



[Solutions](#) [Products](#) [Industries](#) [Customers](#) [Partners](#) [Support](#) [Company](#) [Contact Us](#)



[Solutions](#)

[Security & Log Management](#)

[Compliance Auditing](#)

[PCI DSS](#)

[HIPAA](#)

[Sarbanes-Oxley](#)

[NISPOM](#)

[FISMA](#)

[DCID](#)

[NERC](#)

[ISO 27002](#)

[IT Operations & Risk Management](#)

[Business Data Intelligence](#)

Compliance with Corporate & Operational Policy

Regardless of industry vertical, global enterprises face a multi-faceted regulatory standards conundrum. For example, all publicly-traded companies are required to comply with SOX regulations. However, the subset of publicly-traded financial services is further required to comply with FFIEC and GLBA mandates, while publicly traded health services enterprises must concurrently meet SOX and HIPAA standards. Because of the many common control objectives existing among these various mandates, a unified framework for corporate governance would yield the most efficient approach to regulatory compliance. A number of organizations have elected to use ISO 27002, Code of Practice for Information Security Management, as their governing framework.

Most analysts agree that using the twelve domains of ISO 27002 as a governing framework, is an effective method to reduce risk and document compliance performance, and demonstrate security due diligence to auditors, board members, and customers.

The ISO 27002 Standard

ISO 27002 is an international security standard published and maintained by the Industrial Electro-technical Committee (IEC) of the International Standards Organization (ISO). As an international standard, it has achieved worldwide recognition and acceptance as a management model for information security. The standard consists of information security management guidelines for use by those responsible for initiating, implementing or maintaining security in their organization.

SenSage's Solution for Operational Compliance

As the ISO 27002 standard provides a unified framework for information security, SenSage provides a virtual "single-server" enterprise security analytic process. By providing a comprehensive network-wide view of log data activity, SenSage delivers an extremely efficient platform from which to address an enterprise's complex compliance obligations. With over 180 available log adapters, and the flexibility to quickly generate additional log adapters as needed, SenSage is unsurpassed in its broad support of log sources to meet any industry or compliance requirement. Furthermore, SenSage solution packages contain multiple pre-defined reports that address specific compliance requirements across the diverse regulations.

These pre-defined reports consist of dozens of queries, organized in the following categories:

- Hosts with Suspicious Network Activity
- Internal Users with Suspicious Activity
- Suspected Data Leakage
- Suspected Online Transaction Fraud
- Investigate Email Usage
- Investigate Hosts
- Investigate Users
- Authentication and Access Control
- Business Critical System Activity
- Operating System Activity
- Email Activity Firewall Activity
- IDS Activity
- Remote Access
- Systems and Security Event Management
- Use of Privilege
- Database Activity
- Web Traffic
- Web Surfing Activity

Resources

Gartner

[Gartner 2009 SIEM Magic Quadrant](#)

» Contact Us