7 Steps to Successfully Implement the Top 20 Controls in Your Organization

If you think of the CIS Top 20 Critical Security Controls as a minimum set of security requirements, then being able to show how your protocols map in compliance with these controls can help you get management buy-in on developing your security program. We’ve assembled seven practical steps to help you implement key controls into both your tactical day-to-day practices, as well as your high-level strategic plans and decisions.

1. Take inventory of your assets

This step provides an essential foundation—after all, you can’t implement any controls meant to protect devices and users if you don’t know what you’re protecting.

Maps to: Critical Security Controls 1, 2

Key considerations:
• Identify target systems
• Catalog installed software

2. Measure asset controls

Next, determine your baseline for what controls are already in place and where you have invested funds and effort. Make sure you understand how well you are (or aren’t) currently protected so you can make it clear to IT and upper management.

Maps to: Critical Security Controls 3, 4, 7, 8, 10

Key considerations:
• Secure configurations for mobile devices, desktops, and servers
• Security products, like malware prevention and whitelisting
• Internal processes, like patching and configuration management
3. Detect and respond to incidents

It might be minor, it might be random, it might be targeted—you can’t know exactly how an attack will go down, but you can count on it happening. Be prepared with a plan of action, as well as a documented internal process that feeds back into your overall plan for improving security by implementing and maintaining controls.

**Maps to:** Critical Security Controls 6, 16, 19

**Key considerations:**
- Detect indicators of compromise or breach
- Perform forensics to investigate how it started
- Take action to stop the attack and prevent it from happening again

4. Evaluate the most critical gaps

You need to know where the gaps are to help you prioritize how to move your security program forward. But be ready: Determining which gaps are the most critical requires consensus across teams. While this step can take some time to get through, the extra effort pays dividends.

**Maps to:** All Critical Security Controls

**Key considerations:**
- Get buy-in from IT and management
- Compare new vs. existing controls
- Measure the value to the organization

5. Plan and implement your controls

Okay, so now you know how secure you are and where your most critical gaps are. Next up: Deciding how you’ll approach short-term and long-term maintenance and tracking over time. Remember, controls should be treated as a continuous process that’s maintained over time, not a one-off project.

**Maps to:** All Critical Security Controls

**Key considerations:**
- Agree on metrics and goals for tracking progress
- Coordinate efforts between security and IT
- Communicate progress regularly with management
6. Train and monitor users

People – as much as we love them – are often the weakest link in the security chain. That’s why it’s essential to train and test users to make sure they understand what to look out for, as well as the importance of security. It’s also good to have a backup plan: Limiting privileges and monitoring user behavior for anomalies are both effective fail-safes.

**Maps to:** Critical Security Controls 5, 7, 14, 16, 17

**Key considerations:**

- Conduct simulated phishing campaigns
- Track web browsing traffic to malicious websites
- Control the use of administrative privileges

---

7. Test your controls

Now that your controls are in place, use tools such as penetration testing and red team exercises to make sure they’re working. This exercise should be done regularly (and with enthusiasm), as knowing your efforts are paying off gives you both confidence and internal credibility.

**Maps to:** Critical Security Control 20

**Key considerations:**

- Test effectiveness of your controls against attack
- Explore how controls complement each other
- Generate reports to share with stakeholders
INDEX: Top 20 Critical Security Controls

Numbers represent Rapid7’s score from SANS, calculated by totaling the number of measurements Rapid7 offers, divided by the total number of measurements listed for that control. Download the Top 20 Critical Security Controls.

CSC 1 - Inventory of Authorized and Unauthorized Devices

| 60-79% | 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. |

CSC 2 - Inventory of Authorized and Unauthorized Software

| 40-59% | Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution. |

CSC 3 - Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

| 80-99% | Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |

CSC 4 - Continuous Vulnerability Assessment and Remediation

| 60-79% | Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remEDIATE and minimize the window of opportunity for attackers. |

CSC 5 - Controlled Use of Administrative Privileges

| 100% | Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. |

CSC 6 - Maintenance, Monitoring, and Analysis of Audit Logs

| 100% | Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. |

CSC 7 - Email and Web Browser Protections

| 100% | Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems. |

CSC 8 - Malware Defenses

| 60-79% | 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. |

CSC 9 - Limitation and Control of Network Ports, Protocols, and Services

| 60-79% | Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers. |

CSC 10 - Data Recovery Capability

| 100% | Properly back up critical information with a proven methodology for timely recovery. |

CSC 11 - Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

| 60-79% | Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. |

CSC 12 - Boundary Defense

| 80-99% | Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data. |

CSC 13 - Data Protection

| 100% | Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. |

CSC 14 - Controlled Access Based on the Need to Know

| 40-59% | Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification. |

CSC 15 - Wireless Access Control

| 20-39% | Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems. |

CSC 16 - Account Monitoring and Control

| 100% | Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them. |

CSC 17 - Security Skills Assessment and Appropriate Training to Fill Gaps

| 60-79% | Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify, and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization. |

CSC 18 - Application Software Security

| 100% | Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses. |

CSC 19 - Incident Response and Management

| 60-79% | Protect the organization’s information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight). |

CSC 20 - Penetration Tests and Red Team Exercises

| 100% | Test the overall strength of an organization’s defenses (technology, processes, and people) by simulating the objectives and actions of an attacker. |