Demystifying Compliance

Compliance Myths, Mandates and Considerations

EXECUTIVE BRIEF

splunk>

IT organizations today often struggle to satisfy compliance mandates—whether they are based on external requirements, internal policies or both. Inconsistent interpretations by different auditors and regulators have contributed to the problem and created situations where what worked in one year's audit could fail in the next. Meanwhile, escalating enforcement, greater penalties and a higher standard for "duty of care" are creating a new urgency within IT organizations to meet and maintain compliance.

While many vendors that provide enterprise services claim that they meet compliance requirements, these solutions are often only partially compliant. To compound the problem, organizations rarely understand how IT systems relate to compliance. Quick fix IT "compliance packages" that claim to be a total compliance solution for a given regulation are many times just a group of additional reports written by vendors that are rarely complete and difficult to customize. Even with a variety of solutions in place IT organizations often operate in reactive mode, shouldering the cost of responding to multiple requests for new reports, access to new data sources and specific investigations.

There are many pitfalls to avoid and best practices to consider when moving an IT organization to a compliance focus. In the end, the best compliance solution in the face of an audit or negligence lawsuit is to demonstrate an understanding of the spirit of the mandates that apply to your organization.

What is Compliance?

Compliance is the process of adhering to all of the standards, policies and regulations (both internal and external) that apply to a given organization in an effort to create public trust. Part of the reason nearly all business activities seem to have a compliance angle is that a compliant organization is simply doing the things it does in the normal course of its business in specific, dictated ways. Compliance is simply playing by the rules.

Being compliance is not simply about adhering to external laws and regulations. Many compliance mandates come from internal policies developed to control identified risks. For example, there may be policies about application management, data lifecycle management and many other management activities—all developed to control the risk that critical applications will fail or other issues will occur and therefore threaten revenue.

Every business process in a mature organization should be viewed with compliance in mind. Many times it is a business process that no one has considered that creates a compliance policy violation. For example, IT departments often discover that the need to lock down access to data sources and systems is the hidden issue that fails to meet auditor demands. Moreover, it is often these formerly undiscovered issues that have a serious impact on the ability to respond to real IT incidents, problems and failures.

Next let's uncover some of the myths about compliance.

Top Five Compliance Myths

Myth #1: Compliance equals regulations with specific actions.

Reality: Most regulations contain incomplete or little detail about how to achieve compliance with an actual IT implementation (one notable exception being PCI). And many compliance demands arise from internal assessments of risk of business disruption or litigation. You need to engineer for compliance just as you engineer for availability.

Myth #2: Compliance is an IT security issue.

Reality: A lot of compliance mandates have a security dimension because they are trying put in place controls to limit the risk of things like data information leakage and breaches due to insider threats or sabotage. Yet just as many mandates are concerned with the integrity and availability of mission-critical applications, and so preventing, detecting and responding to ordinary failures matters just as much. And beyond that, there are a lot of mandates that govern business issues such as use of insider information, which may be outside the realm of IT, although IT systems play a role in recording the evidence.

Myth #3: I have to store my original logs for seven years.

Reality: Although PCI spells out specific retention times for log data for systems in-scope for PCI audit, almost no other mandates, and certainly not the most common ones concerning IT departments, specify log retention times. Log retention times are driven by assessments of what it will take to service other requirements such as the need to investigate incidents, detect long-term patterns and prosecute intruders. You may want to keep a seven-year record but you may choose different strategies for saving more recent data vs. archived data.

Myth #4: A specific set of reports will make me compliant.

Reality: See Myth #1. The regulations almost never list a specific report. There are reports that can clearly assist with particular requirements, such as the need to review failed logins, but they require a lot of fine-tuning for each unique environment. At best, a set of standard reports is a starting place. The dirty secret: most compliance report packs are developed by product managers reading the regulations and taking a guess at what reports might be helpful. The most recent auditing trend to ask an IT representative to demonstrate an ad-hoc query in response to an auditor request or requirement.

Myth #5: I need to buy a commercial solution to be compliant.

Reality: Your decision to buy a log management system rather than roll your own logging infrastructure should be based on ROI. A well-designed system should save you on initial development and integration as well as make ongoing log reporting, ad-hoc analysis and alerting more efficient across multiple regulatory compliances. But the regulations don't say you have to buy a commercial log management system or a security information and event management system (SIEM) system, and the vendors of these systems don't have any special insight into what it takes to make you compliant.

