ISO/IEC 27001/27002 & Tenable

Streamline ISO/IEC 27001/27002 Adoption

SecurityCenter Continuous View® Security ISO/IEC 27001/27002 Capabilities

- **Conformance Assessment** - Automate the assessment of ISO-27K technical controls to determine what is in place and operating effectively
- **Continuous Monitoring** - benefit from both active and passive monitoring to ensure all stakeholders have near real-time visibility into your security posture
- **Complete Coverage** - Gain continuous visibility across your IT networks and industrial control systems, including physical and virtual infrastructure, cloud, and mobile environments
- **Assurance and Reports** - Use customizable ISO-27K reports, dashboards, and Assurance Report Cards to evaluate and communicate security status

Many organizations are basing their security programs on established security frameworks, such as ISO/IEC 27001/27002 (ISO-27K), to manage risk using proven practices. The ISO-27K standards have a rich history dating back to ISO/IEC 17799 in the year 2000 and beyond. Today, ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS).

ISO-27K is especially attractive to multinational organizations that need their systems and security programs to inter-operate across borders. Additionally, thousands of organizations wanting to reassure customers and business partners that they follow ISO-27K recommendations have obtained certification of ISO/IEC 27001 conformance.

ISO/IEC 27002:2013, a code of practice for information security controls, is a companion document to ISO/IEC 27001. It provides guidelines and practices pertaining to the selection, implementation and management of security controls to support an ISMS. ISO/IEC 27002 contains 14 security control clauses containing 35 main security control categories and 114 controls. The 114 security controls are not mandatory and you may select them based on your organization's risk assessment.

Six of the 14 security control clauses contain only administrative controls, e.g. Information Security Policies, Organization of Information Security and Human Resources Security. Approximately 75% of the security controls are administrative. Automating administrative controls is not mandatory, and in many cases, is not feasible. For example, automating the Human Resources Security Control 7.2.3 "There should be a formal and communicated disciplinary process in place to take action against employees who have committed and information security breach" would be difficult.

Conversely, most technical controls require automation to collect and process the high volume of data. Management of Technical Vulnerabilities is an example technical control requiring automation to obtain timely vulnerability information, evaluate exposure and take appropriate measures. Tenable addresses seven of the eight security control clauses that contain at least one technical security control.

Challenges of ISO/IEC 27001/27002 Conformance

Your organization will benefit from adopting ISO-27K, but doing so will introduce unique challenges to address. You must determine how to do so effectively and efficiently – often alongside an array of mandates and industry compliance requirements.

You need automation to implement ISO-27K without straining IT resources that are already stretched thin. Manual validation of adherence to ISO-27K technical controls is nearly impossible, and at best would only provide a snapshot-in-time. Assessing your current security posture "on the fly" is difficult without the right tools.

You may decide to supplement ISO-27K's technical controls with technical controls from other frameworks, such as the Center for Internet Security's Critical Security Controls. If so, you will need an easily extensible solution that can implement and monitor a broad set of technical controls. More importantly, your solution must integrate disparate control information into a single system of record and provide comprehensive reporting.

Automate Effective Conformance

Tenable SecurityCenter Continuous View™ (SecurityCenter CV™) enables you to measure, visualize and effectively communicate adherence to security controls. It automates the assessment of many ISO/IEC 27001/27002 technical controls to ensure they are in place and operating effectively.

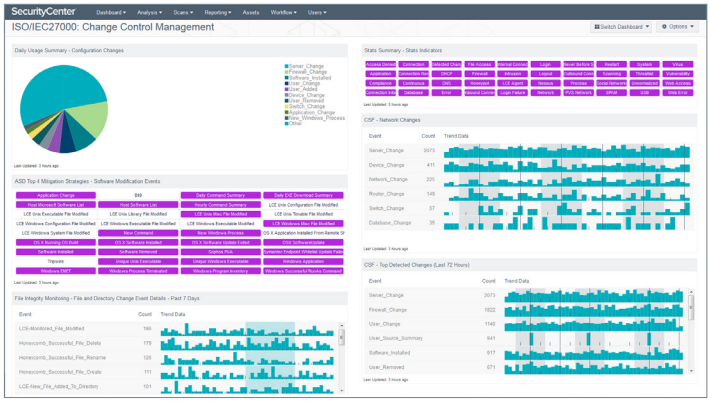
SecurityCenter CV will fit your specific needs. It delivers broad and continuous coverage across your entire environment, including physical, cloud, virtualized and mobile systems used in IT and industrial control networks. Dynamic asset lists let you logically segment, manage, and report on the status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

Communicate Security Status

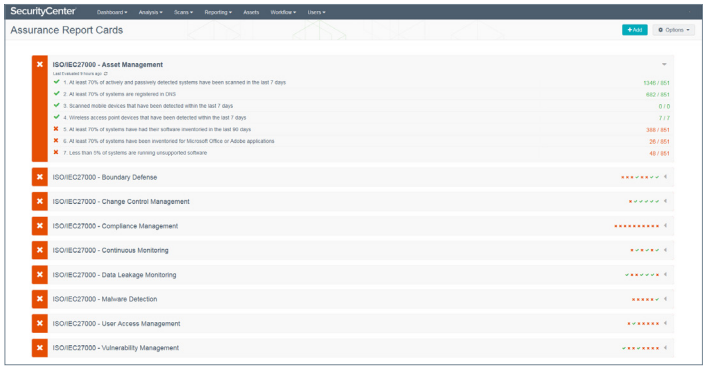
SecurityCenter CV provides fully customizable reports, dashboards, and Assurance Report Cards (ARCs) specific to ISO-27K – all out-of-the box. You can use them "as-is" or quickly and easily tailor them to meet your specific security and business needs. For example, you can combine similar controls from multiple frameworks into a single dashboard.

The data that SecurityCenter CV gathers and analyzes for ISO-27K is often the same data needed 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 reports, dashboards and ARCs demonstrate adherence with best practice security controls to external business partners and large customers that may have the right to audit your security program.



Interactive dashboards consolidate information that you can quickly drill into Assurance Report Cards present security status at a high level for a non-technical audience



ARCs complement the Tenable 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 with the ability to:

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

About Tenable

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact