

CIS 18 Critical Security Controls Checklist

Learn how to Achieve CIS®
Compliance.



Lansweeper

What Are the 18 CIS Critical Security Controls®?

When companies struggle with what to do and how to demonstrate their Cyber Security efforts, many turn to ISO27001 & ISO27002. These frameworks are excellent for showing compliance but not well-suited for prioritizing, measuring, and implementing practical IT-security initiatives. To that end, you need a consensus-based framework, such as the [CIS 18 critical security controls®](#), which includes detailed practical and prioritized advice on how to implement cyber security. The CIS® controls include detailed instructions on what to do, how to measure, how to prioritize, and how to audit your cybersecurity posture.



3 reasons why you would want to become CIS compliant.



An IT Asset Inventory Database for CIS® Compliance

A well-maintained asset inventory is key in building a more comprehensive security program based on the CIS Critical Security Controls. As you prioritize CIS® Controls, you should focus your efforts on **6 of the controls – also named the Cyber Hygiene Controls or Basic Controls**. The first two controls call for an **Inventory of Hardware Software Assets** and rely heavily on the IT asset inventory.

Lansweeper can be used to support additional controls, but as the controls are most effective when implemented in order, we'll focus on how Lansweeper can support your CIS® compliance for these 6 controls below.

#1: Inventory & Control of Enterprise Assets

#2: Inventory & Control of Software Assets

#4: Secure Configuration of Enterprise Assets & Software

#5: Account Management

#7: Continuous Vulnerability Management

#8: Audit Log Management

See the next page for a few of the questions you need to be asking yourself to become compliant in 6 of the CIS Controls.

CIS 18 Critical Security Controls Checklist

CIS® CONTROL #1

Inventory & Control of Enterprise Assets

- ☐ Do you have a passive network scanner to automatically detect new hardware assets on your network?
- ☐ Does the system in place automatically report on changes of new hardware assets?
- ☐ Do you have a system in place to automatically remove unauthorized devices?

CIS® CONTROL #2

Inventory & Control of Software Assets

- ☐ Are you able to automatically discover new software on your hardware devices?
- ☐ Are you able to automatically discover new software updates/versions on your hardware devices?
- ☐ Do you have a system in place which allows you to mark software as 'allowed', 'denied', or 'neutral'?
- ☐ Are you able to remove unwanted software from your devices?
- ☐ Are you able to create real-time reports & dashboards from these marks?

CIS® CONTROL #4

Secure Configuration of Enterprise Assets & Software

- ☐ Are you able to check and report on Processes, Services & System settings?
- ☐ Are you able to check and report on Bitlocker's status?
- ☐ Can you scan for the existence or absence of specific files and registry keys to adhere to CIS benchmarks guidelines?
- ☐ Are you able to check and report on misconfigured DNS settings?
- ☐ Are you able to uninstall or disable unnecessary services on Enterprise assets?

CIS® CONTROL #5

Account Management

- ☐ Are you able to see detailed user information including account state and password audit data in real-time for AD, O365 & Exchange & local accounts?
- ☐ Are you able to tell which users have local administrative rights on an asset-by-asset basis?
- ☐ Are you able to capture all unauthorized administrators who can manage your assets?
- ☐ Are you able to control who can manage your assets and place restrictions per user?

CIS® CONTROL #7

Continuous Vulnerability Management

- ☐ Are you able to identify if software updates have been updated with important security patches?
- ☐ Are you able to pull vulnerability reports when software updates have been made with important security patches?
- ☐ Are you able to easily assess whether a particular software-related vulnerability has been addressed in dashboards or reports?
- ☐ Can you pull an audit report to address trending vulnerability issues such as [PrintNightmare](#) or [PetitPotam](#)?
- ☐ Are you able to create email alerts to review or alert people when a vulnerability has been addressed or spotted?

CIS® CONTROL #8

Audit Log Management

- ☐ Do you have the possibility to access event log information and keep an eye on anything that might indicate a security risk?
- ☐ Are you able to automatically collect logs from Windows servers and desktops?
- ☐ Is there a way for logs to be searched, reported, and exported?
- ☐ Does your system allow you to check on error logs?
- ☐ Are you able to Retain audit logs across enterprise assets for a minimum of 90 days?

About Lansweeper

Lansweeper is an IT asset management software provider helping businesses better understand, manage and protect their IT devices and network. Lansweeper helps customers minimize risks and optimize their IT assets by providing actionable insight into their IT infrastructure at all times, offering trustworthy, valuable, and accurate insights about the state of users, devices, and software.

Since its launch in 2004, Lansweeper has been developing a software platform that scans and inventories all types of IT devices, installed software, and active users on a network - allowing organizations to centrally manage their IT.

The Lansweeper platform currently discovers and monitors over 80 million connected devices from 28,000+ customers, including Mercedes, FC Barcelona, Michelin, Carlsberg, Nestle, IBM, and Samsung to governments, banks, NGOs, and universities, driven by its 150+ strong teams in Belgium, Spain, Italy, the UK and the USA.

How Lansweeper helps implement CIS Critical Security Controls.

[Click Here To Learn More](#)