Why IT and the Business Care about Compliance

Compliance has always been a factor in large organizations, but until recently it's been a fairly minimal investment for most organizations. However, it's now a priority for IT organizations because of several independent trends:

- The perceived threat of electronic sabotage to critical infrastructure including banking, communications, and utilities
- The wave of accounting scandals that have exposed a lack of internal controls
- Many well-publicized incidents involving the theft of personal financial and health information.
- The continued expansion of IT into every aspect of corporate, public and private life
- What's Driving Compliance?

New legislation and regulations have real teeth. Organizations that don't comply with PCI are not allowed to process credit card transactions through VISA. Any HIPAA violation will result in a large fine from the Department of Health and Human Services Office of Civil Rights. Federal agencies are now allowed to keep dollars collected as fines from businesses to fund additional audits. Companies have been delisted as a result of failing to pass SOX audits. If SOX compliance problems are detected after a company's corporate officers and board have signed off on financial statements, they could face criminal prosecution.

But even beyond the clearly defined penalties, there is an even bigger threat. Companies are getting hit with lawsuits charging negligence when their IT practices contribute to financial losses.

For example, if there is no proxy server ensuring that employees don't browse inappropriate material, a company may be sued for civil damages if an employee claims there was a hostile work environment. If there is lax security on databases containing consumer financial information, a company may be sued for damages associated with identity theft losses.

The Best Way to Prove Compliance

The best way to prove compliance is to show that your company has adopted and follows its own internal corporate best practices security policies and any other written processes mandates (first) in addition to any specific regulatory requirements within your industry or business vertical. This internal documentation should exist across IT and should be designed to minimize this risk.

The Illusion of Best Practices

In an audit, telling the auditor that your company utilizes best practices will not help you pass an audit. First, best practices cant' be quantified and as such are in the eye of the beholder. Second, there are plenty of companies that insist they follow "best practices" that have had a data breach. Finally, any "best practice" can be ignored by the business for business reasons provided the risk of not following a best practice is justified and documented to an auditor's satisfaction. That said, there are plenty common practices when it comes to security like having the necessary security architecture or not configuring a firewall to allow all traffic. Talk to other companies that do what you do through information channels, share the types of activities you perform to mitigate risk and adopt ideas if they are right for you. But, don't expect doing what everyone else does to help you pass an audit. If you're not doing the things your best-run competitors are doing, you're open to the charge that you have not met reasonable standards for "duty of care."

Why Compliance is Painful

Perhaps the most painful aspect of compliance is the fact that it is based on interpretation and interpretations are inconsistent. Compliance is an ongoing process, not a one-time event. The auditors usually get stricter in second-year audits on any new mandate. Deficiencies identified in the first audit usually have to be fixed in the next.

And your business and IT environment is changing all the time —these changes often drive changes in the requirements to meet a given compliance mandate. You'll be in the best position to deal with this inevitable change if you continuously monitor processes, people, and technology and adherence to internal and external mandates policies and thoroughly understand how they the spirit of the mandates that affect your organization.

What Compliance Means for IT

There is no doubt that compliance places a significant new burden on IT. New and growing requirements include:

- Provide reporting on IT data as proof-of-compliance controls
- Protect IT data against unauthorized viewing, modification or deletion and provide audit trails
- Day-to-day review of systems to compare behavior versus policy
- Monitor network devices, servers, applications and transactions for operational and security risks for business resilience
- Perform root-cause investigations
- Service electronic discovery requests by law enforcement
- Conduct HR investigations of employee activity
- Enable ad-hoc access to IT data by compliance personnel
- Proof that audit data has integrity

Compliance means access to IT data from applications, servers, network devices, physical security systems—anything that might be used in data center operations in the datacenter. Security analysts, IT operations, human resources, compliance and audit officers and security, risk and financial officers all need secure access to IT data.

Recipes for Interpretation

For any mandate, you should be sure that you understand its motivation and origin. Once you understand its motivation, your best recipe for success is to make that motivation your own. Educate your organization on what the mandate is designed to do.

