

# COMPLIANCE AND SECURITY STANDARDS WITH TENABLE.SC

Meeting multiple industry, regulatory and business partner compliance obligations can require a team to produce an endless list of documents needed to satisfy auditors. The result: scarce security resources can be diverted from reducing the organization's cyber exposure gap to keeping the auditors satisfied.

Many organizations are implementing controls recommended by a security standard to provide a control foundation to support one or more compliance obligations. A Dimensional Research study sponsored by Tenable found that in the U.S., the four most popular standards are PCI DSS (PCI), ISO/IEC 27001/27002 (ISO), CIS Controls, and NIST's Framework for Improving Critical Infrastructure Cybersecurity (CSF). The research also found that organizations that use a security standard typically use more than one. In some cases, different standards were used by different parts of an organization. In other cases, a single part of an organization was using multiple standards.

Adopting a security standard is rarely like buying off-the-shelf clothes from a local retailer. Instead, most organizations tailor standards to meet their specific situation. For example, an organization could use CSF or ISO to guide risk assessment and use CIS Controls to prioritize technical control implementation.

Whatever security standard your organization selects, you need to automate as many controls as possible.

## AUTOMATE COMMON CONTROLS

In many cases, controls prescribed by a leading security standard will satisfy compliance obligations. However, some compliance requirements will specify additional or modified controls. If so, it may be more efficient to tailor the security standard to incorporate specific compliance requirement than to design, implement and maintain multiple control variants.

Tenable.sc™ enables you to measure, visualize, and effectively communicate adherence to security controls. Tenable.sc automates the assessment of many technical controls from ISO/IEC 27001/27002, NIST Cybersecurity Framework, NIST SP 800-171 and CIS Critical Controls to ensure they are in place and operating effectively.

Tenable.sc delivers broad and continuous coverage across your entire environment, including physical, virtual, cloud, and mobile devices used in IT and industrial control networks. Dynamic asset lists let you logically segment, manage, and report on the status of specific systems, such as those used for processing EU personal data or for processing payment card data. Intelligent connectors to your existing IT and security products audit configurations and analyze events to identify control weaknesses.

## KEY BENEFITS

- **Build a common control foundation to efficiently address multiple compliance requirements.** Rather than tackling each compliance requirement with ad hoc controls, Tenable.sc can provide a single, extensible foundation to meet multiple compliance requirements.
- **Meet due care/due diligence standards to limit liability.** Many organizations have a legal obligation to understand the cybersecurity risks they face and then implement appropriate controls to manage that risk. Failure to adequately manage risk may open the organization, its executives, and board members to legal action.
- **Communicate business risk to executives and board members.** Business leaders increasingly demand information describing the organization's cyber exposure. Tenable.sc helps you communicate status at a level they will understand.
- **Discuss security with external stakeholders.** Major customers, cyber-insurance suppliers, and other business partners may have questions about an organization's security program, and Tenable.sc provides the information you need for these discussions.

