solarwinds

INTRODUCTION TO COMPLIANCE FOR IT PROFESSIONALS

SOLARWINDS
WHITEPAPER

INTRODUCTION TO COMPLIANCE FOR IT PROFESSIONALS

IT professionals grow and maintain an organization's IT infrastructure, ensuring that the business can operate efficiently and without interruption. So why should an IT professional be concerned about compliance? This paper is designed to help IT professionals understand and prepare for compliance because most compliance involves IT. Here we'll outline the basics of the major IT compliance schemes, provide a foundation in compliance programs, and introduce common terminology that IT staff will encounter as they engage with compliance program managers, stakeholders, and auditors.

WHAT IS COMPLIANCE?

Compliance involves the efforts and programs of an organization to ensure that the business complies with government and industry regulations. If your organization is subject to a compliance scheme, it means your business is bound, by contract or law, to follow rules set by external bodies. Unlike internally driven programs, the failure to adhere to a compliance program can have severe consequences, specifically (i) withdrawal or suspension of a business critical service; (ii) externally defined remediation programs; (iii) fines; (iv) investigation and fines or consent decrees by federal agencies; and, (v) in extreme cases, criminal liability (some compliance schemes hold individuals responsible even if they are working for a corporation).

COMPLIANCE SCHEMES

IT compliance is usually designed to remediate risk for a specific set of activities, systems, or services. Some common schemes, risks, authorities, and scopes are listed below. Within particular compliance schemes, some of the requirements may initially appear overly engineered and costly to implement. However, organizations often discover that adhering to a compliance scheme does generate ancillary benefits. Some benefits include:

- A better understanding of the IT infrastructure.
- Clearly delineated responsibilities between IT and security teams.
- Improved incident response.
- More effective utilization of existing security and IT investments.
- Reduced IT risk.
- Competitive positioning against competitors.
- Lower cyber insurance costs.

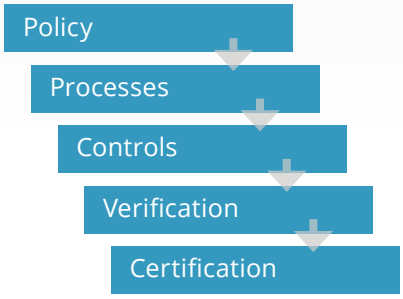
On the other hand, there are additional costs associated with implementing a compliance program, such as staff time, new solutions for processes or controls, and tools for verification. But over time, most compliance programs add value to the organization.

Which program might your organization be subject to today or in the future?

COMMON COMPLIANCE SCHEMES

Scheme	Applies to	Authority	Scope	Addresses risk
27001	Information security management	Industry	WW	Unauthorized misuse of information systems
Data Protection Directive	EU citizen data	EU Council	WW	Privacy of EU citizen data
Federal Financial Internet Examiner Council	Online and mobile banking applications	Legislature	US	Security of online banking
NIST Federal Information Security Management Act	U.S. government systems	Legislature	US	Misuse of federal systems
DISA Security Technical Implementation Guides	U.S. Department of Defense	Mandate	US	Device configuration compliance
Gramm Leach Bliley	Financial customers	Legislature	US	Privacy of financial data
Health Information Portability & Accountability Act	Health records	Statutory	US	Misuse of medical records
National Credit Union Administration	Credit unions	Administrative Law	US	Security of credit union systems and consumer funds
North America Electric Reliability Council, Critical Infrastructure Protection	Power generation	FERC	North America	Cyberattack against the power grid
Payment Card Industry (PCI)	Processors of card holder data	Industry	WW	Monetary losses due to credit card theft
Sarbanes Oxley (and similar international)	Financial systems and processes of publicly traded companies	Legislative	US+	Financial fraud in public companies

Compliance schemes all have similar components and follow a logical order of implementation:



Each of these components may be owned by a different group within the organization, however, in smaller organizations an individual or group may be responsible for more than one component.

