Internet Security®

CIS Controls™

V7.1

Figure source: Center for Internet Security

CIS Controls (cont.)



CIS Control 10:
Data Recovery Capabilities

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

Why Is This CIS Control Critical?
When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

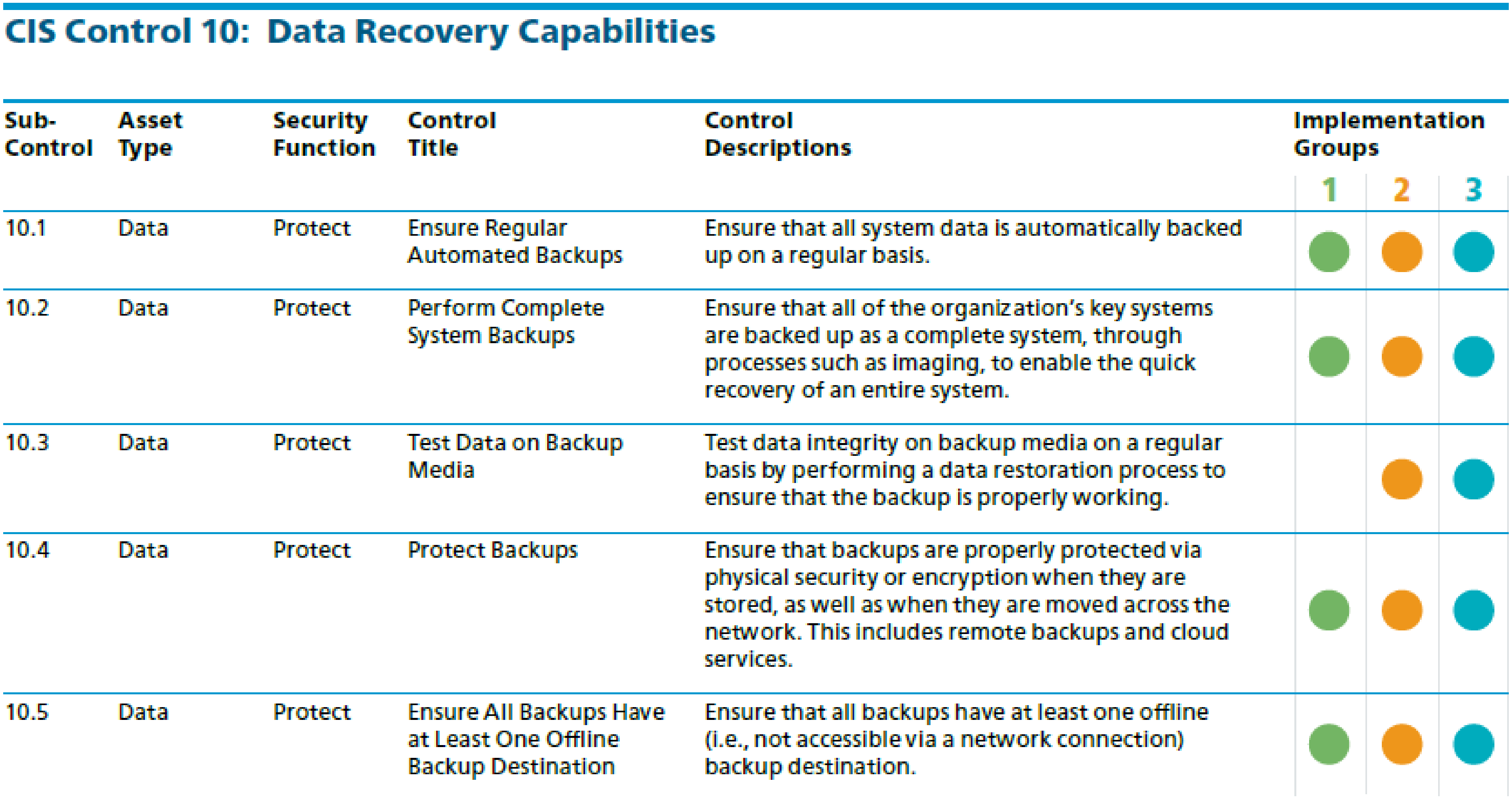
Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Figure source: Center for Internet Security

CIS Controls (cont.)

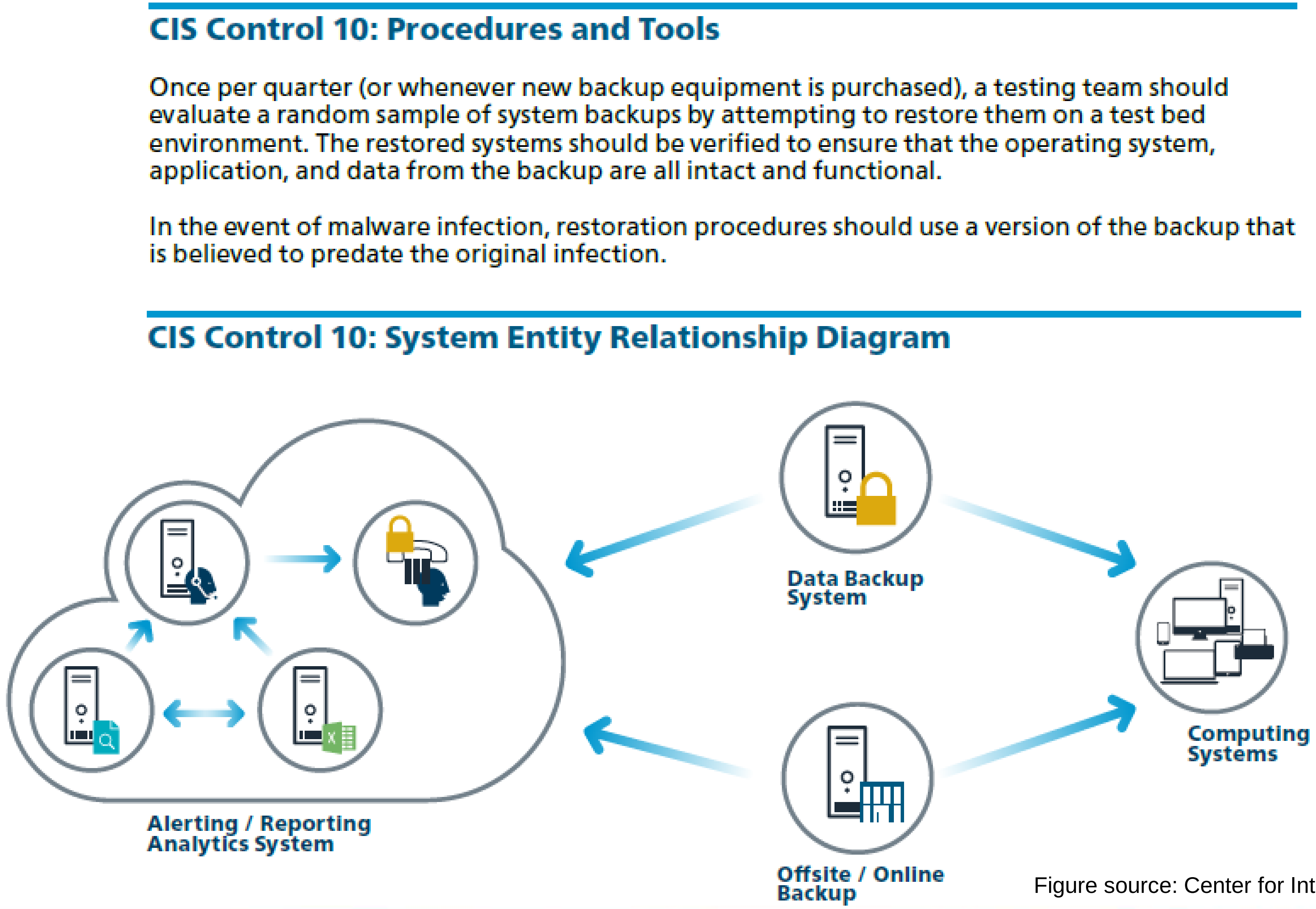


CIS Control 10: Data Recovery Capabilities

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
10.1	Data	Protect	Ensure Regular Automated Backups	Ensure that all system data is automatically backed up on a regular basis.	●	●	●
10.2	Data	Protect	Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	●	●	●
10.3	Data	Protect	Test Data on Backup Media	Test data integrity on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.		●	●
10.4	Data	Protect	Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	●	●	●
10.5	Data	Protect	Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.	●	●	●

Figure source: Center for Internet Security

CIS Controls (cont.)



CIS Control 10: Procedures and Tools

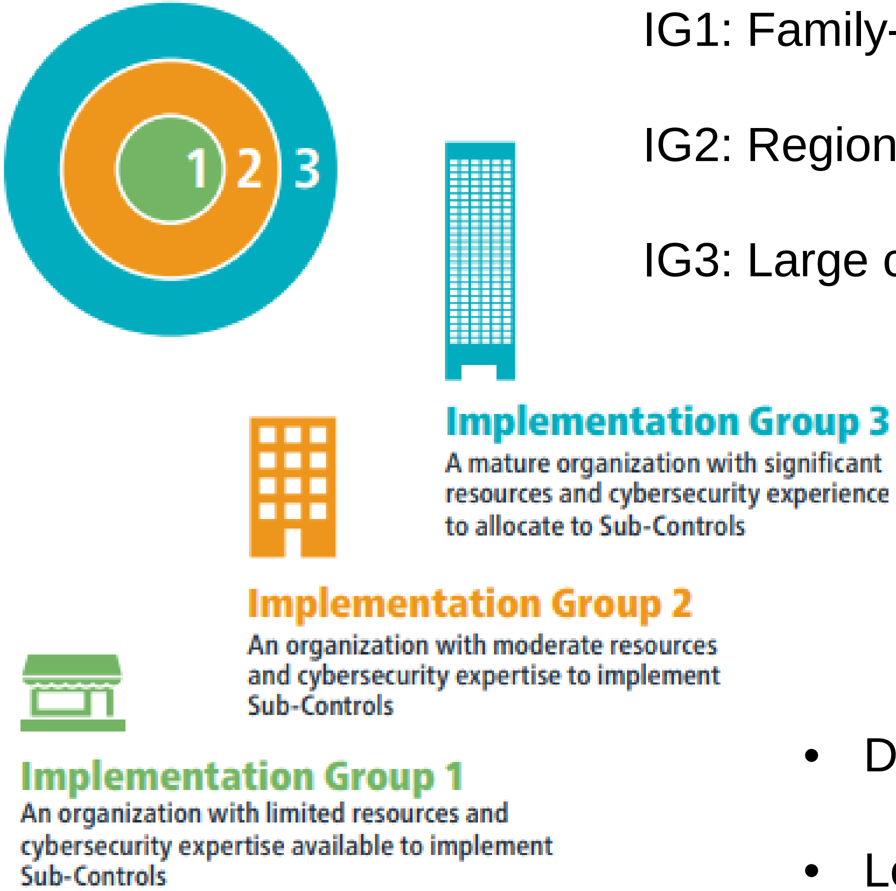
Once per quarter (or whenever new backup equipment is purchased), a testing team should evaluate a random sample of system backups by attempting to restore them on a test bed environment. The restored systems should be verified to ensure that the operating system, application, and data from the backup are all intact and functional.

In the event of malware infection, restoration procedures should use a version of the backup that is believed to predate the original infection.

CIS Control 10: System Entity Relationship Diagram

Figure source: Center for Internet Security

CIS Controls (cont.)



