



Achieving IT Compliance with a Minimum of Cost and Disruption

A Practical Strategy

Executive summary

IT leaders are under pressure to bring their department's operations into compliance with a variety of regulatory mandates, such as Sarbanes-Oxley, HIPAA and Basel II. This pressure is the result of the central importance that IT has assumed in the day-to-day operations of every business in every market - as well as the increasingly diverse threats that can jeopardize a business by compromising corporate data and systems.

There is no single "magic bullet" that can enable a company to achieve compliance. Compliance requires implementation of a set of technologies and ongoing best practices appropriate to each organization's needs. These implementations can require the IT department to allocate its limited resources either excessively or exclusively to compliance unless a more leveraged play is used. In fact, investments in compliance can actually benefit IT in a multiplicity of other ways - including improved security, better service management, enhanced change management and higher overall operational efficiency.

Compliance requires an IT organization both to fulfill a set of requirements mandated by government, trade or internal corporate authorities and to be able to prove that those requirements are being consistently realized. Compliance thus challenges IT to become more disciplined in both its operational processes and the way it audits those processes.

Achieving compliance would be difficult enough by itself. However, the task is made even more challenging by the fact that IT has plenty on its plate already. It has to support existing business services, provision new ones and plan for the future - all within tight financial and human resource constraints. So the challenge for IT isn't just to achieve compliance. It's to achieve and maintain compliance over time as resource-efficiently as possible without disrupting other critical IT activities.

This paper offers a practical strategy for achieving IT compliance with minimal incremental resources or disruption to core IT activities. Essentially, this strategy is based on leveraging technologies and processes that support other IT objectives - most notably service management and security - to enable compliance. By adopting this integrated approach to compliance-enablement, IT organizations can fully leverage their investments in people and tools to fulfill multiple operational objectives. This approach also helps maintain compliance over time, since it reduces the number of management systems that have to be modified to accommodate the inevitable changes that occur over time in the IT environment.

What is IT compliance?

As information technology has come to play an increasingly critical role in day-to-day business operations, government regulators and industry associations – as well as corporate executives themselves – have had to take measures to protect the interests of customers, shareholders, employees, markets and other constituencies from a variety of IT-related risks. These risks include fraud, unintentional error, business interruption and violations of personal privacy. By setting standards and enforcing compliance, these regulators and authorities reduce the exposure of their constituencies to risk and facilitate the healthy, trustworthy economic activity of open markets.

Regulations typically require an IT organization to:

- **do** things in a repeatable fashion
- **prove** that it can do them
- **document** what it has done
- **maintain** these abilities over time

Compliance with a privacy protection mandate, for example, requires more than just avoiding an incident of information theft. It requires the implementation of best-practice processes for information security and articulating those processes to regulators. This can be done by providing audit logs and any other reports necessary to validate the effectiveness of those processes, and diligently managing those processes so that they are appropriately modified as necessary to accommodate changes in the IT environment, the business and the threat matrix.

Regulatory mandates typically don't specify exactly how an organization must achieve compliance. Instead, they outline a set of high-level requirements. For example, the Payment Card Industry (PCI) Data Security Standard has several requirements as noted below:

- **Build and Maintain a Secure Network**
 - Install and maintain a firewall configuration
 - Do not use vendor-supplied defaults
- **Protect Cardholder Data**
 - Protect Stored Data
 - Encrypt transmission of cardholder data
- **Maintain a Vulnerability Management Program**
 - Use and regularly update anti-virus software
 - Develop and maintain secure systems
- **Implement Strong Access Control Measures**
 - Restrict access to data by need-to-know
 - Assign a unique ID to each person
 - Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
 - Track and monitor all access to resources
 - Regularly test security systems and processes
- **Maintain an Information Security Policy**

The standard doesn't specify which firewalls should be used or where they should be placed. It doesn't specify how often passwords should be changed or what their characteristics should be. It doesn't even fully define terms such as "need-to-know." But it does present a set of objectives that IT must fulfill to be compliant.

