



SecureVue®: Operational Security for the ISO 27002 Standard

Solution Brief

The following table provides a complete summary of how eIQnetworks' SecureVue platform provides operational security capabilities for the international standard ISO 27002, "Information Technology - Security Techniques - Information Security Management Systems - Requirements", including the scope of supported systems for each ISO 27002 control objective. These capabilities are in addition to specific ISO 27002 reports identified in the companion document, "SecureVue: Compliance Reporting for ISO 27001 and ISO 27002".

ISO27002 Control Objective	How SecureVue Implements this Capability
A.5 - Security Policy	<ul style="list-style-type: none"> ■ SecureVue allows users to translate specific information security policies, such as system configuration standards, acceptable use policies, and others, into actionable policies within SecureVue. ■ SecureVue enables visualization of security strategy across all key types of security data, including: logs and events; configuration data; asset data; known vulnerabilities; performance metrics; and network flow data. ■ SecureVue collects configuration data from a broad range of system assets, including OS's (Windows, UNIX, Linux, and others) and network devices (routers, switches, VPNs, IDS/IPS, and others). The platform can be extended to support custom devices through SecureVue's built-in Universal Parser. ■ Collected configuration data includes (but is not limited to): hardware profiles (all devices/servers); running configurations (devices), including ports/services/protocols; registry settings (Windows servers); configuration settings (devices/servers); running services/daemons (devices/servers); installed applications (servers); and disk configurations, memory configurations, users, groups, and shared resources (servers). ■ Collected data can be measured against any defined security policy, such as system configuration standards, acceptable use policy, and others.
A.6 - Organization of Information Security	<ul style="list-style-type: none"> ■ SecureVue's integrated role-based access control allows organizations to centralize security and compliance monitoring across the enterprise, while providing appropriate separation of duty to security operations, network operations, executive management, compliance and audit, and other stakeholders.
A.7 - Asset Management	<ul style="list-style-type: none"> ■ SecureVue captures a broad range of technology asset data in support of asset inventory. ■ SecureVue can correlate individual users with specific application and process execution, in support of software usage monitoring and restrictions. ■ SecureVue can identify and report on all applications and patches installed on hosts, including the user and run level of the application or patch. ■ SecureVue can monitor applications and process using a combination of events, performance metrics, and flow data, to validate that these applications and processes are compliant with the organization's security engineering principles. ■ SecureVue allows assets to be categorized into user-defined groups based on any criteria, including geographic location, business unit, risk classification, or any other criteria.
A.8 - Human Resources Security	<ul style="list-style-type: none"> ■ SecureVue can enumerate access controls on multiple object types, including: filesystem objects (directories, files, symlinks on Windows, UNIX, and Linux hosts) and Windows registry keys. ■ SecureVue can enumerate user permissions on operating systems. ■ SecureVue can enumerate the default access permissions on filesystem objects. ■ SecureVue establishes monitoring policies to ensure appropriate user/group access controls are assigned to filesystem objects, and users/groups have appropriate operating system permissions. ■ SecureVue can validate that terminated personnel do not have active accounts, and that no network, host, application or database activity is attributable to user after their termination. ■ SecureVue provides alerting (with notification) when policies are violated. ■ SecureVue provides historical reporting of compliance with policies over time.



ISO27002 Control Objective

How SecureVue Implements this Capability

A.9 - Physical and Environmental Security

- If physical security devices (e.g., cameras, badge readers, doorlocks, etc.) and/or visitor check-in software systems generate text-based log files that can be syslogged, SecureVue can capture these log files into its database, normalize the data, and correlate it with other events, system configuration changes, network traffic changes, hardware changes, and other unexpected behavior across the environment.
- SecureVue provides alerting (with notification) when access control policies are violated.
- SecureVue maintains records of all collected data, including physical access control data, for any period of time.
- SecureVue provides historical reporting of compliance with policies over time.

A.10 - Communications and Operations Management

- SecureVue provides a complete inventory of all network and host assets, including (but not limited to): CPU details; local disk/storage details; attached peripheral details; local users and groups; applications; and patches.
- SecureVue establishes configuration baselines for all supported OS's, devices, and databases.
- SecureVue allows customers to establish configuration policies identifying specific user identities and credentials that should not be present on systems.
- SecureVue can identify the prioritization of running processes on systems, and can use performance metrics to determine whether specific service(s) are utilizing inappropriate resources.
- Within SecureVue, users can establish "what is normal" for traffic crossing into or out of the electronic security perimeter by either manually defining allowed sources/destinations, ports, protocols, and services, or by allowing SecureVue to monitor the perimeter and automatically establish a baseline of "normal" traffic patterns.
- SecureVue establishes monitoring policies to determine whether unusual network traffic is identified across the boundary of the electronic security perimeter.
- SecureVue establishes configuration policies to ensure the presence of installed antivirus/antimalware applications and packages.
- SecureVue establishes configuration policies to ensure the presence of running antivirus/antimalware services and daemons.
- SecureVue establishes configuration policies to ensure that antivirus/antimalware data files are within appropriate aging guidelines.
- Different risk profiles, monitors, alerts, compliance requirements, and other monitoring criteria can be created for individual groups of assets, allowing users to see the relative impact of threats based on asset classification.
- SecureVue allows users to establish availability baselines for critical systems, applications, services and ports.
- SecureVue monitors the availability of critical systems, applications, services and ports, and can generate a real-time alert when system availability fails to meet a required threshold.
- SecureVue provides a real-time, out-of-box "Availability" dashboard that identifies the current state of all critical systems, applications, services and ports using a straightforward "stoplight" visualization.
- Using SecureVue's optional agent software, SecureVue can identify data egressing onto removable media, including USB keys, writable CD/DVD devices, and other media.
- SecureVue captures the current system date and time for all systems, validates that an appropriate time service (NTP) is running, and enumerates the time servers associated with each system.
- SecureVue provides alerting and notification when any system or device is no longer compliant with established baselines or policies.
- SecureVue provides historical reporting of compliance with policies over time.