Implementation Group 3
A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls

Implementation Group 2
An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

Implementation Group 1
An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

IG1: Family-owned business with ten employees

IG2: Regional organization with hundreds of employees

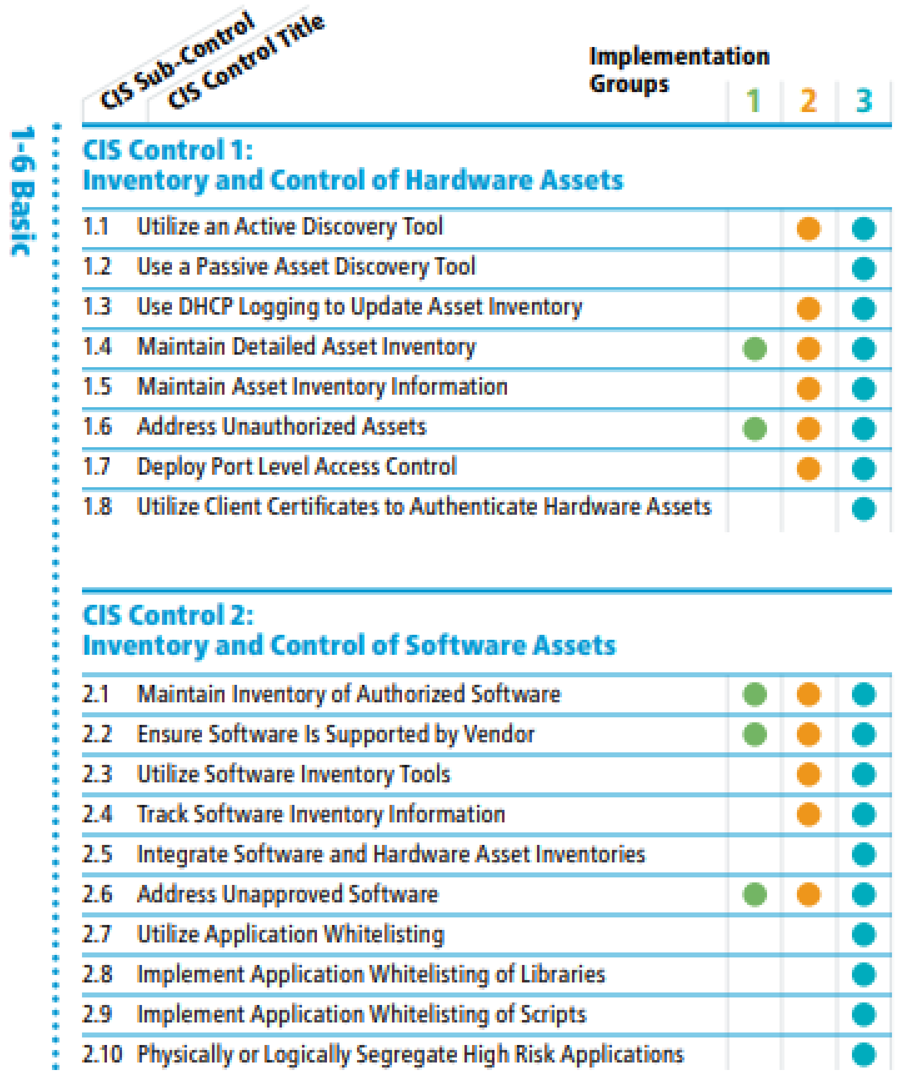
IG3: Large corporation with thousands of employees

IG1 = 43 sub-controls
IG2 = 128 sub-controls
IG3 = 171 sub-controls

- Data Sensitivity / Criticality of Services
- Level of staff technical expertise
- Available resources

Figure source: Center for Internet Security

CIS Controls (cont.)



1-6 Basic

CIS Sub-Control	CIS Control Title	Implementation Groups 1	2	3
CIS Control 1:	**Inventory and Control of Hardware Assets**			
1.1	Utilize an Active Discovery Tool		●	●
1.2	Use a Passive Asset Discovery Tool			●
1.3	Use DHCP Logging to Update Asset Inventory		●	●
1.4	Maintain Detailed Asset Inventory	●	●	●
1.5	Maintain Asset Inventory Information		●	●
1.6	Address Unauthorized Assets	●	●	●
1.7	Deploy Port Level Access Control		●	●
1.8	Utilize Client Certificates to Authenticate Hardware Assets			●
CIS Control 2:	**Inventory and Control of Software Assets**			
2.1	Maintain Inventory of Authorized Software	●	●	●
2.2	Ensure Software Is Supported by Vendor	●	●	●
2.3	Utilize Software Inventory Tools		●	●
2.4	Track Software Inventory Information		●	●
2.5	Integrate Software and Hardware Asset Inventories			●
2.6	Address Unapproved Software	●	●	●
2.7	Utilize Application Whitelisting			●
2.8	Implement Application Whitelisting of Libraries			●
2.9	Implement Application Whitelisting of Scripts			●
2.10	Physically or Logically Segregate High Risk Applications			●

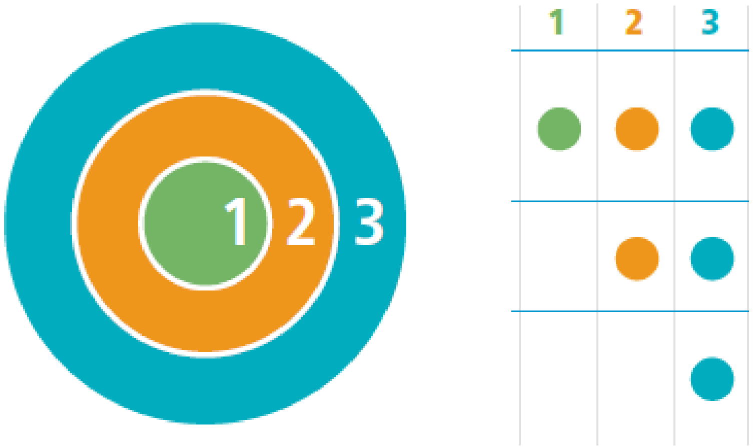
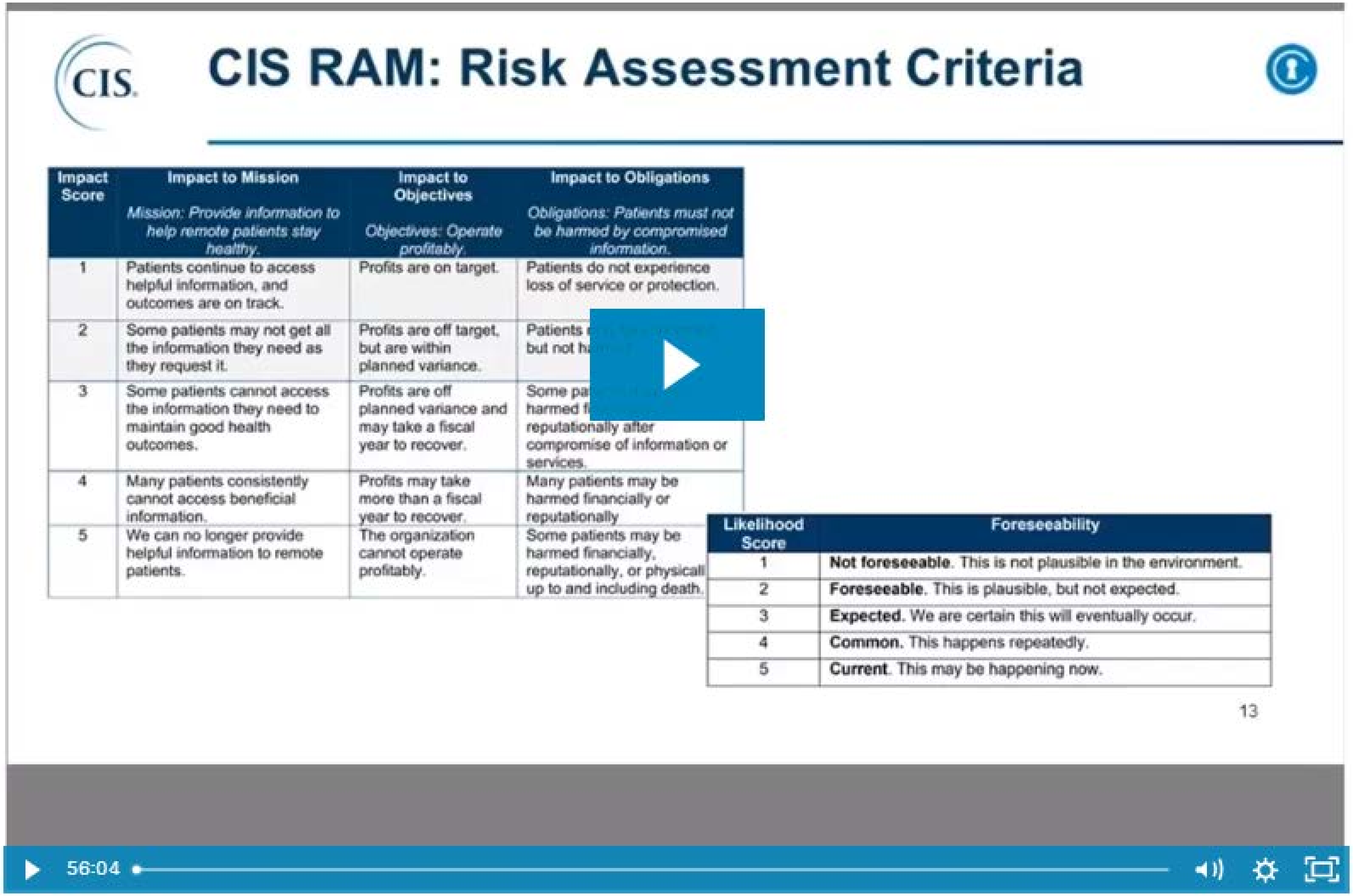


Figure source: Center for Internet Security

CIS Controls (cont.)



