



IT Security Controls

By: Jay Chen

What are IT Security Controls?

- Safeguards or countermeasures to avoid, detect, counteract, or minimize security risk
- Types of Controls
 - **Preventive Controls**
(E.g. Password lockout after 5 failed attempts)
 - **Detective Controls**
(E.g. Intrusion Detection System (IDS) Alerting on Attacks)
 - **Corrective Controls**
(E.g. Patch management, Incident Response Team)
 - **Physical Controls**
(E.g. Locks, fences, doors)
 - **Procedural Controls**
(E.g. Security awareness training, incident response plan)
 - **Technical Controls**
(E.g. Anti-virus, firewall, user authentication)
 - **Legal Controls**
(E.g. Policies)

Why do we need IT Security Controls?

- Laws and regulations (HIPAA, PCI, GDPR)
- Protect critical infrastructure
- Ensure the CIA Triad
- Prevent security incidents
 - “Global Average Cost of a data breach is \$3.86 million”
 - “Average cost for each stolen record is \$148 per record”

<https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx>

Regulations and Industry Standards

- HIPAA (Healthcare)
- FERPA (Education)
- FISMA (Government)
- State Laws – NY DFS (Financial)
- International Laws – GDPR (EU)
- Industry Standards – PCI DSS (Payment Processors)

So how do we ensure we have the correct IT controls?

By using frameworks

What is a security framework?

- A framework consisting of policies, procedures, and processes that define how information is managed in a business, to lower risk and vulnerability
- A framework is not:
 - A regulation
 - A legislation
- However, a framework is a best practice



List of Security Frameworks

- **COBIT**
 - Created by ISACA
 - Risk Management Framework
- **ISO 27000 Series**
 - Created by International Organization for Standardization (ISO)
 - Information Security Standards
- **NIST SP 800 Series** (<https://csrc.nist.gov/publications/sp800>)
 - Created by National Institute of Standards and Technology
 - Technology/Computer Security Frameworks and Guidelines
 - 100+ SP Series Publications
 - Highlights
 - 800-53 (Security and Privacy Controls for Information Systems and Organizations) 494 Pages
 - 800-37 (Risk Management Framework)
 - 800-12 (An Introduction to Information Security)
 - 800-121 (Guide to Bluetooth Security)
 - 800-184 (Guide for Cybersecurity Event Recovery)
 - 800-115 (Technical Guide to Information Security Testing and Assessment)

List of Security Frameworks

- **PTES (Penetration Testing Execution Standard)**
 - Created by a group of information security practitioners
 - http://www.pentest-standard.org/index.php/Main_Page
- **NIST Cybersecurity Framework (NIST CSF)**
 - Created by National Institute of Standards and Technology
 - A shorten 800-53 for private sector businesses
- **HiTrust CSF (Health Information Trust Alliance Common Security Framework)**
 - Cybersecurity Framework for healthcare industry (HIPAA)
- **CIS Top 20**
 - Created by Center for Internet Security
 - Top 20 Security Controls

CIS Top 20



- Center for Internet Security Top 20 Controls
- CIS Top 20 Critical Security Controls is a prioritized set of best practices created to stop the most pervasive and dangerous threats.
- 3 Tier Implementation Level



- CIS Category
 - Basic CIS Controls
 - Foundational CIS Controls
 - Organizational CIS Controls



Basic CIS Controls (Technology)

Basic CIS Controls

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 CIS Controls (Technology)

Foundational CIS Controls

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 CIS Controls (People & Process)

Organizational CIS Controls

- 17. Implement a Security Awareness and Training Program
- 18. Application Software Security
- 19. Incident Response and Management
- 20. Penetration Tests and Red Team Exercises

Analyzing CIS Controls

Inventory and Control of Hardware Assets

CIS Controls™ • CIS Control 1 *This is a basic Control*

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 gaining access.

Main Points:

- Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.
- Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.

CIS Control 1 Implementation Guide

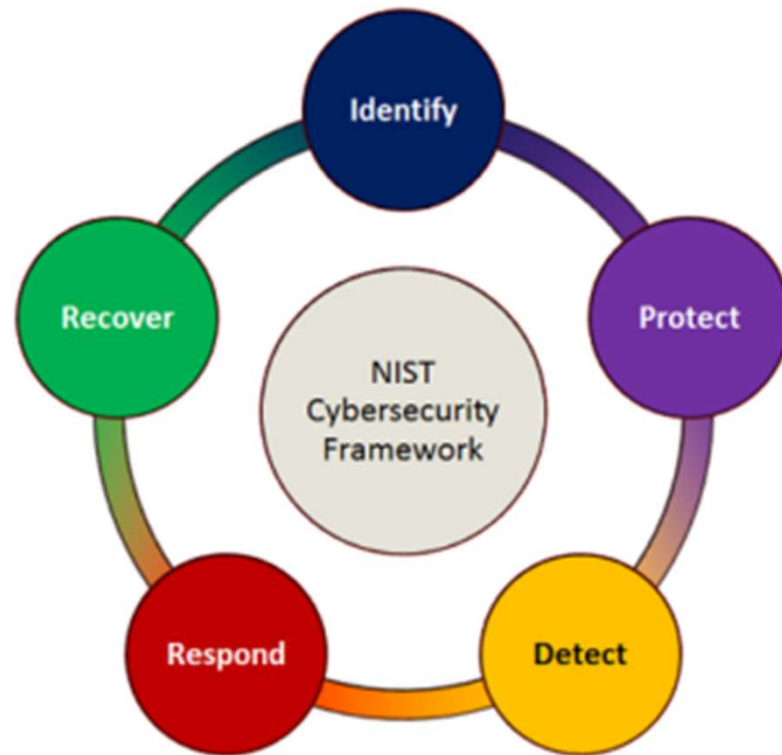
CIS Control 1: Inventory and Control of Hardware Assets

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
1.1	Devices	Identify	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory.		●	●
1.2	Devices	Identify	Use a Passive Asset Discovery Tool	Utilize a passive discovery tool to identify devices connected to the organization's network and automatically update the organization's hardware asset inventory.			●
1.3	Devices	Identify	Use DHCP Logging to Update Asset Inventory	Use Dynamic Host Configuration Protocol (DHCP) logging on all DHCP servers or IP address management tools to update the organization's hardware asset inventory.		●	●
1.4	Devices	Identify	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	●	●	●
1.5	Devices	Identify	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		●	●
1.6	Devices	Respond	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	●	●	●
1.7	Devices	Protect	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.		●	●
1.8	Devices	Protect	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

What is NIST CSF?

- NIST Cybersecurity Framework
- Created by the National Institute of Standards and Technology (NIST)
- The NIST cybersecurity framework separate into five cores
 - Identify
 - Detect
 - Protect
 - Response
 - Recover
- These five cores represents industry standards, guidelines, and practices for cybersecurity activities across an organization.

NIST Cybersecurity Framework



Identify

- Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

Protect

- Develop and implement appropriate safeguards to ensure delivery of critical services.

PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology

Detect

- Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes

Respond

- Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements

Recover

- Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Control Breakdown

Functions	# of Subcategory (Controls)
Identify	29
Protect	39
Detect	18
Respond	16
Recover	6
Total	108

NIST CSF Structure (Categories)

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational		
DETECT			
RESPOND			
RECOVER			

Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational confidentiality, integrity, and availability requirements.

NIST CSF Structure (Subcategories)

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational	PR.DS-1: Protect data (including phys records) during storage to achieve	
DETECT			
RESPOND			
RECOVER			

PR.DS-1: Protect data (including physical records) during storage to achieve confidentiality, integrity, and availability goals

NIST CSF Structure

Framework Core			
Functions	Categories	Subcategories	References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational	PR.DS 1: Protect data (including phys records) during storage to achieve	COBIT APO01.06, BAI02.01 ISO/IEC 27001 A.15.1.3
DETECT			
RESPOND			
RECOVER			

- COBIT APO01.06, BAI02.01
- ISO/IEC 27001 A.15.1.3
- CCS CSC 17
- NIST SP 800-53 Rev 4 SC-28

NIST CSF Structure

1	Function	Category	Subcategory	Satisfied?	Risk (1-5)	Informative References
2	IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	Yes	3	<ul style="list-style-type: none"> CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
3			ID.AM-2: Software platforms and applications within the organization are inventoried	No	4	<ul style="list-style-type: none"> CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5
4			ID.AM-3: Organizational communication and data flows are mapped	Yes	5	<ul style="list-style-type: none"> CIS CSC 12 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
5			ID.AM-4: External information systems are catalogued	Yes	1	<ul style="list-style-type: none"> CIS CSC 12 COBIT 5 APO02.02, APO10.04, DSS01.02 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
6			ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	No	2	<ul style="list-style-type: none"> CIS CSC 13, 14 COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
7			ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Yes	1	<ul style="list-style-type: none"> CIS CSC 17, 19 COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						

NIST CSF (First Two Controls)

Function	Category	Subcategory
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried

NIST CSF Mapping

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	CIS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	CIS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 NIST SP 800-53 Rev. 4 CM-8, PM-5

CIS Control Mapping

CIS Controls™ • CIS Control 1 *This is a basic Control*

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 gaining access.

CIS Controls™ • CIS Control 2 *This is a basic Control*

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

The End

- Questions?