



Achieving Regulatory Compliance through Security-Information Management

Executive Summary

The Compliance Challenge

The explosion of legislation regarding the privacy and security of information is having a profound effect on organizations of all sizes and shapes. These laws, in combination with less formal standards agreed to among nations and organizations across the world, are driving executives and boards of directors to look very closely at details they never cared about before. Suddenly the CIO, CTO, and CSO find themselves accountable for a daunting amount of security requirements and a relentless cycle of compliance auditing.

The challenges associated with these pressures vary to some degree by industry and regulation, but in general they can be satisfied by tailoring an information-security program and architecture to provide the necessary elements of risk management, policy development, active monitoring and incident response, documentation and reporting, and organizational security awareness. No one product or mechanism can ever be a complete solution for the challenge of information security. Maintaining an acceptable level of risk is achieved through a combination of program and process elements, effective management and expertise, and use of the right tools for the task.

Common Requirements of Regulations

Though the industries and focus of privacy and security regulations vary, there are some requirements, either stated or implied, that are common to them all:

- A policy-driven security management program
- Validation of security controls
- A risk-management approach to information security
- Demonstration of due diligence in the application of “internal controls”
- An effective security-incident management process
- Reporting
- Archiving / document preservation

Whether an organization is seeking compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Act (GLBA), the Federal Information Security Management Act (FISMA), or the BASEL II Accord, the most common aspect of succeeding in attaining and demonstrating compliance with any of these is the ability to prove diligence in managing information security risk. Most major regulations require or suggest documentation and some demonstration capability to prove compliance in the case of an audit, but these requirements often vary and are dependent on the auditor’s thoroughness and methodology. The best way to ensure that an audit is completed with the best possible result is first to maintain compliance with the auditing criteria in question and then to ensure quick access to the information an auditor needs.



How Security Information Management (SIM) Solutions Address Compliance Requirements

A fully implemented Security Information Management (SIM) system provides the ability to leverage existing technology and tools to provide real, tangible evidence of security efforts and compliance for clients, business partners, executives, staff, and auditors. Risk assessment is an integral part of any compliance program, and SIM provides the necessary visibility into an infrastructure to assess and manage risk on a real-time and historical basis. A proper SIM implementation is not only an integral part of continuous improvement in the security management life cycle; it also permits an organization to track, prove, and show its success in measurable risk reduction. Internal controls to be audited may include logs, incident reports, alerts, and other data spread across the entire organization on different platforms and systems. Without a SIM solution in place, the average organization would have to spend an inordinate amount of time, energy, and money to sort through and provide this sort of information if it could provide it at all. SIM solutions allow an organization to show not only the individual controls required to maintain security in its environment but also the correlation of those controls and mechanisms as they exist in the broader spectrum of the organization's information security infrastructure.

The central nature of a SIM solution also provides one-stop reporting to provide concise and effective evidence to auditors, managers, and executives, showing just how valid and real those controls are. By integrating security measures, processes, and policies into a framework that can automate critical security operations and safeguards, an organization can dramatically improve its security posture while providing decision support data to continuously improve the information security management process.

Achieving Compliance through Security Information Management

Policy-Driven Security Management

Security policy sits at the center of an organization's security controls. All people, process, and technology controls are instruments of policy, and must implement management intent as stated in an information security policy governing the organization. Since a managed security program flows from security policy, it is the best place to start implementing the necessary changes required to achieve compliance with regulations. If an organization's security policy does not reflect the requirements of a given statute or regulation, the processes and controls that enforce that policy cannot provide the compliance desired. After adjusting policy as necessary, the controls themselves must be designed and configured to implement that policy. A SIM solution permits an organization to measure how well its controls are implementing policy, and thus are complying with applicable regulations. netForensics' Open Security Platform (nFX OSP) can be configured to implement policy and thus relate the management of security directly to the organization's policy.

Validation of Security Controls

Most organizations can truthfully claim to have implemented security controls. How many can provide validation of those controls? How can an organization show that not only has it implemented the necessary controls but, in fact, that they are operating properly and providing the intended protection of critical information assets? At the highest level, regulations such as SOX, HIPAA, GLBA, and FISMA require that an organization demonstrate the presence and effectiveness of security controls. Specific "security controls" are left open to interpretation, but the phrase is widely judged to include:

Controls on human actions and decisions – such as physical barriers to entry for facilities, information stores, and external review of policies

Process controls – such as a formal process for signing off on financial statements; policies and procedures for managing infrastructure changes; defined procedures for investigating possible security breaches; and clearly defined policies, roles, and responsibilities

Information technology controls – a wide range of devices, software, configuration management tools, and policies that apply to all of the organization's information infrastructure elements

Different regulations have their own specific requirements that focus on security, but a well-conceived and implemented security program that effectively leverages people, process, and technology is essential to any compliance initiative. The nFX OSP's ability to correlate data from the inside and perimeter of the network and provide real-time information showing the effects of an attempted attack provides positive validation of the operation of security controls.

Risk Management through Active Monitoring

In order to determine and ensure that systems, processes, and personnel are compliant, an organization must be able to assess and manage risk. Most regulations even demand that risk assessment and management take place as the core of the security program. Risk management and active monitoring go hand in hand because determining and managing risk are based on understanding three things:

1. The relative value of information assets
2. The threats to the confidentiality, integrity, and availability of those assets
3. The vulnerability of the systems and architecture that store and carry those assets

In the past, active monitoring of threats and vulnerabilities was limited to how many logs or alerts a security administrator could manually receive, interpret, and act on. Under this approach, even elaborate prioritization schemes still permit breaches to occur. With the proliferation of security controls in the enterprise and the information they collect, this approach has become wasteful and ineffective; the organization's investment in security infrastructure often occurs without real risk reduction. In the absence of some sort of toolset for managing all of this information, an organization lacks the ability to correlate security events as a meaningful whole, and real-time risk management remains elusive. Compliance starts at the core of the organization, not at the perimeter. Compliance-related assets and groupings must first be identified, and through active monitoring their individual alerts and log entries are then correlated with perimeter devices to provide a managed risk landscape.

Organizations required to comply with HIPAA or GLBA are faced with very severe rules for disclosure in the event of a security breach of protected private information. Under those regulations, a breach of protected healthcare information (PHI) or client financial information, respectively, currently requires that all potentially affected subjects of those breached records be notified of the breach. Since both sorts of records are stored in large databases, if an organization responsible for protecting those records cannot identify which specific record was breached, the entire database must be notified of a potential security situation. For these types of organizations, this can be a catastrophic business event with the potential to inflict permanent and irreparable damage in both financial terms and public perception. With a properly configured netForensics SIM solution such as the nFX OSP, audit trails at the record level from these databases can be centrally collected, stored, and correlated with perimeter devices to provide specific information that allows an organization to recognize and prevent such a breach before it occurs. If for some reason a breach does occur, the depth of active monitoring the product provides allows for accuracy in the disclosure process limiting the necessary notifications and resulting damage. Without a SIM solution with the capabilities of the nFX OSP in place in this situation, pinpointing the depth of the breach would be almost impossible.





Effective Incident Management

An incident-management program is essential to a successful security effort, and this is also borne out in detail in the majority of today's compliance requirements. As one example, the Gramm-Leach-Bliley Act requires protection of customer information and requires the institution to have controls in place to manage and control risk. One required control is an incident-response program for unauthorized events. Without defined procedures for detecting, identifying, mitigating, and eradicating a threat – such as a self-propagating virus – a financial institution would be remiss in its duties under the law. The nFX OSP includes a full incident-management capability that provides the required control and offers one platform for the full cycle of incident management: event detection, evidence collection and archiving, ticketing, prioritization, mitigation, and resolution as events occur. This incident-management capability coupled with the SIM's ability to correlate data from critical assets and perimeter devices in real time offers unprecedented control over the security of valuable data.

Comprehensive Reporting

Regulations instruct companies to provide reports proving control effectiveness, but decentralized reporting at the individual server and resource level can become almost impossible in the sprawl of today's IT environment. Auditors need specific information that must often be collected and manually reconciled among multiple systems and presented in a way that enables them to drill down to underlying detail – down to system event logs if necessary. Network and security operations need details as well, but they need it abstracted to a level that shows operational status and capacity across the enterprise, with alerts to quickly point out problems or changes. Executive reports should provide digestible information that describes *events' significance to the organization* – not thresholds and log detail, but rather vulnerability highlighting, risk assessments, and high medium, and low threat levels – so that executives can more easily decide where to allocate resources.

The organization must be able to maintain its security information integrity while presenting it in a range of formats for audiences – both internal and external. Executive reports must be able to translate technical and operational data into meaningful assessments and reports of current vulnerabilities, document specific improvements, and record incident resolution in order to help executives meet the regulation's burden of proof.

How does an organization know whether it has achieved the compliance levels it desires? How can it show an auditor that it has taken significant steps and prove its efforts? Comprehensive reporting is the key, and the nFX OSP offers a full reporting capability that takes advantage of its correlated archives of security information drawn from sources across the enterprise. Only this approach offers the ability to provide management and auditors alike the answers they need to prove compliance and measure progress all from one combined source.

Archiving and Data Preservation

To meet with the spirit and letter of compliance, as well as to continuously improve their own security postures, organizations must also capture underlying enterprise data in their purest form and preserve that data for forensics and evidentiary presentation. This requirement indicates the need for a secure, fully auditable repository.

All regulations require that some form of logging and audit controls be established, the purpose of which is to collect and retain audit events from security, networking, and computing devices. Organizations must have a way to remain current with the threat environment and the ability to use information from its security infrastructure to continually learn, improve controls, train employees, and maintain high threat awareness. All of the regulations require an established process for providing security awareness and training to employees, as well as ongoing improvement efforts. This demands some kind of information repository, where event data can be available for ongoing improvement efforts. The nFX OSP does this through its archiving

capability which has the architectural flexibility to allow the creation of dedicated compliance reporting installations so real-time monitoring and historical analysis for compliance purposes are always available.

netForensics Compliance Solutions

netForensics understands that there is no single product that can make an organization compliant. However, the nFX Open Security Platform is strategically positioned in the heart of the security infrastructure to incorporate information from strategic applications and critical compliance-related assets, as well as from the perimeter devices that protect them. By providing an open infrastructure to integrate information from all phases of the information security life cycle, the nFX OSP creates a foundation for incorporating policy information, correlating asset and device events to identify potential compliance violations and, following a standard incident-handling process, to mitigate threats to critical compliance-related assets. The nFX OSP facilitates comprehensive compliance solutions delivered by our strategic partners with the following functionality:

Architecture and Integration

The industry's only three-tier SIM architecture allows organizations to create redundancy at every level of the infrastructure to ensure 24x7 monitoring and archiving of events. The flexible architecture also creates flexible deployment options – allowing an organization to monitor events locally and centrally while creating a dedicated compliance reporting installation. Unlike solutions that require all events to be written to a database prior to being presented (a significant problem in a denial-of-service attack that could bring the database to its knees exactly when it's needed most), the nFX OSP allows real-time correlation and notification to continue uninterrupted. This is critical for identifying potential attacks against compliance-specific assets before systems are compromised.

nFX OSP uses a robust database to maintain critical historical data for reporting and audit purposes. *Flexible Storage Management* enables security organizations to have short-term, mid-term, and historical information easily accessible for investigative analysis for operational and compliance reports. These advanced data-management options reduce the cost of storing vast quantities of event information and support efficient compression of data to keep a larger amount of near-term information immediately available "online," while supporting efficient archiving of mid-term and historical data in the event of an audit.

Compliance requires monitoring and correlation of events at an application or database level. In rare cases where a device or application is unsupported, the enhanced GUI-based *Quick Connect* integration kit allows customers, integrators, and technology partners to easily develop and maintain new-agent collectors to incorporate device or asset information into the nFX OSP. This "wizard" style integration kit guides users through the process of new-agent development step-by-step. New agents developed using Quick Connect automatically categorize and normalize security events and automatically support existing rules. This custom integration is critical to supporting compliance initiatives by allowing organizations to easily integrate key compliance-related applications and data into the SIM infrastructure.

Correlation

The unique nFX OSP correlation capabilities support regulatory compliance in two important ways. nFX OSP applies three different types of correlation techniques to reduce false positives and detect real attacks that allow security operators and analysts to take action before compliance violations can occur. By delivering vulnerability correlation and a large library of rules out of the box, nFX OSP enables teams to build a security management infrastructure to support compliance faster. Furthermore, multi-state rules require security analysts to write and maintain fewer rules to identify threats against compliance asset groups.



Asset-Tagging capabilities use rules to assess risk against specific assets and asset groups. This is critical for regulatory compliance reporting as well as for safeguarding customer identity information, or measuring risk against key e-business assets. For example, enterprises can now create asset groups relevant to a particular regulation such as SOX, HIPAA, FISMA, or GLBA and generate specific reports to understand the vulnerability level of each asset in the group as well as the group as a whole based on correlated information from server logs, devices, and scanners.

Incident-Resolution Management Workflow

nFX OSP provides an integrated incident-resolution management workflow to help security teams apply a consistent incident-handling process that guides the team through the process of identifying and eradicating a threat. By enforcing a consistent process, nFX OSP promotes compliance by making sure that threats are fully eradicated and documenting the actions taken. Incident-management reports allow teams to “retrace” the stages of a particular incident for training and evidentiary purposes.

Compliance Reporting

nFX OSP now ships with a standard suite of operational and executive reports that address specific sections of key compliance regulations such as SOX, HIPAA, FISMA, and GLBA. Operational reports leverage risk-assessment information generated by nFX OSP’s powerful correlation and asset-valuation technology to create a timely, prioritized view of threats against compliance asset groups, as well as individual assets most pertinent to demonstrating compliance, such as a financial reporting server or patient-records database. Executive reports and dashboards show overall security posture, vulnerability, and incident management trends for compliance-related asset groups, to measure the effectiveness of compliance initiatives over time. All nFX OSP compliance reports can be customized to address the compliance policies and processes unique to an organization. Finally, incident management reports allow organizations to “retrace the steps” taken to show that an incident was managed properly in the event of an audit.

Conclusion

True compliance can be achieved only as the result of human, process, and information controls meshing to provide objective, documented proof of security. Because of an emphasis on independence and objectivity, proving the presence of effective controls is increasingly achieved through technological means. A SIM solution like that offered by netForensics is the best way to aggregate, analyze, and report the security information necessary for the compliance effort.

About netForensics

netForensics is the leading authority in Security Information Management (SIM) with more than 400 clients – including Global 1000 enterprises and government organizations operating some of the largest networks in the world. netForensics is the only SIM provider with an integrated family of enterprise-class products and services that are based on the proven, repeatable nFX information security methodology. This combination empowers security organizations to combat threats more efficiently while connecting the security organization with network operations, compliance, and risk management. With award-winning technology, netForensics improves security operations performance by extracting real-time intelligence from point security products and applications into a single data repository, flagging the most critical issues and launching integrated incident resolution and remediation processes.



nFX OSP Compliance Information

The following are regulatory control objectives that the nFX OSP assists in meeting.

Sarbanes-Oxley Act (SOX) – COSO / COBIT Guidelines

Sarbanes-Oxley Control Objective	nFX Open Security Platform Support
Determine if an audit trail exists of all emergency activity and that it is independently reviewed.	Comprehensive collection, analysis, correlation, and reporting and retention of audit events from security, networking, computing devices, and business applications
IT security administration monitors and logs security activity and identified security violations.	Security activity and identified security violations are monitored and logged
Review a sample of problem or incident reports, to consider if the issues were addressed (recorded, analyzed, and resolved) in a timely manner.	Integrated incident resolution management and knowledge base
Determine if the organization's procedures include audit trail facilities – tracking of the incidents.	Incident resolution management includes all audit trails and steps for tracking incidents
Review a sample of problems recorded on the problem-management system to consider if a proper audit trail exists and is used.	Archiving capability allows full review of incidents
System-event data are sufficiently retained to provide chronological information and logs to enable the review, examination, and reconstruction of system and data processing.	System event data archives provide chronological information and logs to enable the review, examination, and reconstruction of system and data processing
Determine if sufficient chronological information and logs are being recorded and stored and are useable for reconstruction of system if necessary. Obtain a sample of log entries, to determine if they sufficiently allow for reconstruction.	Archiving features allow reconstruction of an event from start to finish





Gramm-Leach-Bliley Act (GLBA)

GLBA Control Objective	nFX Open Security Platform Support
Assess risk that may threaten customer information.	Risk assessment based on asset value, threats, and vulnerabilities
Manage and control risk.	Correlation and monitoring of security events from applications and databases that contain customer information, as well as security devices; incident resolution workflow ensures risk mitigation.
Training	Knowledge base and archiving provide training materials and case studies for awareness and training programs.
Testing	Complete view of security events provides evidence of the adequacy of controls.
Oversight of service-provider arrangements	Monitoring capability provides ability to ensure that all third-party contracts and agreements are being met in terms of security controls.
Program Adjustments	Provides information and feedback to facilitate control and program changes for continuous security improvement, gives insight into the validity of an adjustment after it is made.
Reporting to the Board	Comprehensive compliance reporting allows for robust, tailored communication with management entities.



Federal Information Security Management Act (FISMA)

FISMA Control Objective	nFX Open Security Platform Support
Risk Assessment (RA-2)	Risk assessment based on asset value, threats, and vulnerabilities
Incidence Response (IR-1, IR-2, IR-3)	Integrated incident-resolution management and knowledge base
Intrusion Detection System and tools (IR-5)	Strong correlation of IDS events Detects common and unique attacks IDS-centric reports.
Malicious code protection (IR-6)	Detection and reporting on viruses, worms, and other malicious code
Individual Identification and Authentication (IA-1)	Strong AAA activities correlation and reporting
Monitor Change Activity (CM-7)	Detects and reports on all system status and configuration changes.
Supervision and Review (AC-12)	Detects and reports on privilege and authorization changes.
Logging and Audit controls (AU-2,3,4,5)	Comprehensive collection, correlation, analysis, reporting, and retention of audit events from key applications, security devices, network devices, servers, and desktops



Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Control Objective	nFX Open Security Platform Support
Security Management Process - 164.308(a)(1)	Risk assessment based on asset value, threats, and vulnerabilities; provides support throughout the security management lifecycle; includes incident management process.
Security Awareness and Training - 164.308(a)(5)	Log-in monitoring through central logging, protection from malicious software through IDS and event monitoring, and knowledge base for continued learning
Security Incident Procedures - 164.308(a)(6)	Integrated incident resolution management system and knowledge base
Audit Controls - 164.312(b)	Comprehensive collection, analysis, reporting, and retention of audit events from security devices, network devices, and applications; application level integration demonstrates security throughout the life cycle.