CIS RAM: Risk Assessment Criteria

Impact Score	Impact to Mission *Mission: Provide information to help remote patients stay healthy.*	Impact to Objectives *Objectives: Operate profitably.*	Impact to Obligations *Obligations: Patients must not be harmed by compromised information.*
1	Patients continue to access helpful information, and outcomes are on track.	Profits are on target.	Patients do not experience loss of service or protection.
2	Some patients may not get all the information they need as they request it.	Profits are off target, but are within planned variance.	Patients [illegible] but not h[illegible]
3	Some patients cannot access the information they need to maintain good health outcomes.	Profits are off planned variance and may take a fiscal year to recover.	Some pa[illegible] harmed f[illegible] reputationally after compromise of information or services.
4	Many patients consistently cannot access beneficial information.	Profits may take more than a fiscal year to recover.	Many patients may be harmed financially or reputationally
5	We can no longer provide helpful information to remote patients.	The organization cannot operate profitably.	Some patients may be harmed financially, reputationally, or physicall up to and including death.

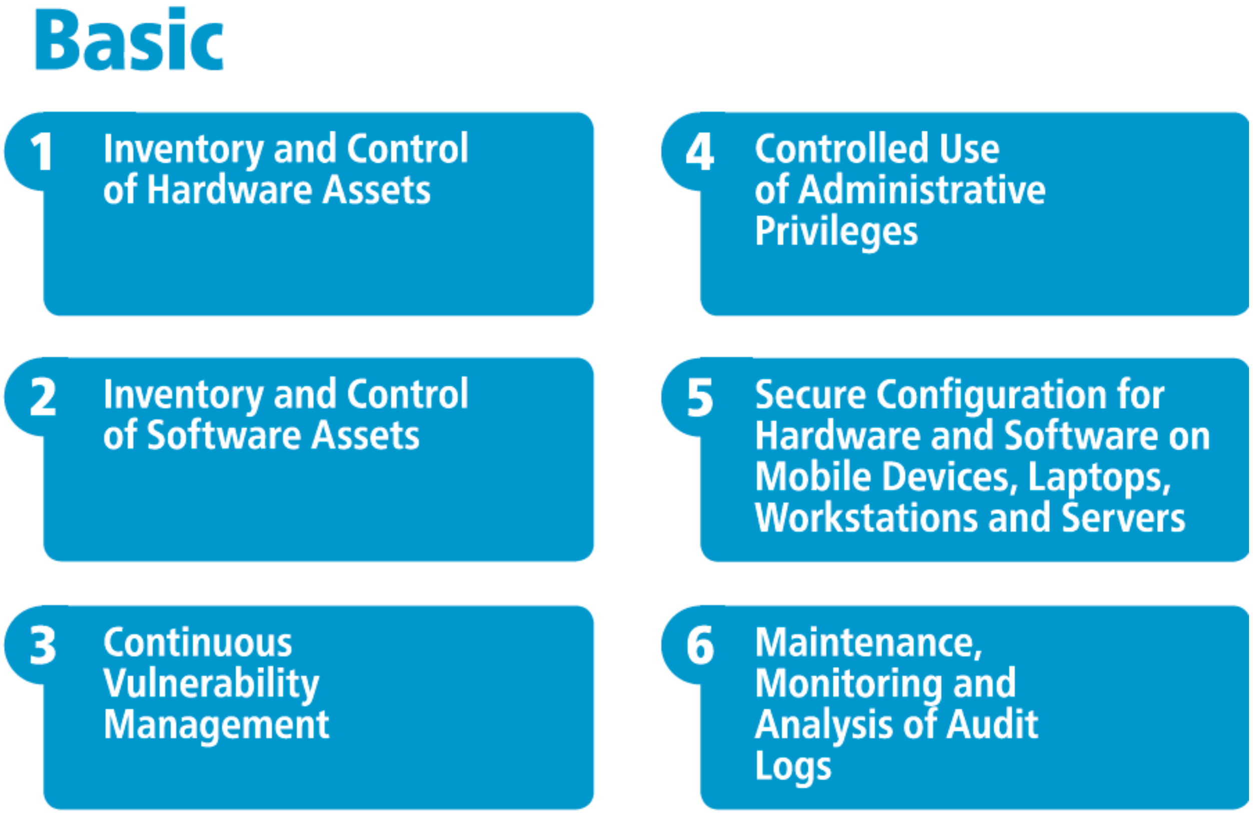
Likelihood Score	Foreseeability
1	**Not foreseeable**. This is not plausible in the environment.
2	**Foreseeable**. This is plausible, but not expected.
3	**Expected**. We are certain this will eventually occur.
4	**Common**. This happens repeatedly.
5	**Current**. This may be happening now.