ISO27002 Control Objective

How SecureVue Implements this Capability

A.11 - Access Control

- SecureVue captures user-based events across a broad range of operating systems (Windows, Linux, UNIX, and others), network infrastructure devices (routers, switches, firewalls, IDS/IPS, and others), applications, and databases.
- SecureVue captures the complete record of all user-based events (both successful and failed), including (but not limited to): user ID; date and time of login attempt; success or failure of login attempt; originating system/IP address of login attempt.
- SecureVue can enumerate the lifecycle of user accounts, including creation date, modification date, active/inactive state, deletion date, and other properties.
- SecureVue can enumerate access controls on multiple object types, including: filesystem objects (directories, files, symlinks on Windows, UNIX, and Linux hosts) and Windows registry keys.
- SecureVue can enumerate user permissions on operating systems.
- SecureVue can enumerate the default access permissions on filesystem objects.
- SecureVue establishes monitoring policies to ensure that terminated users are not associated with any system, network, or application activity.
- SecureVue can enumerate which accounts have been inactive for a defined period of time.
- SecureVue can enumerate the allowed logon periods of user accounts.
- SecureVue can enumerate password policies, including (but not limited to): mandatory password complexity; maximum password age; minimum password length; previous password use; password lockout threshold; password lockout duration; session timeout; and screensaver lockout.
- SecureVue can enumerate users across individual systems, as well as directories (Active Directory, LDAP, and RADIUS), and identify duplicate ID's.
- SecureVue establishes configuration policies to ensure that systems are configured to support specific authentication models (e.g., passwords; two-factor) for both local authentication and remote access authentication.
- SecureVue establishes monitoring policies to ensure that password files and log files containing passwords have appropriate authentication and encryption around these files.
- SecureVue provides alerting (with notification) when authentication and access control policies are violated.
- SecureVue provides historical reporting of compliance with policies over time.

A.12 - Information Systems Acquisition, Development and Maintenance

- SecureVue captures a broad range of technology asset data in support of systems acquisition, development and maintenance.
- SecureVue can correlate individual users with specific application and process execution, in support of software usage monitoring and restrictions.
- SecureVue can identify and report on all applications and patches installed on hosts, including the user and run level of the application or patch.
- SecureVue can monitor applications and process using a combination of events, performance metrics, and flow data, to validate that these applications and processes are compliant with the organization's security engineering principles.
- SecureVue establishes configuration policies to ensure that systems are correctly configured for use of encryption technologies.
- SecureVue can perform basic file integrity monitoring without agents (via file properties), and using the optional agent, can perform hash-based file integrity checking.
- SecureVue captures vulnerability data from a broad range of vulnerability assessment tools, including (but not limited to): Nessus; ISS; Qualys; Foundstone; Retina; and Harris STAT.
- SecureVue captures log data from a broad range of IDS and IPS applications and appliances. IDS/IPS data can be correlated with all other system data (configuration, asset, performance, vulnerability, and netflow) to build detailed monitoring policies.
- SecureVue establishes vulnerability baselines for all supported OS's, devices, and databases.
- SecureVue provides alerting and notification when any system or device is no longer compliant with established baselines (e.g., discovery of a new vulnerability; change in severity of an existing vulnerability).

A.13 - Information Security Incident Management

- SecureVue provides over 150 out-of-box alerts for common security incidents, such as failed logins, host hack attempts, and data breaches. All alerts can be customized, and users can create an unlimited number of additional alerts that correlate across any and all collected security data.
- SecureVue users can create their own incident triggers via SecureVue's advanced, GUI-based alerting engine. Alerts can correlate across any type of collected data, including events, configuration and asset changes, network flow data, vulnerability data, and performance metrics.



ISO27002 Control Objective

How SecureVue Implements this Capability

A.14 - Business Continuity Management

- Different risk profiles, monitors, alerts, compliance requirements, and other monitoring criteria can be created for individual groups of assets, allowing users to see the relative impact of threats based on asset classification.
- SecureVue allows users to establish availability baselines for critical systems, applications, services and ports.
- SecureVue monitors the availability of critical systems, applications, services and ports, and can generate a real-time alert when system availability fails to meet a required threshold.
- SecureVue provides a real-time, out-of-box "Availability" dashboard that identifies the current state of all critical systems, applications, services and ports using a straightforward "stoplight" visualization.

A.15 - Compliance

- SecureVue provides out-of-box compliance reporting for a broad range of regulations, best practices, and standards, including (but not limited to): PCI DSS, HIPAA, ISO 27001 and 27002, COBIT, NIST 800-53, NER CIP, GLBA, CIS benchmarks, DISA STIGs, and many others.
- SecureVue provides comprehensive audit-ready reporting for all supported regulations, best practices, and standards. Reports can be generated in a variety of formats including PDF, XLS, TXT, and others, and can be scheduled for automatic delivery via e-mail.
- Users can quickly identify compliance gaps in specific controls, and on specific assets or groups of assets, and immediately address them.



eIQnetworks
31 Nagog Park
Acton, MA 01720
t. +1 978.266.9933
f. +1 978.266.0004
www.eIQnetworks.com