ENTERPRISE ARCHITECTURE RESEARCH GROUP

INTELLIGENCE BRIEF

Compliance and Auditing

Q3 2019

ANDREW LOWE

Overview

Many factors influence an organization's decision to adopt compliance as a practice. Driving factors could be a law, such as GDPR or HIPAA, proof of due diligence for insurance, C-level management, unique client requirements, raising efficacy and processes not only in security but also in operations, and even marketing and/or public relations initiatives to instill confidence in clients and partners.

When auditing in a multi-framework compliance program, mapping control families to a baseline framework will significantly improve the program.

Meeting compliance requirements can be a strain on any size organization, especially if the organization does not have the correct policies and procedures in place. Knowing what the organization's mission is will help departments collaborate on compliance efforts.

Auditing is the most important part of a compliance program. A variety of compliance evidence is gathered prior to and during an audit for proof of audit and proof of adherence to controls. This evidence includes screenshots, logs, documentation, video, recordings, or testing. Audits should be performed in phases, which can be more efficient in the long term as they separate larger scopes into manageable components. During a gap analysis, an audit is conducted to discover what is missing from the chosen framework. Audits can reveal what processes should be added, improved, or even removed. While a final audit is most often completed by a third-party service (also called an external audit), internal audits can streamline the auditing process, help organizations understand where the gaps are in compliance controls, and help improve security posture.

Security products play a valuable role in auditing and compliance. The logs that many products generate are often crucial sources of data for evidence gathering during security control audits. Additionally, many regulatory compliance controls call for specific security functions to take place, including monitoring, access control, threat detection/prevention, and network segmentation for scope, which creates a perimeter for sensitive data.

This paper details the process for building a new compliance program and provides guidance on how analysts new to compliance can get up to speed on programs already in place. Common compliance frameworks and typical misconceptions about compliance are reviewed, and laws and best practices are defined.

Findings/Recommendations

- Understand that your organization will never be completely compliant.
- Proof is everything; if you tell an auditor you do something be prepared to defend that statement.
- Firewalls are preferred over routers for network segmentation, since ACLs provide more rigorous control.
- Conducting a gap analysis after implementing CIS Top 20 can speed up new compliance programs.
- The tasks that must be completed to be compliant with regulatory and guideline frameworks are very similar.
- Internal "mock audits" should be performed bi-annually at a minimum.
- Leverage tools and processes that allow you to map users to the data they access.
- Avoid redundant work by mapping multiple frameworks into a single master framework.
- Laws for regulatory compliance often justify bringing in an external auditor for gap analysis.

Contents

Compliance Terminology and Roles

Compliance and auditing can be complex; it is important for organizations to understand the difference between policy, process, and procedure (PPP) as well as the difference between security and compliance. Moreover, by correlating the regulatory and guidance frameworks used in compliance, organizations will have a better understanding of which data protection measures they must implement.

Frameworks, Laws, and Best Practices

Enterprises building or maintaining a compliance program must invest in understanding the frameworks, laws and best practices that pertain to their industry. Regulatory frameworks are enforced by law, examples include HIPAA, SOX, and GDPR. Guidance frameworks are not enforced by law, but are best practices that can be required by industry, examples include ISO27001, PCI-DSS, and NIST. Both frameworks can result in fines due to failed compliance programs.

Policy, Process, and Procedure

Defining an organization's PPP can be a challenge for someone new to compliance. However, doing so will result in simplified communication, cleaner programs, and quicker audits, since the compliance team will be less likely to misinterpret the external auditor's requests. Individuals working with audits and compliance should clearly understand these terms. The following are simple examples of the terms:

- **Policy:** A directive or law to be followed, usually static in nature and clearly defined (e.g., "Passwords must be complex.").
- **Process:** General instructions on the steps that must be taken to achieve a specific result (e.g., "Create a password that meets policy requirements.").
- **Procedure:** Specific instructions on the steps that must be taken to achieve a specific result (e.g., "Create a password that has two capital letters, two lowercase letters, two numbers, and two symbols and that is 15 characters long but no longer than 23 characters.").

Roles in Compliance

Compliance and auditing programs don't just impact the compliance team. The task of ensuring compliance is often in addition to standard tasks for IT professionals. Typically, program and asset owners are identified, but anyone may be part of a "tiger team" that gathers data and collaborates on documentation.

Compliance efforts require the participation of multiple individuals. The *CISO*, if the organization has one, will handle risk analysis, risk registry for accepted risk, and budget decisions. The *risk analyst* assists with risk analysis, user awareness, internal auditing of controls and documentation, and even vendor management and security surveys. The risk analyst may also be specialized in regulatory laws, guidelines, or privacy practices. The *internal auditor/assessor* is an employee who audits the controls (the risk analyst can assume this role). The *external auditor/assessor* is the third party or contracted auditing entity brought in to verify that the organization meets the minimum requirements of a framework and can be awarded accreditation/certification. *Legal* advisors can be included to facilitate better understanding of a regulatory framework.

Differentiating Between Law and Best Practice

It is important to understand the difference between frameworks that are laws and those that are best practice, as this can determine the urgency of a compliance effort.

Regulatory laws are put in place by governing entities (usually after a major breach or major security incident) as a result of recognition that more protection must be provided for data. Laws are enforced with fines, which makes compliance with them a top priority in most organizations. *Best practices* are typically created after individuals or organizations recognize a need and collaborate to create a framework that will better protect our data as a whole. Best practices are not legally binding, unless stated otherwise.

Figure 1 and Figure 2 outline the more common laws and best practices for compliance in the United States.

Common Frameworks for Law (US)

Law	Description
Health Insurance Portability and Accountability Act (HIPAA)	Made up of five titles that protect medical, personal, insurance, and financial data through data privacy and security standards
Sarbanes-Oxley Act (SOX)	Requires the boards of directors and management of public companies to be accountable for maintaining financial records via data retention and protection to counteract fraud
Federal Risk and Authorization Management Program (FedRAMP)	Authorization path for cloud services to provide services to US government agencies. Utilizes a subset of NIST 800-53 and FISMA.
General Data Protection Regulation (GDPR)	A European Union (EU) law created to protect the data and privacy of individuals within the EU. Sets requirements for the collection, processing, use, and destruction of data.
Gramm-Leach-Bliley Act (GLBA)	Federal law for any organization that provides loans, financial and/or insurance as a product or service. Controls how financial institutions deal with the private information of individuals.
Federal Information Security Management Act (FISMA)	Requirement for federal agencies, which requires agencies to run a security program that documents and implements controls under the E-Government Act of 2002.
Family Educational Rights and Privacy Act (FERPA)	Law applying to all educational institutes that receive funds from the Department of Education; the law dictates protection for the privacy of student records.

Figure 1 – Common Frameworks for US Law

Common Frameworks for Best Practice (US)

Law	Description
Payment Card Industry Data Security Standards (PCI-DSS)	Created to protect credit card users and companies with PoS (point of sale) systems. Any company and/or product with credit card data should go through PCI auditing. At the time of writing, three states refer to the framework in law.
System and Organization Controls (SOC)	Framework that provides organizations with the capability to report the effectiveness of their risk management programs to stakeholders, partners, future partners, and boards
National Institute of Standards and Technology (NIST)	The NIST 800 Series publications provide cybersecurity guidelines and standards. This paper will focus on 800-53 and 800-171 as they are compliance-based publications and can be utilized for mapping any framework to for simplicity.
Control Objectives for Information and Related Technologies (COBIT)	Created by the Information Security Audit and Control Association (ISACA) as a "good-practice" framework for IT management and governance. Originally created for financial industry auditors but slowly being adopted and expanded to include management and other industries.
Center for Internet Security Top 20 (CIS)	Framework that is updated utilizing known attack vectors to protect an organization's data. Good resource for an organization looking to start a compliance and security program with no regulatory needs
Information Systems Infrastructure Library (ITIL)	Framework for IS management best practices that helps set procedures, which are intended to allow for an organization's IS management to be more efficient when utilizing tools
International Organization for Standards (ISO)	ISO 27000-series are standards for information security management and security techniques. Arguably the gold standard for information security creditability

Figure 2 – Common Frameworks for US Best Practices

The Path to Compliance

Many factors contribute to the need for compliance. Most organizations are forced into the process by a legal obligation or an upcoming audit.

New to Compliance? Start with the Basics

Companies new to compliance have the advantage (and disadvantage) of starting with a clean slate. While any framework can be used as a baseline for initial planning, the Center for Internet Security (CIS) Top 20 (CIS Top 20[1]) is a good foundation. Internal "mock audits can be conducted within an organization to understand its compliance posture, and building these audits into a quarterly or bi-annual schedule will ensure the compliance program stays relevant.

Once an organization successfully adopts the CIS Top 20, it can assess which framework(s) to adopt. A gap analysis should be conducted against the new framework(s) to find out which "missing pieces" are needed to meet framework(s) requirements. While the gap analysis can be performed by internal auditors, it is best performed by an external auditor who can independently verify compliance with the chosen framework. This external view of your program will reduce the likelihood of surprises in future audits.

Auditing Short-Take

The CIS Top 20 aligns well with larger frameworks and is easy to consume. Conducting a gap analysis between the CIS Top 20 and an organization's chosen framework(s) will identify key issues that would halt awarding of accreditation, verification, or certification.

Documenting these findings will help leadership identify which processes need to be fixed and will also record a program's progression.

Mature Programs: Iterate Toward the Goal

Mature compliance programs must be maintained if they are to remain relevant; policies, processes, and procedures must be reviewed and updated where possible or even removed if they are no longer relevant.

It is not uncommon for organizations to introduce new frameworks. Mapping framework controls to a master framework can improve a program's efficiency by reducing redundant work, simplifying auditing, and enforcing policies. This can also save time during audits: the internal compliance team will know how to audit the controls and where relevant documentation is located.

[1] https://www.cisecurity.org/controls/

Three Phases of Compliance

Regardless of the maturity of your program, a phased implementation approach is recommended.

Phase 1: Documentation and Assessment

- **Documentation:** Proper documentation is the foundation of all compliance programs and includes a mission statement and an outline of current policy, process, and procedures. In this phase, enterprises conduct a gap analysis of established programs to gain insight into what is missing.
- **Data discovery:** As you decipher your organization's needs, the need to protect sensitive data will drive which regulations you are required to follow and which standards you must implement. Make every effort to discover the types of sensitive data your organization generates and utilizes.
- **eDiscovery and asset documentation:** Map out your network. The goal is to document all computing assets including cloud assets, so you can accurately define the project's scope. Questions to ask include:
    - What types of assets does the organization have?
    - Which teams can access these assets?
    - Which vendors support which operations?

Phase 2: Decision and Execution

- **Framework decision selection:** The decision framework you select will depend on the data you have analyzed. PCI-DSS is the anomaly here since it is a law rather than a framework. In some states, PCI-DSS can be referred to by law. Figure 1 lists the frameworks enforced by law and Figure 2 lists the frameworks for best practices.
- **Education:** Educate yourself on the compliance framework and regulations you will be utilizing, and educate your employees on what they should expect and what their roles will be in the compliance program.
- **Implement controls:** Utilizing guidance from the framework selected, implement the controls required.
- **External audit:** External auditors will verify your organization meets the standards and/or laws. They also will provide consulting services, such as a gap analysis. This is a crucial step in providing documentation to auditors that demonstrates you are meeting framework standards.

Phase 3: Maintain

Unlike phases one and two, there are no steps to follow in the Maintain phase; the focus is on keeping the program running. Employees will follow the documentation and processes put in place by policies and procedures. Continuous monitoring should be practiced at this point as it will allow for proper scheduling of audits of controls and will provide structure to your auditing practices in general. If a platform is needed for setting up a continuous monitoring program, the analyst can refer to the Department of Defense's Risk Management Framework (RMF)[2], which is based on NIST 800-53.

[2] https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

Example of an Audit Workflow

The following case study of a fictitious organization depicts a common workflow for audit and compliance.

The Challenge

The organization was approached by its marketing team because potential clients were inquiring as to whether a product line met certain compliance standards. With a variety of security products installed and actively managed, it was not thought to pursue regulatory compliance standards such as HIPAA, or guidelines such as PCI-DSS. Furthermore, there was no compliance personnel on staff. The highest-ranking security officer was a Director of IT.

The Solution

The organization recognized the importance of the opportunity. Several strategic changes were made; for example, a CISO was hired to lead compliance efforts and assemble a compliance team composed of two risk analysts and a director of compliance. An aggressive schedule was put into place; the organization targeted HIPAA, PCI, and SOC2 within the first year, and ISO 27001 for the following six months.

The team chose to incorporate the RMF workflow into its process. The workflow's circular path can be useful for many organizations starting out in compliance. The path includes several steps: Categorize, Select, Implement, Assess, Authorize, Monitor, Repeat. Figure 3 depicts the RMF workflow.

The organization took the following steps to meet the 12- and 18-month deadlines for becoming compliant with the four frameworks selected.

- A "master" document was built that detailed the location for all documentation, along with evidence from auditing. The compliance team followed the steps, auditing existing controls and inserting the information into the master document. In this way, they began building an evidence bin for the external auditor.
- A risk assessment and a gap analysis were performed to learn which compliance controls were missing, what data was being processed, and what the organization's risk tolerance was, along with narrowing scope to just the product.

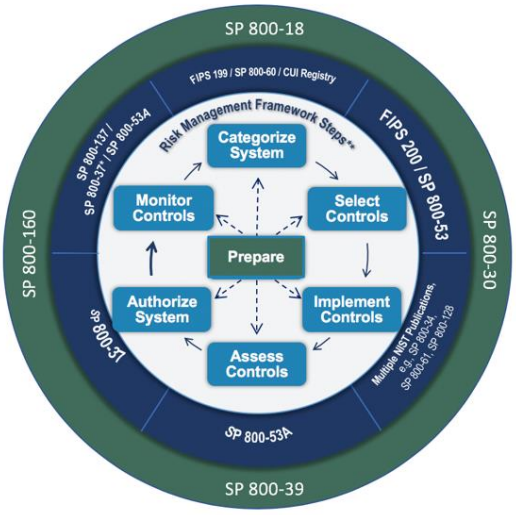

Figure 3 – DoD Risk Management Framework

- Next actions were prioritized; for example, What should be fixed?; What should be created?
- Findings were communicated with affected departments so that problem areas could be mitigated.
- Policies and procedures relevant to the framework(s) were documented. Documentation included configuration management plans, incident response plans, privacy policies, network diagrams (this is also evidence), and firewall configuration policies.
- Tools, in this case X and Y, were identified as needed and then purchased and deployed.

- At the nine-month mark, the team had enough in place to create a schedule for assessments; for example, external and internal vulnerability scans were to be performed once a month and a vulnerability management plan was instituted to fix findings within a certain amount of time according to level of severity.

Outcome

Once all assessments were conducted, policies written, controls implemented, and an internal audit conducted, the organization was ready for the external HIPAA, PCI-DSS, and SOC2 audits. After successfully passing audits, the organization used the same workflow for ISO 27001.

Because of this success, the team was more easily able to meet the requirements of the GDPR, a new regulatory standard that had been written into law during this time. The team mapped the new controls to their already established baseline and were able to repeat their process as they did for ISO 27001.

Security and Compliance

Security and compliance work hand in hand and are often mistaken to be the same as they share the goal of protecting an organization's assets. Operationally speaking, however, the two vary considerably. *Security* specifically refers to the protection of electronic data while *compliance* references efforts to meet industry and/or government standards.

Security Products: Where Security and Compliance Come Together

Security and compliance may be managed by different teams within an organization, but the goal is the same—protect the organization's data. The teams may handle the same data, but for different use cases. For example, firewall logs are utilized by security teams to track malicious activity and by compliance teams to provide evidence of due diligence for audit purposes. Firewalls can also be utilized by security teams to help compliance teams narrow scope by isolating data to a smaller "corner" in the network. The two departments can share data from different products such as firewalls, advanced endpoint protection (AEP) products, intrusion prevention systems/intrusion detection systems (IPS/IDS), and security information and event management (SIEM).

Figure 4 provides examples of security products and the frameworks they support.

Frameworks	PCI-DSS	HIPAA	SOX	FISMA	ISO27001	SOC2
Firewall	✓	✓	✓	✓	✓	
AEP	✓	✓				✓
SD-WAN	✓	✓				
IDS/IPS	✓	✓	✓	✓		
SIEM	✓	✓	✓	✓	✓	✓

Figure 4 –Security Products and the Compliance Frameworks They Assist

About the Enterprise Architecture Research Group

The mission of the Enterprise Architecture Research Group is to work with enterprises to solve security architecture and product challenges. We provide research and advisory services that are objective, accurate, reliable, and actionable. Our data comes from NSS test results, first-hand experience in the lab, novel primary research, and interaction with our enterprise clients.

Contact Information

NSS Labs, Inc.
3711 S. MoPac Expressway
Building 1, Suite 400
Austin, TX 78746-8022
USA
info@nsslabs.com
www.nsslabs.com