

# Demystifying Compliance

Compliance is high on the IT agenda. What does it involve?

## Compliance on the IT Agenda

Compliance is high on the IT agenda today, yet no one seems to have a clear picture of what it really involves. Inconsistent interpretation by different auditors and regulators means what worked in one year's audit is failing in the next. Escalating enforcement and penalties and a higher standard for "duty of care" have organizations scrambling for answers and solutions.

Vendors of everything from access control to email are claiming they address compliance requirements. But most companies have a limited notion of exactly how IT systems relate to compliance. Glib claims of "compliance packages" that are supposed to be total solutions for one or another regulation sell the idea that all you have to do is plug them in and you'll be compliant.

Companies or organizations who bought these packages are often finding out their auditors are still not happy. Even with a variety of solutions in place, IT remains in reactive mode, shouldering the cost of responding to multiple requests for new reports, access to new data sources, and specific investigations.

IT is also finding that the need to lock down access to data sources and systems is the hidden enemy of meeting auditor's demands and can have a serious impact on the ability to respond to real IT incidents, problems and failures.

We're not going to tell you that just plugging a product in and turning on a few canned reports will make you compliant. Instead, we'd like to demystify compliance as it relates to IT and give you some simple recipes for analyzing your own environment in the light of specific mandates.

In the end, your 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.

We'll start by smashing some of the myths about compliance.

## Top Five Compliance Myths

### Myth #1: Compliance equals regulations with specific actions

**The reality:** Most regulations have fuzzy or no detail about IT implementation. 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.

**The reality:** Sure, a lot of compliance mandates have a security dimension because they are trying to control the risk of things like information leakage and sabotage. But 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 are really 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 7 years.

**The reality:** Where does it say that? Almost no 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 7 years available, but you may choose different strategies for more recent vs archived data.

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

**The 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 kinds of reports might be helpful.

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

**The 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/integration as well as make ongoing log reporting, ad hoc analysis and alerting more efficient. But the regulations don't say you have to buy a commercial system, and the vendors of these systems don't have any special insight into what it takes to make you compliant.

So if these are myths, what's the truth?

## What is Compliance?

Compliance is the process of adhering to all of the standards, policies and regulations that apply to a given organization. Part of the reason everything seems to have a compliance angle is that the

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.

Not all compliance is with external laws and regulations. Many compliance mandates are internal policies developed to control internally identified risks. For example, there may be policies about application management developed to control the risk that critical applications will fail and therefore threaten revenues.

Every business process in a mature organization has a compliance dimension. The only compliance-specific process is documenting compliance.

## Why IT Cares About Compliance

Compliance has always been a factor in large organizations, but it's been fairly shallow till recently, especially in its impact on IT. It's now high on the IT agenda 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.

Compliance matters to IT because everything depends on IT.

## What's Driving Compliance?

New legislation and regulations have real teeth. If you don't comply with PCI, VISA won't let you process credit card transactions. If you have a HIPAA violation you'll be fined big money by the Department of Health and Human Services. If you don't pass SOX audits, you're not going to be able to stay listed as a public company. If SOX compliance problems are detected after your corporate officers and board have signed off on financial statements, they could be prosecuted in the criminal courts.

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 only way to fight this is to show that the company has adopted and follows best practices across IT that are designed to minimize this risk. 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 thoroughly understand the spirit of the mandates that affect your organization, and can therefore anticipate what auditors and courts will think about the quality of your compliance program.

## 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 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 risks
  - 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
- growing IT requirements include:

Compliance means access to IT data from applications, servers, network devices – anything in the data center. 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.

Nearly every mandate you will face is motivated by one or more of these concerns. 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 & discovery requests

Now, let’s take this framework and apply it to each of the major categories of compliance mandates.

## 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 includes 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.

### Typical IT requirements for privacy protection

<b>Monitoring</b>	Monitor for network intrusions, suspicious outgoing traffic.
<b>Reporting</b>	Report on access control, firewall events to prove these controls are in place and properly configured.

<b>Ad hoc Search</b>	Be able to investigate logs of access to data via applications, database queries, filesystem access.  You may have to investigate any and all consumer reports that they believe your organization mismanaged their data – which may involve hundreds of ad hoc searches a week if you’re a major consumer financial or healthcare organizations.
----------------------	---

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 restrict access to production servers that store or transmit sensitive consumer information. You will be concerned with encrypting and protecting information transmitted on the network, accessible via applications, and stored in the filesystem and in databases. You will want to carefully inventory the servers, applications, databases, network domains, firewalls, IDS and other infrastructure that are involved in transmitting, storing, protecting or providing access to the class of data the mandate is designed to protect. 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.

### Typical IT requirements for critical infrastructure protection

<b>Monitoring</b>	Monitor for network intrusions, system failures, unauthorized changes.
<b>Reporting</b>	Report on the activity of access control systems and firewalls to show that these controls are in place.
<b>Ad hoc Search</b>	Enable rapid investigation of all operations and security alerts.

For this type of mandate, the primary concern is business continuity. 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. 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.

#### Typical IT requirements for financial reporting mandates

<b>Monitoring</b>	Monitor for suspicious transaction patterns, data changes that bypass application logic, and system failures.
<b>Reporting</b>	Report and review on new kinds of events, system changes, and data changes.
<b>Ad hoc Search</b>	Ensure that developers can do ad hoc search of logs without accessing production systems, as strict access controls will be in place.

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 Sarbanes-Oxley 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.

Mandates motivated by protection of government information have similar characteristics to those concerned with consumer privacy – data leakage and secrecy are the primary concerns.

#### Typical IT requirements for classified information protection

<b>Monitoring</b>	Monitor for network intrusions, suspicious outgoing traffic.
<b>Reporting</b>	Report on access control, firewall events to prove these controls are in place and properly configured.
<b>Ad hoc Search</b>	Be able to investigate logs of access to data via applications, database queries, filesystem access.  You will be expected to thoroughly investigate all network intrusion and firewall alerts as well as reports of lost data.

### 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.

#### Typical IT requirements for employee policy management

<b>Monitoring</b>	Monitor for use of inappropriate / non-business websites, unusual bandwidth usage patterns, suspicious external destination domains.
<b>Reporting</b>	Report on web proxy, email and firewall traffic.
<b>Ad hoc Search</b>	Be able to search proxy and email logs by user id on an ad hoc basis, often by non-technical HR personnel.

## 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.

### Typical IT requirements for e-discovery support

Monitoring	None
Reporting	None
Ad hoc Search	Easy search by userids, email addresses, IP addresses, etc., often by non-technical compliance personnel.

## 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 IT 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.
- 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.

## Get Started Today !

- Download your own free copy of Splunk today at [www.splunk.com/download](http://www.splunk.com/download).
- Visit [www.splunk.com/compliance](http://www.splunk.com/compliance) for more information on using Splunk IT Search to power your compliance requirements.