Task 6

IT security experts use the CIS Critical Security Controls Version 7 to establish digital security protections within organizations. With these defenses firmly in place, organizations can flush out most of the typical cyberattacks.

Here are the seven fundamental principles that serve as the bedrock of the framework.

1. The CIS Critical Security Controls Version 7 must address current attacks, emerging technology, and changing business requirements for IT.

As part of its core promise, the CIS Controls continually update and re-structure to reflect the presence of new cybersecurity tools and new threats as they happen.

1. There has to be more focus on authentication, application whitelisting, and encryptions.

The guidance for these essential topics is more precise, robust, and consistent across all CIS Controls.

1. The CIS Controls now have better alignment with other frameworks such as the [NIST Cybersecurity Framework](https://blog.rsisecurity.com/why-you-should-adopt-the-cybersecurity-nist-framework/). With more emphasis on multi-framework functionality, it offers better dynamics to companies.
2. Improvement of the wording of each sub-control has been prioritized. Each sub-control only has one “ask,” and the consistency of the syntax has been simplified.

The expert community worked tirelessly to clarify the intention of each CIS Control to be more user-friendly. Multiple tasks have been eliminated so that they can be measured, monitored, and implemented more efficiently.

1. A rapidly growing ecosystem of devices, products, and services from both CIS and the marketplace now has a better foundation set in place. The documentation is better since Version 6 made an effort to improve importing, tracking, and integrating the CIS Controls.
2. The layout and format have been bolstered with structural changes. And flexibility is prioritized so that various organizations can help keep the Controls adaptive and relevant to their industries.
3. With growth encouraged, there is now a system in place that will reflect the feedback of a global community of supporters, volunteers, and adopters. The CIS Security Controls Version 7 believes it is only as strong as the support that sustains it. The hope is to provide more guidance and resources for the entire cybersecurity community.

The CIS Controls V7 are now separated into three particular categories listed below:

* Basic (CIS Controls 1-6): All organizations must follow the key controls for essential protection against cyber threats.
* Foundational (CIS Controls 7-16): Companies must adhere to these best practices to have further security protection.
* Organizational (CIS Controls 17-20): These have more technical elements to boost a more robust cybersecurity system in place.

**Basic Controls**

* **CIS Control 1: Inventory and Control of Hardware Assets**

 All hardware devices within the network must undergo active management. This encompasses inventory, tracking, and correction. All devices must be authorized to screen unmanaged devices from gaining access to the network.

* **CIS Control 2: Inventory and Control of Software Assets**

 All software within the network must undergo active management. Companies must adhere to this basic control, including the proper inventory, tracking, and correction of authorized software, in order to avoid installing and executing unmanaged software.

* **CIS Control 3: Continuous Vulnerability Management**

 New information must be continuously acquired, assessed, and taken action so that vulnerabilities are identified and remediated. The objective is to minimize the window of opportunity for cyber attackers.

* **CIS Control 4: Controlled Use of Administrative Privileges**

 There must be proper supervision of the tools and processes used for the active management of hardware and software. Administrative privileges on networks, computers, and applications must be adequately managed.

* **CIS Control 5: Secure Configuration for Hardware/Software on Mobile Devices, Laptops, Workstations, Servers**

 The security configuration of servers, workstations, mobile devices, and laptops must be implemented and established using a rigorous configuration management and change control process. The active management of this security will prevent attackers from tampering and exploiting vulnerabilities.

* **CIS Control 6: Maintenance, Monitoring, and Analysis of Audit Logs**

 Audit logs of events are essential to monitor, understand, troubleshoot, and detect attacks. There must be a system in place for its collection, management, and analysis.

**Foundational Controls**

* **CIS Control 7: Email and Web Browser Protections**

 The window of opportunity of cyber attackers using email systems and web browsers must be minimized so that human behavior cannot be manipulated easily.

 One of the popular types of cyberattacks is phishing, a fraudulent attack wherein cybercriminals try to acquire critical and sensitive data such as usernames and passwords through spam emails or text messages. The modus operandi uses a disguise as a trustworthy organization such as a bank or a government agency to scam employees into providing necessary information.

* **CIS Control 8: Malware Defenses**

 Malicious code can spread and execute if there is no existing installation control at multiple points in the organization’s digital environment. The company can optimize automation to help with the rapid updating of cyber defense, data gathering, and corrective action.

* **CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services**

 The operational use of ports, protocols, and services on networked devices must be managed actively using tracking, control, and correction protocols. This minimizes the available vulnerabilities that can be exploited by cyber attackers.

* **CIS Control 10: Data Recovery Capabilities**

 Data recovery is essential for the overall security of an organization. There must be a proven methodology for the timely recovery of data using processes and tools to back up vital information. Without a system in place for data recovery, the long-term operations of a company can severely suffer. When crucial data is gone forever, it can have damaging implications to a company’s reputation and output.

* **CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches.**

 Organizations must enforce a rigorous configuration management and change control process of network infrastructure devices. When actively managed, this security configuration can prevent attackers from vulnerabilities and exploitations. These serve as the first line of defense of an organization. When these are left vulnerable, cyberattackers can easily exploit these weaknesses with impunity.

* **CIS Control 12: Boundary Defense**

 There must be a focus on security0-damaging data when monitoring the flow of information across networks. Detection, prevention, and correction are vital processes in this Control.

**Organizational Controls**

* **CIS Control 17: Implement a Security Awareness and Training Program**

 There must be a program in place to identify specific knowledge, skills, and abilities essential in defending the organization from cyber-attacks. This must be assessed across all functional roles in the organization, especially the business’s mission-critical designations. An integrated plan must assess, determine gaps, and remediate through awareness programs.

* **CIS Control 18: Application Software Security**

 Whether in-house or acquired, the software must have a robust security life cycle to prevent security vulnerabilities.

* **CIS Control 19: Incident Response and Management**

 A reliable incident response infrastructure must be implemented and developed to protect the organization, particularly its reputation. This includes defined roles, plans, training, management oversight, and communications. The flow of the response must begin with discovering the attack and must commence with damage control, eradication of the attacker’s presence, and the restoration of network integrity.

* **CIS Control 20: Penetration Tests and Red Team Exercises**

 Simulating an attacker’s objectives and methodology can help the organization prepare and test its defensive strategy strength. This should cover all aspects, including the technology, the policies, and the personnel.