

Compliance Auditing for FFIEC



Ease your FFIEC Compliance Efforts While Reducing Overall Costs

Compliance is a critical concern for almost every organization. The Federal Financial Institutions Examination Council (FFIEC) has issued an IT Examination Handbook, describing the processes and standards required for identifying and mitigating risks to consumer financial data privacy. The collection, retention and analysis of event and log data is a key requirement for compliance. SenSage helps organizations quickly implement Compliance Auditing for FFIEC solutions that uniquely deliver actionable results.

Protecting consumer financial information is unquestionably a top priority for IT departments within financial services firms. Unfortunately, protecting against sensitive information leakage is not the only strategic objective for the information security team. The other challenge is effectively demonstrating due diligence with respect to compliance with federal and state mandated regulation. These guidelines require a number of information security controls, many of which include activity monitoring and retention of event log data.

Information security is an ongoing process. Like other risk management activities, good compliance policy not only requires deploying various safeguards, but also reviewing them frequently to ensure their effectiveness. The FFIEC standards call for financial institutions to implement security processes in various areas of control, such as user access rights administration, firewall policy, and remote access. These guidelines also specify that logs and audit trails of these activities be collected, retained, and inspected on a regular basis.

Banking on Audit Logs

With gigabytes of event data collected every day, performance and capacity bottlenecks are common, impacting a financial services firm's ability to adhere to compliance mandates. Managing the process to obtain, store and analyze aggregated data progressively becomes more burdensome, driving substantial expenditures. Yet despite all this increased effort, most organizations still

lack the oversight necessary to meet compliance mandates and perform the required deeper analysis.

SenSage Positions Banks for Success

SenSage Compliance Auditing for FFIEC empowers banks to collect, retain and review terabytes of log data from all sources, and delivers FFIEC-specific compliance reporting.

The solution is specifically built to deliver peerless scalability, with an enterprise-class architecture that can accommodate over 200 log source types – including financial, database, and home-grown applications. Due to this flexibility, SenSage can correlate events between core business systems, operating systems, Web and database applications, empowering financial services firms to address FFIEC guidelines – for immediate as well as long term analysis.

By leveraging an optimized data storage model, SenSage enables financial services firms to manage the enormous amounts of event data required by regulatory standards such as those included in the FFIEC IT examination handbook. When storing this data, SenSage can compress it to as little as 10 percent of the original, raw, event-log data volumes; and 2.5 percent the volume required by a compliance solution based on a Relational Database Monitoring System RDBMS. Since SenSage is based on a purpose-built repository with self-optimized storage, banks can store all their event data without outrageous storage and administrative costs, and ensure that long-term data retention requirements are met. All retained data is rapidly

accessible. In fact, SenSage can produce results from complex queries within minutes rather than the hours often required by other commercial and home-grown solutions.

SenSage Compliance Auditing for FFIEC includes out-of-the-box pre-defined rules and customized report capabilities

to offer IT security professionals more accelerated compliance adherence. Leveraging SenSage’s robust query and reporting capabilities empowers staff to rapidly meet specific audit process requirements and conduct timely forensic investigations.

Log Collection, Retention and Review Requirements as Defined by the FFIEC IT Examination Handbook:

See <http://www.ffiec.gov/guides.htm>

Audit Category	Requirements Addressed by SenSage	SenSage Report Category
Access Control	» Logging and auditing the use of privileged access	» Use of Privilege
Public Key Infrastructure (PKI)	» Recording Certificate Authority (CA) events, secure audit log retention. » Reviewing exception reports and system activity by the CA's employees to detect unauthorized activities	» Authentication and Access Control » Use of System Utilities on Financial Systems
DNS Servers, Routers and Switches	» Logging and monitoring administrative access to these devices	» Use of Privilege » Business Critical System Activity
Firewalls	» Restricting, logging and monitoring administrative access to these devices	» Firewall Activity » IDS Activity
Operating Systems	» Monitoring user or program access to sensitive system resources, including files, programs, processes, or operating system parameters » Filtering logs for potential security events, and providing adequate reporting and alerting capabilities » Activating and using operating system security and logging capabilities, and supplementing them with additional security software » Logging access to system utilities, particularly those with data altering capabilities » Monitoring operating system access by user, terminal, date, and time of access	» Firewall Activity » IDS Activity » Sensitive File System Activity » Use of Privilege » Operating System Activity » System Utility Usage Summary » Hosts with Suspicious Network Activity » Users to Investigate for Financial Fraud » Internal Users with Suspicious Activity
Applications	» Access activity and security events » Using software that enables rapid analysis of user activities	» Sensitive File System Activity » Internal Users with Suspicious Activity
Remote Access	» Monitoring remote access » Monitoring the date, time, user, user location, duration, and purpose for all remote access	» Firewall Activity » Authentication and Access Control

SenSage, Inc. offers patented event data warehouse solutions that provide actionable results from massive amounts of log and event data. Hundreds of customers have deployed SenSage solutions to reduce security, fraud and compliance risks at a fraction of the cost of traditional data warehouses and log management solutions. Based in San Francisco, the company markets its solutions directly and through partners, including Cerner, EMC, HP, Hitachi Data Systems, McAfee, Tokyo Electron Device and many others. Visit www.SenSage.com for more information.