



- [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](#)**

**Demonstrate Compliance with FISMA Security Control Requirements**

The Federal Information Security Management Act (FISMA) mandates security programs for all organizations which possess or use Federal information systems on behalf of a Federal agency.

In a Special Publication 800-53, in particular, The National Institute of Standards and Technology (NIST) details the safeguards needed to ensure the effectiveness of security controls over Federal agency systems and information. At the heart of these controls is an infrastructure with expensive logging and auditing mechanisms capable of storing and protecting massive volumes of log data throughout a network.

SenSage can store multiple terabytes of operating and security information in efficient, super-compressed format, with full data back-up. Flexible loading of any log type allows agencies to integrate data from different devices and applications. This solution also supports ad hoc queries of historical data and flexible reporting.

**Resources**

**Gartner**

Gartner 2009 SIEM Magic Quadrant

Critical Capabilities for SIEM Technology

**Brochures**

FISMA

**Case Studies**

Noridian

**» Contact Us**