Fulfillment of objectives such as these involves a full range of IT disciplines. These disciplines include network infrastructure and traffic management, server and desktop systems management, security vulnerability management and intrusion detection, and management of other IT assets such as storage devices and peripherals.

Each of these disciplines must be engaged on several levels. First, anyone managing a compliance initiative must understand the relevance of each discipline to any and all specific compliance objectives: Where does network management have to get involved? What role does systems administration have in fulfilling the objectives? Are there things security staff is already doing that align with the objectives - and are there new things they need to start doing?

Second, appropriate enabling technology must be in place to fulfill all compliance requirements, including both the "doing" and the "documenting." Sometimes, the management technologies already in place will be sufficient to fulfill these requirements. In other cases, new technology must be procured to support compliance efforts.

Third, effective processes and policies must be put in place. Again, these processes must support the "documenting" and "maintaining" as well as the "doing" itself. These processes have to be well-defined and hard-wired into the IT organization. That is, they can't depend on someone remembering to do something. Wherever possible, automation should be used to ensure that appropriate actions are taken as required. For example, in the process of creating and tracking a trouble ticket, if an alert is sent to a technician and that technician fails to take timely action, someone else should be notified. This also points out the importance of defining rules for routing trouble tickets based on business policies.

Compliance is thus a holistic effort that involves technologies, processes and people - from top managers to front-line technicians - across the entire IT organization. Without this kind of across-the-board engagement, compliance initiatives cannot reliably fulfill all of their mandated requirements. And, partial compliance with a regulatory mandate doesn't count. Any gaps in compliance expose an organization to penalties that regulators are authorized to impose. Even worse, such gaps can expose an organization to the significant financial risks associated with faulty information, security breaches, business interruptions and other consequences of inadequate IT governance.

Why compliance hurts

Compliance is fundamentally different from the IT initiatives of the past. For one thing, compliance is imposed from the outside. Unlike the integration of systems from a newly acquired line of business or the rollout of a new sales automation application, compliance projects are not always driven by internal business stakeholders. IT can't enter into the same kind of dialog with external regulators as it can with its own executives and departmental managers. So IT can't push back on requirements and deadlines because of resource constraints or requirements that are perceived as unreasonable.

But, compliance has a bit of a learning curve. IT departments have years of experience developing applications and building out infrastructure. But compliance - understanding it, implementing it and managing it - is a whole new ballgame.

By the same token, compliance is not directly linked to a quantifiable business benefit or objective. Of course, *failure* to achieve compliance can result in fines and even potentially expose top executives to legal action, so there is a strong incentive to fulfill compliance requirements. But those are artificially created incentives. One way to look at compliance is that it does not generate return-on-investment by reducing costs, increasing revenue, or improving customer retention rates. So every dollar and hour spent on compliance pulls a dollar and an hour away from projects that can potentially deliver much higher ROI.

Alternatively, compliance initiatives may create the catalyst to make IT improvements, and adopting best practices may in fact generate positive ROI.

All of these factors make compliance painful and disruptive. What makes this situation especially problematic is the fact that most IT organizations are already stretched thin. A large percentage of their budgets are already consumed just maintaining infrastructure and software environments that have already grown to be quite complex. Whatever resources are left over have to be parceled out to a very limited number of new projects. And everyone knows how hard-fought the internal battles over these limited resources are.

That's why, in addition to fulfilling compliance requirements, IT organizations must also make sure they fulfill those requirements at minimal cost and with minimal disruption to their core activities.

In other words, instead of making inordinate investment in compliance-specific tools and processes, IT organizations are better off leveraging existing resources as much as possible - and, when necessary, investing in tools and resources that provide ROI to the business at the same time as they support the fulfillment of compliance requirements.

Compliance, service management and security

IT departments that want to leverage existing resources to fulfill their compliance requirements should focus their attention on two specific areas: service management and security. These initiatives are particularly well-suited for supporting compliance.

The term "service management" in this context refers to all the tools, people and processes IT uses to ensure the end-to-end delivery of business applications and services. It encompasses network management, systems management, asset management and other disciplines that support optimal performance of the IT environment.

Service management resources can support compliance efforts in a variety of ways. Systems management and administration, for example, provide both the command-and-control capabilities that ensure appropriate backup of sensitive data and the reporting capabilities required to document service availability. Asset management provides the ability to document software licenses and to verify the proper retirement of servers.

Security resources have obvious relevance to compliance. These resources will typically include identity management, vulnerability management and intrusion detection. They can be used to fulfill a variety of compliance-related mandates - including protection of sensitive data, the auditing of system access histories, and reduction of threats to business continuity.

In many cases, IT departments will have sufficient service management and security resources in place to meet near-term compliance requirements. By applying a new set of compliance processes over existing resources, many compliance gaps can be quickly and effectively closed.

However, IT departments may have shortfalls in their service management and security capabilities that limit their ability to fulfill their compliance objectives. In these situations, the optimal solution is to make investments that help meet both compliance requirements and provide core operational benefits.

For example, an IT department that lacked the network traffic monitoring capabilities necessary to fulfill its compliance needs could acquire a technology solution that also improves the effectiveness of its service management and security. Such an investment might be justified primarily by its impact on service delivery. Its compliance-related benefits would essentially be free both in terms of cost and effort.

Using a common set of tools and processes for compliance, service management and security also reduces the total number of vendors IT has to deal with, while streamlining change management by reducing the total number of "moving parts."

The bottom line

The cost and disruption associated with IT compliance can be significantly reduced by fully leveraging existing service management and security resources. Restrict new investments as much as possible to technology solutions and processes that enhance compliance, and IT operations in general, in ways that support core business needs. By adopting this leveraged approach, IT departments can prevent their compliance efforts from becoming painful, distracting exercises and instead take advantage of externally mandated requirements to improve the performance and integrity of critical business services.

No IT device or set of software alone can make a company "compliant" any more than a hammer without a carpenter can build a house. Why? Because compliance requires human attention to meet a set of requirements. While IT products can help meet these requirements, they cannot by themselves ensure compliance. The right solutions do, however, provide tremendous capabilities to enforce IT standards and drastically simplify ongoing reporting requirements for compliance initiatives.

Comprehensive Incident and Problem Management

IT departments must implement efficient and effective incident and problem management systems. Such a system should create Events and provide Notifications that notify administrators or users by pager, email or both when specified events occur or thresholds have been exceeded.

A user-defined escalation path should be provided to ensure that an incident does not go unacknowledged or unresolved. Escalation policies should also be established. For example, the policy might state that for a certain type of incident, a particular IT administrator is to be notified at 5 minute intervals until the notification is acknowledged. If the notification has not been acknowledged within 15 minutes then the IT director and CIO should be notified.

Identify Critical Systems

IT departments must identify critical systems that are necessary for the operation of the business, including operating systems and other system data. For example, they should be able to generate asset reports to know what is in the network and to make informed decisions. Events and thresholds should be specified for systems and applications deemed to be critical such that the appropriate personnel receive event notifications and quickly respond to and resolve problems associated with a critical system. Being able to customize XML-based reports means the information needed can be presented the way that best meets the needs of the situation at hand.

It is particularly useful to have active and automatic identification of critical systems by scanning the network and determining what systems exist, what software and services are installed and running on them, and constantly monitoring their availability. IT administrators need at their fingertips real-time hardware and license inventories, hardware and license management tools, and availability and activity reports.

Restrict Physical Access

IT departments must restrict physical access to their data centers. What is needed is a comprehensive way to allow authorized personnel to work from virtually anywhere while restricting physical access to servers with sensitive information.

This can be accomplished through the use of KVM switches and serial console servers. Though many KVM switches and serial console servers can be used to remotely access servers and other IT infrastructure, the best alternatives are ones that provide considerable flexibility in implementation and have security functionality that includes session logging and reporting. The ability to define service-level views and set service-level permissions for the KVM switches and serial console servers would also be extremely helpful.