Create a climate in your organization where the mandates goals are also your goals. When the auditors and courts see that you have adopted the spirit and not just the letter of the law, deficiencies are treated with lenience as anomalies. Some mandates, including HIPAA and FFIEC, are pretty specific about the requirement to conduct an individualized risk assessment for a given organization relative to the mandate's objectives, and based on that risk assessment adopt a customized set of controls.

As we've seen with recent prosecutions of corporate malfeasance, it's those individuals and organizations that take a cavalier attitude toward the law that are receiving the largest penalties and the biggest 'black eye' in the media.

One or more of these concerns motivates nearly every mandate you will face. You can gain leverage in a compliance program by adopting a consistent set of practices for multiple mandates sharing common goals.

Once you understand each mandate, you can identify specific controls using log data, which usually will fit into one of the following categories:

- Monitoring logs for security and operations issues
- Reporting on other controls using log data
- Ad-hoc search of log data for investigations and discovery requests

The following list takes this framework and applies it to each of the major compliance mandate categories.

1. Protect customer/consumer/employee privacy

This is the motivator behind the security and privacy rules within the Health Information Portability and Accountability Act (HIPAA) that impacts all healthcare providers and payers, which include companies who self-insure. The Gramm-Leach-Bliley Act, (GLBA), has a similar concern but with consumer financial information. California's SB-1386 is becoming a model for other states of a particularly aggressive form of privacy protection. And last but not least, the Payment Card Industry security standard (PCI), enforced by the credit card networks for any organization accepting payments by credit card, is an extremely specific program designed to protect consumer financial information.

If you are facing a regulation (or litigation risk) motivated by consumer privacy concerns, the primary risk you need to control for is information leakage. You will be restricting access to production servers that store or transmit sensitive consumer information. You will be concerned with all employee connections to the corporate network, encrypting and protecting information transmitted on the network, accessible via applications, and stored in the file systems and in databases. You will want to carefully audit the inventory the servers to maintain an up-to-date list of, applications, databases, directories, network domains, firewalls, IDS and other infrastructure that are involved in transmitting, storing, protecting or providing access to the class of data. You'll also be expected to know where your most sensitive data is located in the IT infrastructure protecting or providing access to the class of data the mandate is designed to protect.

According to a recent report form AT&T, 74% of smart-phone users access their employer's corporate network at least once a day. If your organization allows this, you should expect an auditor to want to see a risk mitigation strategy and policy that deals with data loss thought this vector. This inventory will define the scope of the compliance program.

2. Control risk in regulated critical industries

This is the motivator behind the Federal Financial Institutions Examination Council (FFIEC) guidelines used by all five U.S. banking regulators (FDIC, OTS, FRB, OCC and NCUA) for their audits of banks, savings and loans, and other retail banking institutions. These guidelines are meant to ensure that banks don't fail. Part of FFIEC is about business compliance, such as rules about reserve to deposit ratios. And part is about IT—to control the risk that sloppy security enables intruders to steal enough from the bank to threaten its viability, and also the risk that poor systems development and management practices leave the bank open to systems failures that could disrupt business operations.

Similarly, the North American Electric Reliability Council (NERC) IT guidelines are intended to control the risk that IT failures and security breaches could cause portions of the power grid to fail.

For this type of mandate, the primary concern is business continuity and resilience. The relevant IT controls will include both systems and security management practices. The systems management practices will be concerned with availability; and the security management practices will be concerned with sabotage. An undetected logic flaw in an application will be as much of a problem as a hacker determined to take your bank or power station down. Privacy issues matter to the extent that violation of other mandates regarding privacy would expose the organization to liability that might threaten its viability.

3. Ensure fairness in financial markets

This is the motivation for Sarbanes-Oxley (SOX). The scope of concern relative to IT is the prevention and detection of financial reporting inaccuracies, fraud, and revenue-generating service interruptions. IT auditors are equally concerned with security and operations. Concerns range from an authorized user of a business system abusing their privilege in order to execute fraudulent transactions, to downtime of a revenue-generating system causing lost revenue. Data integrity and business continuity are of significant concern, while privacy and secrecy are not relevant.

