White Paper

Server

How SUSE® Manager Can Help You Achieve Regulatory Compliance

Table of Contents

page

Why You Need a Compliance Program 2

Compliance Standards: SOX, HIPAA and PCI 2

What IT Is Concerned with for Compliance 4

Ten Ways SUSE Manager Helps Organizations Comply with Regulatory Requirements 5

Summary 6

SUSE®

We adapt. You succeed.

Why You Need a Compliance Program

Compliance in a regulatory context is a growing business concern because of the ever-increasing number of regulations and widespread lack of understanding about what is required for a corporation to be in compliance with both old and new legislation.

Compliance is either a state of being in accordance with established guidelines, specifications or legislation or the process of becoming so. It often refers to behavior in accordance with legislation such as the Sarbanes-Oxley Act (SOX) of 2002, the Health Insurance Portability and Accountability Act (HIPAA)of 1996 or the Payment Card Industry (PCI) standard of 2004.

However, the number of major federal regulations is constantly rising. A 2012 U.S. Congressional hearing of the Independent Community Bankers of America cited a four-fold increase in senior executives' work time on compliance-related issues in the past three years. As business becomes more regulated, the cost of compliance continues to rise, as have the concerns and risks of non-compliance. As a result, regulatory risks can have a significant impact on corporate earnings.

Compliance in a regulatory context is a growing business concern because of the ever-increasing number of regulations and widespread lack of understanding about what is required for a corporation to be in compliance with both old and new legislation. The cost of non-compliance can be high—such as fines and imprisonment of company staff and executives. (Enron is a good example.) These penalties may result in the company going out of business or cause a costly disruption of its ability to provide products and services to its customers, making its survival questionable.

The complexity of today's regulatory environment, the impact of regulations on an organization and the penalties for non-compliance cannot be addressed without appropriate polices and technology to intelligently automate and manage the policies. Many Chief Compliance Officers (CCOs) are still trying to manage significant portions of their corporation's compliance programs without appropriate technology. What they need is support from IT. IT can provide some, but not all, of the technology required. One software product, however, that provides significant help in reducing the time and costs associated with compliance is SUSE Manager. Here's a closer look at major regulations and how IT can help organizations comply with them.

Compliance Standards: SOX, HIPAA and PCI

Three of the most common compliance standards are SOX, HIPAA and PCI. Many public U.S. corporations are required to adhere to at least one of them, depending on a corporation's the type of business. To understand how appropriate system management tools can help companies comply with regulatory requirements, it helps to summarize their requirements, and the role of IT in meeting those requirements.

SOX Regulatory Requirements

The purpose of SOX is to give investors more confidence in the financial reporting process of publicly traded companies by putting controls in place to ensure the confidentiality and integrity of financial information. SOX applies to companies that are publicly traded in the United States, but it has international applicability because many large foreign companies are also traded on U.S. stock exchanges. To be SOX-compliant, corporations must have regular external audits that assess the controls that are in place to ensure their information is accurate and provides a true representation of the corporation's financial position.

SOX was enacted in response to the Enron and WorldCom financial scandals. It protects shareholders and the general public from accounting errors and fraudulent practices in the enterprise. The Securities and Exchange Commission (SEC) administers SOX. SOX defines which corporate records are to be stored and for how long: for example, any records that affect the financial side of corporations. Anyone that knowingly destroys, alters or falsifies business records can be fined, imprisoned or both.

While SOX does not address IT directly, the implications for IT are significant, given that most financial information flows through the computer systems controlled and managed by IT. This means that IT must provide assurance that financial information cannot be altered or viewed by unauthorized individuals and is available when needed by authorized individuals. Specific IT-related SOX requirements include information confidentiality, integrity, availability, auditing and logging and change management.

HIPAA Regulatory Requirements

HIPAA established federal regulations that mandate that doctors, hospitals and other health care providers meet specific baseline standards when handling electronic protected health information (ePHI), such as medical records and medical patient accounts. The major underlying concept of HIPAA is the notion that the owners of databases are not necessarily the owners of the information contained in the databases.

HIPAA-compliant organizations must ensure that record owners are guaranteed:

- *Access to their own records and the right to request corrections of errors*
- *Prior knowledge pertaining to how their information will be used*
- *Explicit consent from the involved individuals before ePHI can be used for marketing*
- *The right to ask and expect health organizations to take reasonable steps to ensure that communications between the individual and organizations are kept private*
- *The right to file formal privacy-related complaints to the appropriate authorities*

Specific IT-related HIPAA requirements include information confidentiality, integrity, availability, auditing and logging and authentication.

PCI Regulatory Requirements

PCI is a standard based on security programs that were independently created by four separate card services: VISA, MasterCard, American Express and Discover. PCI establishes a comprehensive set of worldwide security standards for all merchants and service providers that deal with the storage, transmission or processing of cardholder information from any major card service.

To certify compliance with PCI, an audit must be completed in order to verify that the standards are adequately being met. Quarterly and annual audits for compliance are held depending on a merchant's classification. The more transactions an organization processes, the more critical it is that an organization meets the PCI standards to manage the greater risk. The idea is to protect cardholder information, implement strong access control measures and regularly monitor and test networks.

Confidentiality and authentication are the central goals of PCI—to protect consumer credit card information. Credit card information usually proceeds through several intermediary agents from the individual to the credit card company itself. Therefore, encryption as well as ensuring that only authorized systems or agents have access to sensitive account information are of paramount importance. Logging and auditing are the second most important aspects of PCI compliance.

What IT Is Concerned with for Compliance

The most important regulatory requirements of SOX, HIPAA and PCI are information confidentiality, integrity, availability, authentication, auditing and logging and change management. Some of these requirements are more important for one regulation than another, but in some way they are common to the three compliance standards and for many of the other compliance regulatory standards.

- **Confidentiality.** *Information must be kept confidential to prevent unauthorized parties from accessing it. For HIPAA this information would be ePHI, i.e., information related to a record owner's account. For SOX, this information would be various financial information records, and for PCI it would be credit card information. Encryption should be used when storing confidential information in databases or files, when transmitting this information over a network and when this information is in memory.*
- **Integrity.** *Records should not be modifiable by unauthorized people or entities. All sensitive information should use an integrity/checking mechanism to limit the risk of information tampering. Software needs to support evidence that information has not been modified.*
- **Availability.** *Systems need to be designed to properly handle errors and withstand denial of service attacks. Event logs should contain enough information to make possible to reconstruct system activity up to the point of failure so that the error can be quickly resolved and fixed.*
- **Authentication.** *Authentication involves making information available only to authorized individuals and maintaining resistance to denial of service attacks. This often requires using reliable data storage devices, failover clustering, mechanisms for encrypting keys and data recovery. To securely operate on information such as HIPAA ePHI, it is necessary to know that the entity or person that is working with the information is legitimate and authorized to access said information.*
- **Auditing and logging.** *Software systems must generate all of the necessary logging information to construct a clear audit trail that shows how a user or entity attempts to access and utilize resources. For SOX, this means tracking the key moments where information enters or exits a company: for example, emails sent outside a company or the departure of employees with access to sensitive financial information. It is important that logs are backed up regularly to ensure that auditing information is not lost due to system failure. Logs must not reveal any of the information that the system is trying to protect.*
- **Change management.** *Change management plays a role in compliance from an audit perspective as well as operationally to ensure that all changes meet established policies and the provisions for related regulations. Change management is used to ensure the integrity of systems storing regulated information, such as SOX information. SOX is concerned with change management because the information in financial records may be tampered with, thus requiring accesses to financial records be logged and the records secured. The ability to log system changes in such a manner that the logs are accessible only to authorized individuals is an important requirement for change management.*

For SOX, IT must provide the capability to store all business records, including electronic records and messages for at least five years with an emphasis on financial records and messages. Records include work papers, memoranda, correspondence, communications or other documents and records created, sent or received in connection with an audit or review and contain conclusions, opinions, analysis or financial information relating to such an audit or review.

For HIPAA, IT must provide security mechanisms to ensure confidentiality and information integrity for any information that identifies an individual and protect the confidentiality of all ePHI. The goal of PCI is to protect consumer credit card information as this information travels through various intermediaries from the consumer to the credit card company.

Ten Ways SUSE Manager Helps Organizations Comply with Regulatory Requirements

To provide for the confidentiality, integrity, availability, authentication, auditing and logging and change management mandated by compliance requirements, various system management features such as security patch management, logging, physical and virtual resource monitoring, reporting, probes, etc., are required. All of the regulations have stringent security requirements with patch management as the critical function for guaranteeing that security updates have been made in a timely manner.

SUSE Manager can help organizations comply with these regulatory requirements in, at least, ten ways:

1. Security is a significant requirement for all of the regulatory requirements. SUSE Manager uses OpenSCAP to audit software patch status, automatically confirm that servers have the latest security updates, check system-security configuration settings and examine systems for signs of compromise. Users can access a secure log created by OpenSCAP (**www.open-scap.org/page/Main_Page**) of all activities for auditing. SUSE has worked with one of its partners, UPW, to integrate a solution, UPW Compliance Guard, into SUSE Manager, making security measurable. An organization can run automated regular tests using UPW Compliance Guard and create reports to continuously track compliance as part of an ongoing effort to improve IT security.
2. Patch management (**www.suse.com/promo/automated-patch-management.html**) is important for ensuring that a regulated organization has the latest security updates. Without this assurance, an organization is in danger of not satisfying security-related regulatory requirements. With SUSE Manager, administrators can examine the patch status of individual systems or system groups and either directly apply patches needed or schedule updates to happen in a maintenance window. Patches can be tested in multiple staging areas before they are rolled out in production. The patch metadata provided by SUSE allows the administrator to assess the importance and urgency of patches. In addition to that, SUSE Manager allows for auditing the systems' software inventory based on the IDs provided by MITRE's Common Vulnerabilities and Exposures (CVE) database. SUSE Manager provides a single access point to Novell Customer Center for obtaining updates so administrators can comply with corporate firewall policies and automatically deploy critical security patches that reduce vulnerabilities and threats.
3. Confidentiality involves preventing unauthorized parties from accessing information. SUSE Manager helps provide confidentiality of information via its authentication mechanisms, logging (i.e., logging who has accessed or tried to access information) and encryption capabilities.
4. Integrity involves preventing records from being modified by unauthorized people. SOX tries to prevent unauthorized staff in a corporation from modifying financial records, and HIPAA attempts to keep unauthorized staff from modifying patient records. Some of the same SUSE Manager capabilities used for information confidentiality are also used for information integrity. Logging is important for tracing who is trying to modify information and can be used to help "catch" those who should not be modifying information.
5. Information availability is determined by the strength of overall system security and by how well systems prevent/handle errors, prevent/withstand denial of service attacks, limit system outages, etc. Much of the effort around information availability involves monitoring the health of servers, networks and other system entities, both physical and virtual. SUSE Manager probes allow organizations to monitor the health of physical and virtual servers, virtual guests, networks, etc. and prevent issues that affect availability before they occur.
6. It is one thing to prevent unauthorized accessing or modifying information, but it is also important to ensure through authentication that an entity attempting the access is who it says that it is. The role-based controls in SUSE Manager are used to ensure that administrators have the appropriate level of authority to access and/or modify information. Administrator access can be limited to individual systems or system groups as well as based on tasks. For example, one administrator may have permission to change the update channel setup for a group of systems while another administrator is permitted to actually apply patches.

7. An underlying key to satisfying several of the regulatory standards requirements is the ability to log various events such as who is trying to access/modify information, tracking where information is located as it moves around an organization (internally or remotely), etc. Logging creates an audit trail that provides visibility from an IT point of view and allows preparing reports for external regulatory auditors. SUSE Manager provides these logging and auditing capabilities and significant reporting capabilities that can be used not only for providing auditor reports, but to create internally used reports for examining the health of IT systems.
8. Change management is an often-overlooked process for satisfying compliance requirements. It logs changes that occur such as installing a new server and making changes/updates to hardware/software including security updates, etc. Change management logs are invaluable for monitoring/detecting issues that might be related to loss of confidentiality, integrity and other regulatory requirements. SUSE Manager automatically tracks server changes and keeps a history, so an organization can easily provide change information to auditors.
9. The SUSE Manager Monitoring Module gives users the capability to monitor the health of physical resources such as physical servers and memory as well as virtual servers' memory, disk space and CPU usage to proactively assure the ongoing availability of services. Monitoring benefits from the use of probes and notifications. An organization can create custom probes, use the built-in SUSE Linux Enterprise Server probes or even use third-party probes to monitor the health of physical and virtual servers. SUSE Manager notifications via email or pagers warn system administrators when servers are exceeding usage thresholds or about potential system failures before they actually occur. Server health can be conveniently monitored from one console with single page updates and graphical reports of server performance. Monitoring the health of a system and responding quickly increase system availability, one of the regulatory requirements for compliance.
10. The SUSE Manager API can be used to create custom scripts that manage tasks or work with third-party applications and management tools.

Summary

Compliance standards such as SOX, HIPAA and PCI are placing an increasing burden on organizations to meet regulatory requirements. All compliance standards include a significant number of security requirements including confidentiality, integrity, availability, authentication, auditing and logging and change management requirements.

Today, many of those in charge of compliance within organizations are seeking the help of IT because it is clear that technology is needed to achieve compliance and reduce its costs. SUSE Manager is one of only a few system management tools that provide the features needed to satisfy compliance requirements. It has technology such as patch management, authentication, resource monitoring, logging, report generation, change management auditing, etc. to address all of the regulatory requirements given above. And SUSE Manager can do all of this through a single management interface.

What's more, SUSE Manager is the only Linux system management solution built to manage both SUSE Linux Enterprise Server and Red Hat Enterprise Linux-based systems.

Contact your local SUSE Solutions Provider, or call SUSE at:

1 800 796 3700 U.S./Canada
1 801 861 4500 Worldwide

SUSE
Maxfeldstrasse 5
90409 Nuremberg
Germany

www.suse.com

262-002505-001 | 12/13 | © 2013 SUSE LLC. All rights reserved. SUSE and the SUSE logo are registered trademarks of SUSE LLC in the United States and other countries. All third-party trademarks are the property of their respective owners.