Policies and Procedures

Policies and procedures should be implemented to allow those who need access to gain it easily while limiting access for others. For example, Cisco support staff might be restricted to only Cisco devices and only between 8 a.m. and 6 p.m. Monday through Friday. Or only certain IT administrators are given access to human resource servers to protect employee health records. Access to servers containing financial reports could be further restricted during third-party audits.

Enhancements to security policies include active Intrusion Detection. For example, constantly monitoring network traffic for known security threats, intrusion attempts, and denial of service attacks, and alerting critical personnel when threats are detected. Furthermore, vulnerability scanning capabilities regularly screens managed hosts for potential threats - outdated software patches, inappropriately open TCP ports, etc. These critical functions provide significant, real-world assurance that policies are being adhered to since variances from standard policies can be easily detected.

Raritan CommandCenter® NOC: A fully leveraged platform for IT compliance

Raritan's CommandCenter NOC is a family of IT infrastructure management appliances that enable IT departments to fulfill a wide range of critical compliance requirements - while addressing core service management and security issues. It is designed for businesses or business units of larger enterprises with up to 2500 client PCs, 250 servers and 250 network devices.

CommandCenter NOC provides world-class network and systems management, traffic analysis, vulnerability scanning, intrusion detection, asset management and reporting functionality in easily deployed appliances. In addition to helping IT departments ensure application availability and network optimization, when deployed with CommandCenter Secure Gateway these appliances also provide remote access capabilities that enable external vendors to provide a full range of outsourced management services.

CommandCenter NOC's reporting capabilities are particularly useful for compliance-related audits. These capabilities include:

- ▶ Fully customizable XML-based reporting that can be seamlessly integrated with third-party compliance dashboards
- ▶ IT infrastructure reports that support the audit requirements for regulations such as Sarbanes-Oxley, HIPAA and Basel II
- ▶ Comprehensive hardware and software configuration inventories and installed application license counts that simplify audits and asset management

The appliance also tracks and stores performance metrics and outage information.

CommandCenter NOC provides flexible rules-based event notification tools that support user-defined compliance workflow processes - ensuring that appropriate compliance team members receive any necessary alerts based on their roles and responsibilities. Multiple units can be deployed in a distributed architecture to provide complete coverage of the enterprise or multiple business units.

Because CommandCenter NOC provides such complete management functionality in an economical-to-deploy package, it offers a particularly attractive value proposition to IT departments seeking to fill functional gaps in their management toolkits. For example, intrusion detection and vulnerability management can be used to both improve IT operations and fulfill compliance requirements. Using CommandCenter Secure Gateway's single sign-on remote access to troubled servers leads to further efficiencies because IT administrators can restore service and fix problems without leaving their chairs. By meeting these needs with a common investment, the CommandCenter family significantly reduces the cost and disruption of IT compliance.

Conclusion

Raritan's CommandCenter family of multifunction IT infrastructure management and access equipment enable IT departments to address a wide range of regulatory compliance requirements. CommandCenter NOC's intelligent system identification, management and security capabilities perfectly compliment CommandCenter Secure Gateway's instant remote access platform to address the top requirements of corporate compliance: accurate reporting, secured access, enforced policies and active vulnerability and availability monitoring.

No IT products by themselves can ensure a company is Sarbanes-Oxley, HIPAA or Basel II compliant. However, world-class remote access, network and systems management, traffic analysis, vulnerability scanning, intrusion detection, asset management and reporting functionality provide the needed tools to implement a company's IT compliance tactics and strategies. The integrated management dashboard and reporting give IT decision makers actionable intelligence.

About Raritan

Raritan is a leading supplier of solutions for managing IT infrastructure equipment and the mission-critical applications and services that run on it. Raritan was founded in 1985, and since then has been making products that are used to manage IT infrastructures at more than 50,000 network data centers, computer test labs and multi-workstation environments around the world.

From the small business to the enterprise, Raritan's complete line of compatible and scalable IT management solutions offers IT professionals the most reliable, flexible and secure in-band and out-of-band solutions to simplify the management of data center equipment, applications and services, while improving operational productivity. More information on the company is available at Raritan.com.