COMPLIANCE PROGRAM STRUCTURE

Policy

Most compliance programs begin with policy. The policy is usually owned by legal or finance, or if you have a compliance officer, by the compliance or risk officer. The policy specifies the guidelines for implementing the processes and controls that form the basis of the compliance program. Policies should be technology neutral wherever possible to provide maximum flexibility to the implementers. For example, a policy might state that encryption is required for confidential document transfer and should adhere to FIPS standards, but not specify how encryption is implemented (for example, IPSEC tunnel, SSL, email level encryption, file encryption, etc.). This is because the document transfer mechanism may change from secure ftp, Web upload, email, Dropbox™, or even mobile airdrop. The individual (or group) that produces the policy is usually the responsible party for the compliance program. All compliance schemes require a responsible party, and some of them require that an officer of the company serve as the responsible party.

Processes

Most compliance schemes require the organization to initiate new processes and modify existing processes. A compliance manager or program manager should be assigned to operate this part of the compliance program. The manager needs to have the authority to affect change within the organization, and should have strong program management and people skills. The compliance scheme will usually directly specify the processes that need to be implemented or modified, or characterize the processes needed. Examples of processes are gap analysis, incident handling, threat modeling, and data handling. The process aspect of a compliance program is often the most nebulous and least proscriptively specified, therefore, if the available staff is not experienced in the scheme, training is highly recommended. Without proper training, programs can flounder at this stage.

Controls

The purpose of compliance is to reduce risk and protect the assets specified in the scheme. Identifying and implementing controls is the most visible and active part of a compliance program for IT and security teams. The scheme may proactively define specific controls, such as in PCI, or may define controls at the conceptual level, as in 27001. In either case, knowledgeable staff should be assigned to inventory current controls versus the controls needed for the scheme. Note that a technical control may be impractical to implement, and a process may be substituted as a compensating control in many schemes.

A variety of schemes rely on a standard set of IT and security controls, including (i) identification and authentication; (ii) access controls, such as firewalls (network and application), VPNs, application and database authorization; (iii) data protection (encryption and vulnerability assessment); and (iv) monitoring, alerting, and reporting (log management, SIEM).

Verification and monitoring

The verification and ongoing monitoring function provides oversight on the implementation. Verification is often a combination of manual checklists as well as IT controls. In fact, the log management/SIEM tool can also be leveraged for verification and monitoring. At this stage, processes such as business continuity testing, change control, and vulnerability assessment, are validated. This does not mean the staff performing the verification function actually implements the processes, but this role is responsible for ensuring that the processes have been tested per the policy. It is important that this role operates independently of the teams that implement the processes and controls, but care should be taken to avoid becoming adversarial to the business. Compliance helps the organization reduce risk, and the verification process can uncover gaps, but ultimately it is the compliance owner that is accountable for signoff on the compliance program.

The verification step also ensures that evidence is produced demonstrating the effective implementation of policies, procedures, and controls. It is essential that evidence be collected in a consistent and comprehensible fashion for all elements of a program, as this documentation is necessary for certification.

Certification

Once the organization is confident it has implemented a good program, certification is the step that allows you to claim you are in compliance. Some schemes allow for self-certification, but most require an external audit conducted by a knowledgeable or licensed auditor. 27001, FFIEC, PCI, NERC CIP, and NCUA, for example, all require auditing by trained examiners. Government agencies are audited against FISMA by the Office of Inspector General. Allow adequate time for preparation, and schedule internal resources early when you are planning an audit. If you haven't been through a certification or audit process before, ask around your industry and discuss the

process with someone who has been through it before. Sometimes the examiners will provide you with guidance on the process as well, but their perspective is not the same as yours.

Keep in mind that auditor's reports can contain highly sensitive data. The organization may be asked to provide copies of these reports to customers or prospects for their own compliance evidence, or as part of the sales process. Therefore, it is always a good idea to request an executive summary as part of your audit report. Ordinarily, a copy of the certification should be sufficient evidence for a 3rd-party, but where it is not, the executive summary offers a good compromise by providing additional assurance to the requestor, without sharing highly sensitive data.