13

56:04

Figure source: Center for Internet Security

CIS Controls (cont.)



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

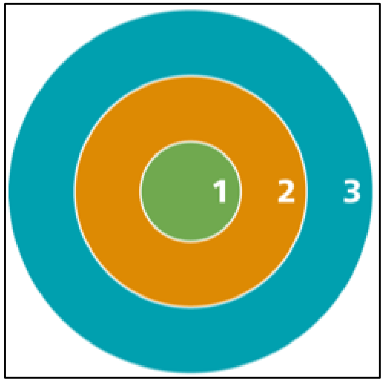
4 Controlled Use of Administrative Privileges

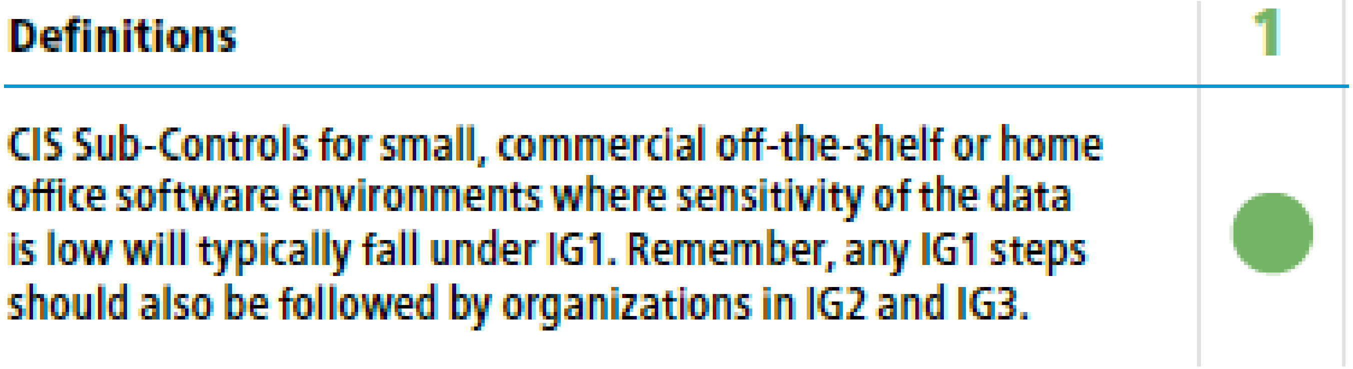
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Figure source: Center for Internet Security

CIS Controls (cont.)





Definitions 1

CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. Remember, any IG1 steps should also be followed by organizations in IG2 and IG3. ●

Identified 5 most important attack types:

- Web-Application Hacking
- Insider and Privilege Misuse
- Malware
- Ransomware
- Targeted Intrusions

Implementing only the 43 sub-controls in IG1 mitigated:

- All 5 attack types
- 62% of all Mitre ATT&CK Techniques

Figure source: Center for Internet Security

CIS Controls (cont.)

CIS Controls	Sub Controls	Asset Type	Title
1	1.4	Devices	Maintain Detailed Asset Inventory
1	1.6	Devices	Address Unauthorized Assets
2	2.1	Applications	Maintain Inventory of Authorized Software
2	2.2	Applications	Ensure Software is Supported by Vendor
2	2.6	Applications	Address unapproved software
3	3.4	Applications	Deploy Automated Operating System Patch Management Tools
3	3.5	Applications	Deploy Automated Software Patch Management Tools
4	4.2	Users	Change Default Passwords
4	4.3	Users	Ensure the Use of Dedicated Administrative Accounts
5	5.1	Applications	Establish Secure Configurations
6	6.2	Network	Activate audit logging
7	7.1	Applications	Ensure Use of Only Fully Supported Browsers and Email Clients
7	7.7	Network	Use of DNS Filtering Services
8	8.2	Devices	Ensure Anti-Malware Software and Signatures are Updated

CIS Controls (cont.)