The scope of systems affected will vary widely depending on the nature of a particular business. For an organization with work that doesn't have any sort of transactional component, such as an advertising agency, the scope of IT infrastructure may be very narrowly defined as a handful of servers hosting the core G/L, A/R and payroll financial systems. For an e-commerce site, the entire production application infrastructure, with the minor exception of a few image servers, might be part of the audit scope.

Similarly, the opportunities for financial reporting problems and fraud will vary widely depending on an organization's specific business processes, even within the same industry. Any vendor looking to sell a SOX log monitoring bundle or reporting bundle should be regarded with extreme suspicion.

4. Protect government classified information

This is the motivation behind NISPOM (National Industrial Security Program Operating Manual), which applies to classified information protection by government agencies and contractors; DCID 6/3 (Director of Central Intelligence Directive 6/3), which applies to intelligence data handled by government agencies and contractors, and FISMA (Federal Information Security Management Act), which is a mandated security program for federal agencies.

Note that mandates motivated by protection of government information have similar characteristics to those concerned with consumer privacy-data leakage and secrecy.

5. Avoid liability due to employee misbehavior

Your compliance program may be motivated by the risk of liability for employee misbehavior. If your employees offend others in the workplace by what they see, abuse business systems to commit criminal acts, or otherwise misbehave, your organization might be considered liable unless you can show that you are taking reasonable measures to protect against such abuse.

6. Service discovery requests by law enforcement

Consumer services providers such as telecoms, ISPs, email providers and online community/gaming sites are subject to frequent e-discovery requests by law enforcement looking to discover the identity of users or understand their Internet usage. Firms employing traders or brokers subject to stringent codes of conduct receive e-discovery requests for regulator investigations of violations such as insider trading. In these cases, the primary log compliance concern is being able to quickly search for log events for particular users and showing the integrity of the audit trail.

Compliance Solution Challenges

IT organizations face many new challenges meeting the requirements for compliance regulations and mandates. IT infrastructures are far more scrutinized for compliance than ever before. They're also far more complicated. Delivering a single service or application can require hundreds or thousands of components. Working with the massive amount of unstructured data generated across thousands of components can be incredibly difficult.

Key new challenges include:

- Securely collecting, transporting and managing large amounts of IT data.
- Ensuring better IT data quality to identify the who, what, when, where, why for every piece of data.
- Robust data correlation.
- Secure, efficient IT data retention.
- Understanding what's normal and what's abnormal behavior
- Providing for alerting, reporting and ad-hoc access to all IT data across heterogeneous formats and sources
- Ensuring integrity and chain-of-evidence and a complete audit trail of data collection, management and access

Compliance and Splunk®

Powerful reporting and controls

Splunk is the engine for machine data™ It collects, indexes and harnesses machine data across an organization's infrastructure in real time. Generate reports in seconds while at the same time meet requirements to collect and retain specific audit trails with Splunk. Splunk's ability to also do both security and change monitoring satisfies requirements to meet these controls. It even allows developers to safely access production data, without distracting operations teams or causing compliance violations or exceptions.

E-Discovery, FFIEC, FISMA, HIPAA, IT Governance, PCI, SOX and other mandates require regular review of logs and IT data. But most solutions only work with a small number of data sources, require constant maintenance and are too rigid to be used for other custom applications. Splunk gives organizations the ability to achieve sustainable compliance and leverages the same investment for other IT use cases (e.g., security, application management, change management, operations management, and more).

- E-Discovery - Search every data source required for E-Discovery from one place. Get instantaneous results across large data sets.
- FISMA - Securely collect, index and store all your log and Machine Data along with audit trails to meet NIST requirements.
- HIPAA - Search all your machine data to instantly assess reports of EPHI leakage and meet HIPAA's explicit log requirements.
- PCI - Rapid compliance with explicit PCI requirements for log retention/review and change monitoring, comprehensive reporting on all PCI controls such as passwords and firewall policy.
- SOX - Splunk makes the ambiguous chore of compliance-mandated routine log review easy and straightforward.

Use Splunk to meet requirements for log review, audit trail collection, reporting and file integrity monitoring. You will empower operations staff and developers too, through access to production data logs without logging into production systems.

Free Download

Download Splunk for free. You'll get a Splunk Enterprise license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

250 Brannan St, San Francisco, CA, 94107 info@splunk.com | sales@splunk.com 866-438-7758 | 415-848-8400 www.splunkbase.com