## REPORTING

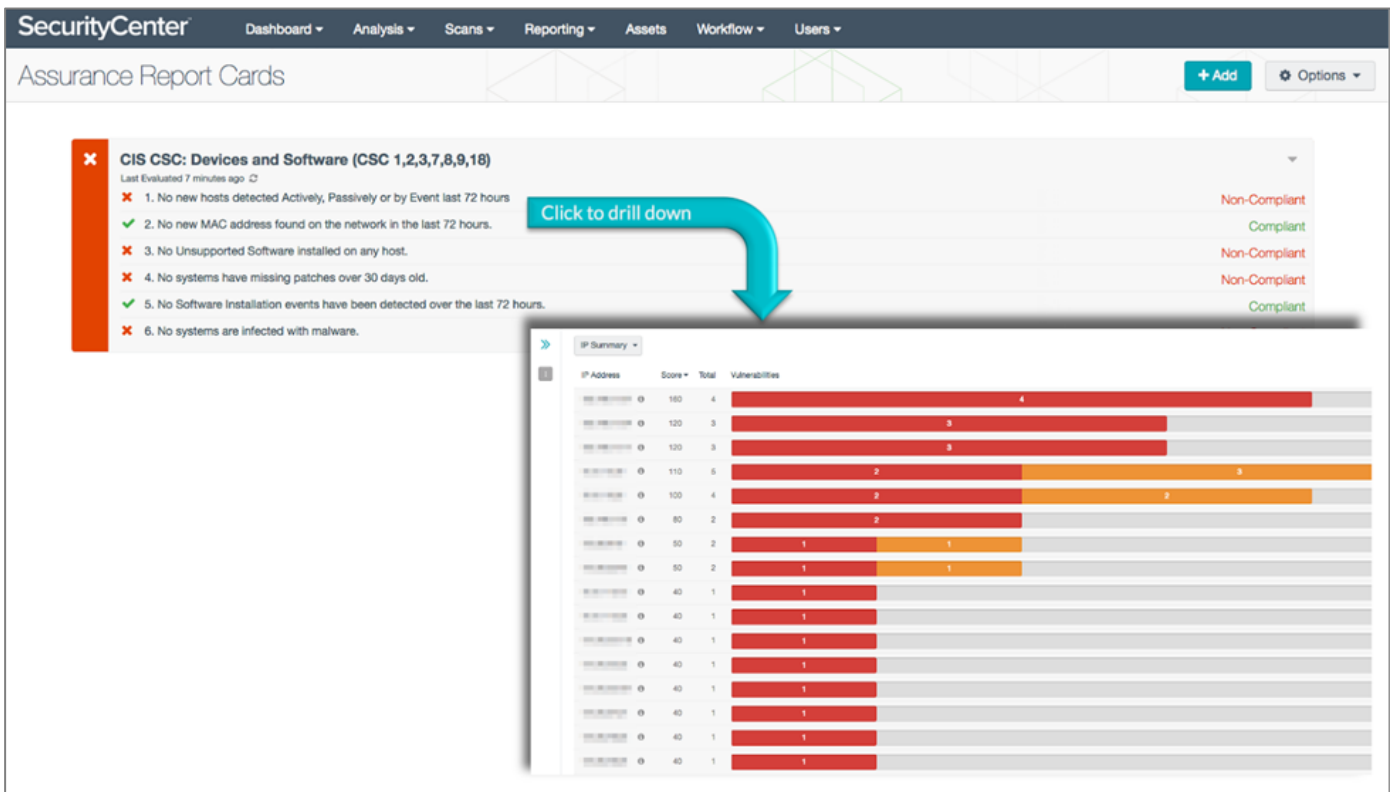
Tenable.sc asset lists linking compliance obligations to in-scope assets include the in-scope assets to specific compliance dashboards and reports. Tenable.sc provides fully customizable reports, dashboards, and Assurance Report Cards (ARCs) specific to the leading security standards – all out-of-the box. You can use them “as-is” or quickly and easily tailor them to meet your specific security and business needs. For example, you can easily create specific reports, dashboards, and ARCs for individual lines of business.

The data that Tenable.sc gathers and analyzes for security standards is often the same data you need for compliance reporting. You can use compliance report templates to present the data in the formats required by multiple compliance standards. The result: redundant controls are eliminated, and the work required by each audit is reduced.

Tenable.sc ARCs complement comprehensive data collection approach, which uses a combination of active scanning, agent scanning, intelligent connectors to your third-party systems, passive listening and host data monitoring to assess the protection status of your complete infrastructure. Together, these capabilities provide you the ability to:

- Measure, visualize, and effectively communicate the technical security controls that help you manage risk.
- Communicate security status to internal and external stakeholders.
- Understand the context you need to prioritize remediation.

Tenable.sc reports, dashboards, and Assurance Report Cards demonstrate adherence with best practice security controls to external business partners and large customers that may have the right to audit your security program.



**SecurityCenter** Dashboard Analysis Scans Reporting Assets Workflow Users

Assurance Report Cards + Add Options

**CIS CSC: Devices and Software (CSC 1,2,3,7,8,9,18)**  
Last Evaluated 7 minutes ago

- ✗ 1. No new hosts detected Actively, Passively or by Event last 72 hours. Non-Compliant
- ✓ 2. No new MAC address found on the network in the last 72 hours. Compliant
- ✗ 3. No Unsupported Software installed on any host. Non-Compliant
- ✗ 4. No systems have missing patches over 30 days old. Non-Compliant
- ✓ 5. No Software Installation events have been detected over the last 72 hours. Compliant
- ✗ 6. No systems are infected with malware. Compliant

**IP Summary**

| IP Address   | Score | Total | Vulnerabilities |
|--------------|-------|-------|-----------------|
| 10.10.10.100 | 100   | 4     | 4               |
| 10.10.10.120 | 120   | 3     | 3               |
| 10.10.10.130 | 130   | 3     | 3               |
| 10.10.10.110 | 110   | 5     | 2               |
| 10.10.10.100 | 100   | 4     | 2               |
| 10.10.10.80  | 80    | 2     | 2               |
| 10.10.10.50  | 50    | 2     | 1               |
| 10.10.10.50  | 50    | 2     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |
| 10.10.10.40  | 40    | 1     | 1               |

*Assurance Report Cards present security status at a high level for a non-technical audience*

**For More Information:** Please visit [tenable.com](https://tenable.com)

**Contact Us:** Please email us at [publicsectorsales@tenable.com](mailto:publicsectorsales@tenable.com) or visit [tenable.com/contact](https://tenable.com/contact)