CIS Controls	Sub Controls	Asset Type	Title
8	8.4	Devices	Configure Anti-Malware Scanning of Removable Devices
8	8.5	Devices	Configure Devices Not To Auto-Run Content
9	9.4	Devices	Apply Host-Based Firewalls or Port Filtering
10	10.1	Data	Ensure Regular Automated BackUps
10	10.2	Data	Perform Complete System Backups
10	10.4	Data	Ensure Protection of Backups
10	10.5	Data	Ensure Backups Have At least One Non-Continuously Addressable Destination
11	11.4	Network	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices
12	12.1	Network	Maintain an Inventory of Network Boundaries
12	12.4	Network	Deny Communication over Unauthorized Ports
13	13.1	Data	Maintain an Inventory of Sensitive Information
13	13.2	Data	Remove Sensitive Data or Systems Not Regularly Accessed by Organization
13	13.6	Data	Encrypt the Hard Drive of All Mobile Devices.
14	14.6	Data	Protect Information through Access Control Lists

CIS Controls (cont.)

CIS Controls	Sub Controls	Asset Type	Title
15	15.7	Network	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data
15	15.1	Network	Create Separate Wireless Network for Personal and Untrusted Devices
16	16.8	Users	Disable Any Unassociated Accounts
16	16.9	Users	Disable Dormant Accounts
16	16.11	Users	Lock Workstation Sessions After Inactivity
17	17.3	N/A	Implement a Security Awareness Program
17	17.5	N/A	Train Workforce on Secure Authentication
17	17.6	N/A	Train Workforce on Identifying Social Engineering Attacks
17	17.7	N/A	Train Workforce on Sensitive Data Handling
17	17.8	N/A	Train Workforce on Causes of Unintentional Data Exposure
17	17.9	N/A	Train Workforce Members on Identifying and Reporting Incidents
19	19.1	N/A	Document Incident Response Procedures
19	19.3	N/A	Designate Management Personnel to Support Incident Handling
19	19.5	N/A	Maintain Contact Information For Reporting Security Incidents
19	19.6	N/A	Publish Information Regarding Reporting Computer Anomalies and Incidents

Conclusion

CIS Controls®

HPH Sector:

- Comprised of organizations of various sizes, budgets, IT-experience, and data
- According to the Verizon DBIR, in 2019:
    - Over 41 million patient records lost in breaches
    - 3.8 million employee-related incidents affecting patient data

CIS Controls:

- They offer an initial starting point for execution of a cyber security strategy
- They are scalable to meet the needs of the smallest to largest organizations
- Execution of the initial 43 sub-controls can defend against the five major cyber attacks and mitigates 62% of Mitre ATT&CK Techniques
- Provide a quick security win for the Healthcare and Public Health (HPH) Sector

Figure source: Center for Internet Security

Reference Materials

References

- Center for Internet Security
  - https://www.cisecurity.org/
- Cybersecurity Best Practices
  - https://www.cisecurity.org/cybersecurity-best-practices/
- CIS Communities
  - https://www.cisecurity.org/communities/
- CIS Benchmarks
  - https://www.cisecurity.org/cis-benchmarks/
- The 20 CIS Controls & Resources
  - https://www.cisecurity.org/controls/cis-controls-list/
- MS-ISAC
  - https://www.cisecurity.org/ms-isac/
- EI-ISAC
  - https://www.cisecurity.org/ei-isac/
- Cleaning Up a Definition of Basic Cyber Hygiene
  - https://www.cisecurity.org/blog/cleaning-up-a-definition-of-basic-cyber-hygiene/
- CIS Blog
  - https://www.cisecurity.org/resources/?type=post

References (cont.)

- Verizon 2020 Data Breach Investigations Report (DBIR)
  - https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
- Tony Sager of CIS on the Origin and Importance of Critical Security Controls
  - https://www.youtube.com/watch?v=SyLSA8kxV8Q
- Cleaning Up Our Cyber Hygiene
  - https://www.sans.org/webcast/recording/citrix/115955/252745
- CIS RAM Webinar
  - https://www.cisecurity.org/webinar/cis-ram-risk-assessment-method-launch-event/

Questions

Questions

Upcoming Briefs

- Fileless Malware (9/10)
- Malspam (9/17)

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV