Meeting Regulatory Audit Requirements with Opmantek

E-book by

Mark Henry
Senior System Engineer

OPMANTEK

Getting Compliant:

How to Meet Regulatory Audit Requirements Using Opmantek's Products

> **...that could mean the difference between a profitable year and (potentially) huge fines or even unemployment.**

It's a spaghetti string of acronyms, SOX, SSAE, PCI-DSS, HIPPA. To the uninitiated, they seem like gibberish, to those dealing with Federal or industry regulatory requirements they can be a sea of difficult to understand and potentially impossible to apply requirements that could mean the difference between a profitable year and (potentially) huge fines or even unemployment.

Today I'd like to address each of these in detail, discuss from an IT standpoint what needs to be done to meet each, and then discuss which of Opmantek's products help address those requirements. Fear not, we're in this together, so buckle-in and make sure your helmet is snug as we dive into Regulatory Audit Requirements.

Table of Contents

Who Do These Regulations Apply to?

First off let's break down the main regulations you might run into. Depending on your country and industry your business might be affected by one or more of these in addition to other regulations not covered here.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard for organizations that handle credit cards from the major vendors (i.e. MasterCard, VISA, Discover, American Express, etc.). Simply put, if your business handles credit card information in any way – maybe through an online shopping cart or by taking cards over the phone and hand processing them – you have exposure under PCI-DSS.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is US legislation that provides data privacy and security provisions for safeguarding medical information. It's important to note that this regulation extends beyond just hospitals and doctor's offices and includes anyone who handles information related to an individual's healthcare. This would include businesses providing billing and collection services, healthcare records storage, and anything to do with the maintenance or upkeep of an individual's healthcare record (physical or electronic). If your business handles any material that includes healthcare information that could potentially identify an individual you have exposure under HIPAA.

Who Do These Regulations Apply to?

SSAE-16

The Statement on Standards and Attestation Engagements (SSAE) No. 16 (previously the SAS-70 and soon to become the SSAE-18) is an audit standard created by the American Institute of Certified Public Accountants' (AICPA). The SSAE-16 is designed to ensure a service organization has the appropriate processes and IT controls in place to assure the safety and security of their client's information and the quality of the services they perform for them. The SOC-1 exam primarily focuses on internal controls over financial reporting (ICFR) but has expanded over the years to often include testing process documentation. The SOC-2 report expands on the SOC-1 to include not only the review of processes and controls but the testing of those controls over the reporting period (generally a year). Generally speaking, if your business performs outsourced service that affects the financial statements of another company you have exposure under the SSAE-16 SOC-1 and if you're handling payroll, loan servicing, data center/co-location/network monitoring, software as a service (SaaS), or medical claims processing (including statement printing and online payment solutions) you would also have exposure under SOC-2.

SOC

The Sarbanes-Oxley Act of 2002 (SOX), also known as the "Public Company Accounting Reform and Investor Protection Act", is a US Federal law that sets requirements for all U.S. public company boards, management, and public accounting firms for financial reporting, disclosures, and records keeping. It is important to note that while the bulk of SOX focuses on public companies, there are provisions in the Act that also apply to privately held companies. Generally speaking, if you are a public company you are covered by the Act.

What Do These Regulations Mean to You?

So, once you've determined which regulations your business needs to adhere to what are the specific activities you need to take to meet those requirements?

Below is a short list of the things needed to be in place in order to demonstrate compliance with these regulations. It's important to note these are only the activities that can be monitored and recorded electronically. Each of these compliance requirements includes additional process documentation, i.e. detail a D&R plan, maintain a ledger, document on an offsite backup process and restore procedure, etc. which is not listed below.

PCI-DSS

This list focuses on small to medium-sized merchants processing credit cards, but not storing credit card data.

This list gets much longer if your company processes large numbers of credit card transactions, processes transactions over certain amounts, acts as a clearinghouse or cc processor, or stores any credit card information.

- Collect event logs from all relevant devices (firewalls, routers, and servers) within the PCI-DSS zone, or entire network if card processing is not segmented, and alert/report on "unusual" activity.
- Collect device configurations and alert/report on changes to all relevant devices (firewalls, routers, and servers) within the PCI-DSS zone, or entire network if card processing is not segmented.
- Confirm any/all DBs that store card data are encrypted at the drive or DB level; credit card data should be encrypted both at rest and while in motion.

HIPAA

- Collect event logs from all servers/workstations that store healthcare information or records and any networking equipment this information passes through, and alert/report on "unusual" activity.
- Confirm any/all DBs that healthcare data are stored on are encrypted at the drive or DB level; healthcare information should be encrypted both at rest and while in motion.

What Do These Regulations Mean to You?

SSAE-16 SOC1/2

This list covers most service provider requirements. However, companies that host or develop software would have additional requirements.

- Provide for NMS/NPM of network devices and servers, this may include processing of event logs; alert on out of performance issues; demonstrate escalation process; log all NMS/NPM setting changes for audit purposes.
- Collect device configurations; alert on unauthorized configuration changes; demonstrate escalation process.
- Ensure all servers/workstations are being patched at the OS-level and for each critical application.
- Ensure all servers/workstations are running antivirus with the most recent antivirus updates.
- Check password criteria (length, complexity, and short and long expiration); this should be managed centrally through AD/MS-LDAP.
- Check to ensure there are no local admin accounts, all guest accounts are disabled, and any local named accounts meet password requirements.
- Report on user account access, all users have limited access (<Admin) and for those that need Admin, they have both a regular account and a separate Admin account.

Sarbanes-Oxley (SOX) (SOX Section-404)

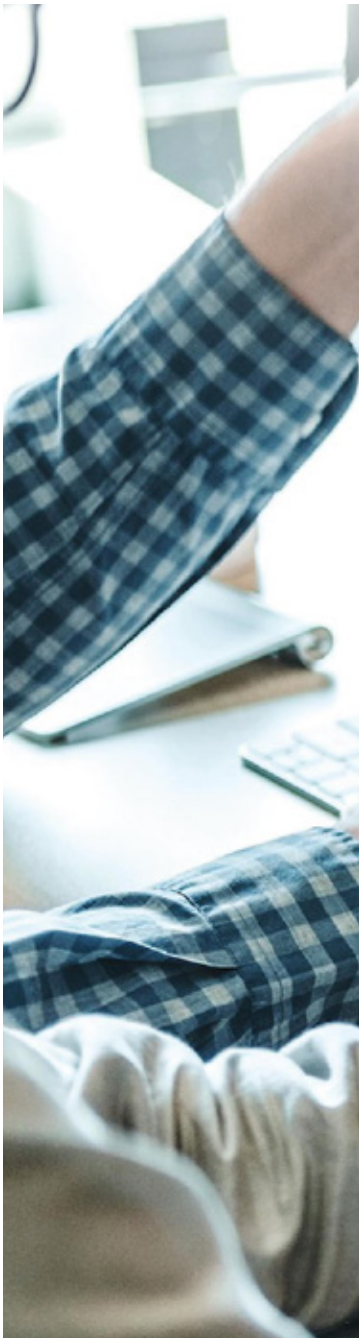
The SOX Act focuses on financial reporting and accountability, but Section-404 covers requirements from an IT perspective. Generally, the SSAE-16 SOC-2 requirements listed above will often fulfil SOX Section-404.

- Provide for NMS/NPM of network devices and servers, this may include processing of event logs; alert on out of performance issues; demonstrate escalation process; log all NMS/NPM setting changes for audit purposes.
- Collect device configurations; alert on unauthorized configuration changes; demonstrate escalation process.
- Ensure all servers/workstations are being patched at the OS-level and for each critical application.
- Ensure all servers/workstations are running antivirus with the most recent antivirus updates.
- Check password criteria (length, complexity, and short and long expiration); this should be managed centrally through AD/MS-LDAP.
- Check to ensure there are no local admin accounts, all guest accounts are disabled, and any local named accounts meet password requirements.
- Report on user account access, all users have limited access (<Admin) and for those that need Admin, they have both a regular account and a separate Admin account.

How Do You Do it?

OK, good.

So, you've made it this far and figured out which regulations apply to your company and you have a list of the activities you need to monitor. But, how do you actually do it?



List of Devices

In almost every regulation you'll need to provide a list of all your equipment – workstations and servers. This can easily be handled through Open-AudIT, which provides automated methods for discovering and auditing all the devices on your network, including reporting on local user accounts and user groups, and antivirus installs. This also includes scheduled reporting that can provide all relevant information the morning that you need it.

Topology Diagrams

You should have a detailed topology diagram available that's always up-to-date. This can be done using a combination of NMIS to gather Layer 2 and 3 connectivity information and opCharts to create the topology diagrams.

Performance and Fault Monitoring

Opmantek's NMIS can provide very robust performance and fault monitoring capabilities, as well as handle event escalation and notifications.

Syslog and Application Log Monitoring

You can expand on NMIS' Performance and Fault monitoring by adding opEvents, which can parse Syslog and application logs, generate notifications, and even perform event remediation.

Device Configuration Change Monitoring

Beyond the basic reporting of performance and fault issues comes the need to monitor devices for unauthorized or improper configuration changes. opConfig can collect device configurations, raise events for changes, and even help you centrally manage your network devices.

Next Steps

Well, here we are at the end. We've covered the main regulations, provided a list of what needs to be done, and even gone over each of Opmantek's products and how they can help you address those requirements. Where you go from here is up to you.

If you still have questions, please reach out. We're here to help you navigate these regulatory requirements by delivering solutions that make your life easier and help you sleep a more soundly.

Best,

Mark H
Charlotte, NC

About the Author

Mark Henry

Senior System Engineer

Mark Henry is a Senior System Engineer in Opmantek's North American office located in Charlotte, NC. A serial entrepreneur, Mark specializes in the ground-level, tactical application of real world processes including Agile Development, Test Driven Design, and Six-Sigma to deliver solutions that often outpace the market and his competition. Mark resides in Concord, NC with his wife Beth, their 8 children, and a dog named Jack Daniels.

Thank You

Need a Hand?

If you'd like some guidance around setup and configuration, or If there's a specific issue you're trying to solve in your network environment - click below to request a demo from an Opmantek engineer.

REQUEST A DEMO

OPMANTEK