Compliance programs, properly positioned and managed, can be a benefit to the organization by:

- Reducing business risk.
- Providing a competitive differentiator.
- Improving internal processes.

However, there are some pitfalls to avoid. Here are some common ones:

1. Failing to obtain buy-in from all stakeholders.
2. Including too many systems or processes in the initial scope.
3. Not designing in evidence gathering from the start (to support certification).
4. Under-communicating with IT and security teams.
5. Ignoring a regulator/auditor.

Unlike internal IT programs, where the risk is controlled by the organization, compliance programs carry external risk, whether contractual or regulatory. Here are some examples of cases where companies have failed to meet their compliance requirements:

- $3,300,000 for unsecured electronic health records (OCR) .
- $300,000 for failing to follow banking regulations (FinCEN) .
- $25,000,000 for data breaches (FCC) .

Fines are only one negative consequence of improperly managed programs. Reputational damage, lost customers, and decreased morale are others. However, if starting a compliance program appears overwhelming, keep in mind that there are many vendors willing to offer services to assist. But if you can't complete the following checklist with confidence, the organization is probably not fully prepared for the effort involved. Even if you engage a 3rd-party expert for assistance, without good answers to the checklist, the level of effort and expenditure can be more significant than expected.

GETTING STARTED

Answering the following questions will help you get started:

1. What compliance scheme applies to your organization?
2. Who will be the designated compliance owner or responsible party?
3. Who will run the day-to-day aspects of the compliance program?
4. Is there an existing program management or change management function you can leverage?
5. Who are the business stakeholders that need program updates?
6. What is your conflict resolution process if business needs and compliance are not completely aligned?
7. Do you have an inventory of current processes?
8. Can IT/security provide a list of existing controls?
9. What verification and monitoring options are currently available?
10. Are there any certification or reporting deadlines?

With the answers to these questions in hand, you can help effectively and efficiently guide your organization through compliance. As with many aspects of IT, though, compliance is a process, not a one-time initiative. Be prepared to make changes and corrections as the organization grows or the compliance scheme changes.

As Will Rogers said, "Even if you're on the right track, you'll get run over if you just sit there."

SOLARWINDS LOG & EVENT MANAGER

SolarWinds Log & Event Manager is an affordable, award-winning SIEM solution that produces out-of-the-box compliance reports for HIPAA, PCI-DSS, SOX, ISO, FISMA, FERPA, GLBA, NERC-CIP, GPG 13, and many others. Log & Event Manager can be installed in minutes and makes it easy to generate compliance reports quickly using hundreds of audit-proven templates.

NEXT STEPS

1. Watch this Continuous Compliance with SolarWinds Log & Event Manager video that discusses the various compliance requirements, including PCI, HIPAA, SOX, FISMA, DISA STIGs and more, the ramifications of not being compliant, and how SolarWinds Log & Event Manager can help in your security and compliance efforts.
2. Try SolarWinds Log & Event Manager for yourself. Download a free 30-day trial have it up and running in less than an hour.

Log & Event Manager is the fastest and easiest way to compliance reporting.

ABOUT SOLARWINDS

SolarWinds provides powerful and affordable hybrid IT infrastructure management software to customers worldwide from Fortune 500® enterprises to small businesses, government agencies and educational institutions. We are committed to focusing exclusively on IT Pros, and strive to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. Regardless of where the IT asset or user sits, SolarWinds delivers products that are easy to find, buy, use, maintain, and scale while providing the power to address all key areas of the infrastructure from on premises to the Cloud. Our solutions are rooted in our deep connection to our user base, which interacts in our thwack® online community to solve problems, share technology and best practices, and directly participate in our product development process. Learn more today at http://www.SolarWinds.com/.

---

1 http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/new-york-and-Presbyterian-hospital/index.html

2 https://www.fincen.gov/news_room/nr/pdf/20141125.pdf

3 https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf