Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

Governance, Risk, and Compliance

Sponsored by: Cisco Systems

Scott Tiazkun Lucinda Borovick

September 2007

EXECUTIVE SUMMARY

Governance, risk, and compliance (GRC) directly impact business processes, IT processes, and the associated IT infrastructure. Companies that once focused solely on regulatory compliance requirements, such as Sarbanes-Oxley (SOX), now need to respond to a broader array of GRC-related issues that span geographies and governments. Removing the borders of where and how an enterprise does business means creating an environment of information transparency, risk visibility, and flexible business process design that is essential to the future of the successful enterprise. In many cases, these efforts may not be supported as robustly as possible, resulting in tepid GRC support and decreased business agility. Many enterprises either have been forced to address GRC (e.g., SOX, Gramm-Leach-Bliley, HIPAA) and its effect on their business innovation road maps or are proactively choosing to tackle GRC (e.g., enterprise risk assessments) and incorporating it into business process changes.

Proactively, efforts to effect business process change and GRC can be robustly supported by IT and enterprise network enhancements to deliver optimal business flexibility with new levels of communication collaboration and transparency across a borderless enterprise.

Industry-leading IT organizations create IT infrastructures and networks that combine the business and policy context with the visibility and rapid responsiveness necessary to deliver strategic benefits to the organization. These organizations are moving from merely reacting to business risks and events toward improving business predictability, transparency, and performance. This requires an integrated transparent and collaborative enterprise GRC architecture that aligns with the business priorities and creates value by providing information on the business operations, flagging impacting events, and taking or recommending action.

To effectively manage GRC, the enterprise must address the trade-offs between increasing regulatory issues and mandates, budding interest in measuring enterprise risk, and the financial burden to support these efforts. These trade-offs place a burden on IT to determine how applications and an integrated network architectural approach can be instantly responsive across a wide range of organizations and geographically distributed business functions.

Enterprises will rely on the network in new ways. As the network becomes the primary entity that spans desktop, campus, branch, and datacenter, the network will be integral to a complete enterprise GRC solution. An example of how this will be implemented is Cisco's Service-Oriented Network Architecture (SONA), which integrates network services such as security, unified communications, mobility, storage, and network management with applications for GRC and other in-context business solutions.

INTRODUCTION

Few enterprise executives would dismiss the need to address and define compliance and risk issues for their particular enterprise and associated business process environment. The growing concern around various forms of enterprise risk, including financial and operational risk, along with the parallel growth in regulatory frameworks that impact enterprises, has created a perfect storm of risk and compliance needs. This did not happen in a vacuum.

Security breakdowns and financial meltdowns over the past decade have been well documented and magnified. Accordingly, governments and regulatory agencies have created a myriad of business and IT regulatory and risk frameworks in their wake. For example:

- COSO
- Sarbanes-Oxley
- ISO 17799
- Gramm-Leach-Bliley
- HIPAA
- CobiT

The bottom line is that some business executives have been wise enough to think proactively about the future of business process change and governance, risk, and compliance. Otherwise, competitive business pressures and GRC will be forced upon them.

Many enterprises have good intentions but ultimately deal with fragmented approaches to manage GRC issues across their enterprise networks and business lines. Those involved with the GRC business process chain may not have historically thought about the IT network, but today it is a necessity.

GRC is not solely an IT issue — an enterprise must evaluate all aspects of a GRC effort. IT solutions, including applications and supporting networks, must integrate with and "understand" the underlying business processes. Processes consist of multiple business events that can happen within the borders of the enterprise or in the extended enterprise with customers, partners, contractors, and vendors. From the IT perspective, both applications and the network are important. Business applications that interact directly with the network and act on real-time events create enormous benefits for enterprise visibility and responsiveness — key components to a proactive approach to GRC. A risk assessment would consider and articulate the potential for problems. For instance, a fragmented IT approach can adversely impact the enterprise view into risk and associated decision processes. Fragmented IT environments are deleterious whether due to siloed applications, outdated data, or lack of visibility into enterprise relationships that impact governance and risk policies and outcomes.

GRC Issues in Today's Enterprise

The efforts and processes around GRC and business agility in the enterprise are easy to define in general terms but more difficult to pin down and actually implement. Compliance can be defined as conforming to a rule or requirement mandated by law, regulations, or policy, whether an external governing body or an internal best practice is enforcing the rule. Further, compliance requires different procedural steps from one regulatory issue to another.

Specifically, companies have seen compliance initiatives directly impact enterprise business processes. The Sarbanes-Oxley Act passed in 2002 was a response to accounting scandals involving large corporations such as Enron and Tyco. This act contains many duties and corresponding penalties for corporate boards and executives. The overarching principle of the act is to create an environment that enforces standards that ensure accuracy of financial statements filed by any publicly traded companies that file a Form 10-K with the Securities and Exchange Commission (SEC).

How One Regulatory Issue Can Impact IT

Sections 302 and 404 are the portions of Sarbanes-Oxley that most affect the IT departments of an enterprise. These sections require yearly certification of internal controls, as verified by an independent auditor. Lack of security of financial data that results in financial misrepresentation is a violation that could subject an enterprise to fines and can subject responsible parties to imprisonment.

For most enterprises, the financial statements filed with the SEC are drawn from data gathered from numerous internal data sources. Therefore, the access to and accuracy and timeliness of this data will be directly impacted by the IT department and the corporate IT landscape it has created. Ideally, a GRC-ready IT landscape allows senior management to collect, secure, retain, control and report the financial information that is necessary for successful and certified report filings.

Of course, all compliance efforts are both detailed and, at times, industry focused. On a corporate scale, compliance impacts financial metrics, business processes, and security and privacy matters. Only by delving deep into the specifics of any regulatory mandate can an enterprise define how a compliance issue will eventually impact financials and business processes. Suffice it to say that regulatory compliance and risk IT initiatives are becoming part of widespread corporate governance and risk strategies.

Governance, compliance, and risk are closely associated, but addressing compliance issues, such as potential violations of Sarbanes-Oxley, is generally more pressing from a corporate perspective than defining and measuring risk. Ultimately, addressing risk from a proactive perspective will be too financially attractive to ignore. Regardless, IT will also have to support risk initiatives, which are data driven across an enterprise and face the same IT challenges as compliance efforts face.

Regulatory Commitment and Industry Standards Translate to IT Need

No corporate boardroom has been able to ignore the impact of high-profile regulatory issues over the past decade. But what is particularly noteworthy concerning many regulatory issues has been the elevation of IT to address issues such as privacy, internal controls, and security that are necessary to meet the requirements of various regulations.

GRC also makes the security of enterprise data of the utmost importance. Companies are required to establish an infrastructure that will keep the data safe from any unauthorized access or alteration, damage, or loss.

These regulatory and risk issues impact the infrastructure and network for a multitude of industries. Government regulations such as HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley require changes to many network security infrastructures and IT procedures. Companies that want to proactively address risk — operational and financial — also need to improve networks to maximize responsiveness and therefore the protection of the enterprise assets. Many of the business processes needed for enterprise risk impact access to information as well. To close the loop on compliance and risk efforts, enterprises must also be able to show and/or provide reporting that prove that they are in compliance with whatever regulatory issue is being addressed.

The rush of regulatory mandates, dictums, and associated standards and frameworks that entail some sort of compliance processes is rapidly growing. Some of the highly visible and widely applicable regulations are shown in Table 1, along with IT solutions that help to meet these requirements.

TABLE 1

Regulations, Requirements, and IT Solutions

Regulatory Mandate	Requirements of the Act	IT That Addresses Compliance Need
Sarbanes-Oxley	The Sarbanes-Oxley Act of 2002 requires public companies to validate the accuracy and integrity of their financial management. IDC believes this act will have long-term effects on federal securities regulation, corporate governance, and the regulation of auditors. SOX requires that businesses not only document and assess their internal controls but also control access to financial systems.	Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by identity access management solutions. Additionally, applications and networks create viable financial reporting framework.
Gramm-Leach-Bliley	The Gramm-Leach-Bliley Act mandates privacy and the protection of customer records maintained by financial institutions.	These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusions.
HIPAA	The Health Insurance Portability and Accountability Act of 1996 requires that to ensure privacy and confidentiality all patient healthcare information be protected when electronically stored, maintained, or transmitted. It also mandates that each user be uniquely identified before being granted access to confidential information. It specifies that access to personal health information (PHI) be restricted to only those individuals who need access as part of their role.	Identity and access management, provisioning. and single sign-on are network-enabled solutions that can enable access to information but also help limit access to appropriate personnel. Additionally, mobile devices that create data to populate health records need to be encrypted and supported by networks that meet security provisions of HIPAA.
USA PATRIOT Act, Title III, anti–money laundering (AML) regulations	Section 352 requires financial institutions to develop internal policies, procedures, and controls to guard against money laundering. Institutions are required to track and report suspicious activities and conduct regular independent audits to test AML programs. Additional rules designed to establish a customer identification program also came into effect recently and require financial institutions to document the methods they utilize to verify a customer's identity.	Enterprises will require networks that enable business processes that can be shared among networked members and invoked using Web services and a service-oriented architecture (SOA).

Source: IDC, 2007

Table 1 by no means offers a complete list of regulations, but some of the standards developed to support and implement compliance with the regulations and address the regulatory issues mentioned include the following:

- **COSO.** This standard was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and provides guidance on how to organize documentation. For SOX compliance, the SEC identifies the COSO Internal Controls Framework as its preferred set of standards in documenting internal controls and processes.

- **CobiT.** The Control Objectives for Information and Related Technology (CobiT) was developed by the IT Governance Institute (ITGI) as an acceptable standard for information technology security and control practices. CobiT contains 34 processes and provides the tools to assess and measure an organization's ability to deliver on those processes. It was originally published in 1996, with versions 2 and 3 appearing in 1998 and 2000, respectively. ITGI's latest version (4) emphasizes regulatory compliance, helps organizations to increase the value attained from IT, and tries to enable alignment and simplify implementation of the CobiT framework.

- **ISO 17799.** ISO 17799 is a detailed security standard organized into 10 major sections: business continuity planning, system access control, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer and network management, asset classification and control, and security policy. The objective of ISO 17799:2005 is to provide a common basis and practical guideline for developing organizational security standards and effective security management practices.

Many of these regulatory issues and standards emphasize issues such as privacy, security, proper authorization to information, and internal controls and documentation. Providing security and appropriate access to information is how the IT department will contribute to meeting the intent of these regulatory issues.

SONA Architecture

Cisco's SONA is an architectural approach that connects network services to applications to enable business solutions. At a high level, SONA address the two key areas of dynamic IT: providing for operational efficiency and aligning IT with business priorities. Using enterprisewide network-based intelligence to support the delivery of integrated business and GRC solutions — from providing increased efficiency, accelerated business innovation and the potential for turning risk into new opportunities — SONA defines the approach that the network is the common element that connects and enables all components of the IT infrastructure, which now puts the business user as the benefactor of this empowered technology (see Figure 1). These qualities are essential components of a network that supports business process change and governance, risk, and compliance. SONA provides the framework for business network transformation, the ability to leverage and benefit from both the network and application intelligence in an enterprise architecture. Integrated Network Services is a crucial component of SONA. The Integrated Network Services layer provides the interconnection from applications to virtualized IP-based services such as mobility, security, identity, storage, and application (message) networking. These network services are treated as dynamic resource pools that are loosely coupled (independently deployable, manageable, and controllable) and are reusable across the enterprise architecture to gain the most efficient use of resources and applications, taking advantage of the ubiquitous access and responsiveness of the network working with the application. As an example, through the collaboration of both application and infrastructure, the network can now serve as the mechanism in which the application has visibility into every niche of the enterprise, from the end user to the datacenter and beyond to customers, suppliers, and partners through the extended enterprise network; now true transparency is achieved for the business becoming the foundation for business agility.

As part of SONA, the network needs to support the application layer. The network supports applications through application services. Application services consist of a set of network-embedded technologies that improve the deployment of distributed applications and support the transformation to loosely coupled service functions integrated in an enterprise network environment. Application delivery services scale applications by offloading processing tasks from the application servers to purpose-built hardware and software devices that integrate into the network infrastructure and optimization of the communication exchange between the client and the application.

SONA also defines the Network Systems layer, which has traditionally provided connectivity to desktop clients, branches, servers, campuses, datacenters, storage devices, and distributed sites and partners. The objective for this layer is to provide users with anywhere, anytime connectivity. Here physical IT resources are interconnected across a converged IP network foundation. The network infrastructure layer represents how these resources exist in different places in the network, including the campus, branch, datacenter, enterprise edge, WAN/MAN, and teleworker.

Business network transformation is essential for deploying a proactive GRC environment; SONA is at the heart of the network's support of GRC. Cisco SONA expands the role of the network to reach GRC solutions into the extended enterprise, beyond the borders of packaged enterprise applications and into the landscape of physical and infrastructure risk. It provides the framework to aggregate, normalize, analyze, and present business and IT events in an appropriate business context for an organization and across existing geographies and organizations. Network infrastructure and integrated network services provide unparalleled transparency and control in support of business process change and all GRC requirements.

Benefits of SONA/Network Architecture for GRC

Many applications in risk and compliance are not standalone and those that are cannot fully realize their value to the enterprise without tying into other applications or extensions in the enterprise suite, be they ERP, CRM, or supply chain systems.

For instance, some business assurance analytics solutions are designed to monitor ERP systems and perform continuous compliance monitoring that ensures segregation of duties during business processes such as purchase to pay. Even with a process as seemingly simple as purchase to pay, there are several steps and therefore systems that are touched upon during the business process, starting with managing vendors and maintaining source lists, creating requisitions and purchase orders, posting received goods and adjusting inventories, and, finally, involving accounts payable to enter and verify invoices and issue payments.

For most enterprises, a purchase-to-pay process is one that cuts across several application systems. Organizations need to try to protect themselves with policy, procedures, and IT that will support the inherent need to minimize risk and possible fraud issues while also supplying the necessary segregations of duties that help achieve business process compliance.

A network, such as Cisco SONA, provides the framework for real-time data collection, event correlation and notification, policy enforcement, and unified communications to locate the compliance officer to rapidly reduce risk to impacting employees, intellectual property, or systems. Going further, the network will support the creation of documentation and reporting methods that show full compliance with anything from a Sarbanes-Oxley compliance effort to a HIPAA privacy issue — whatever the regulation or compliance milestone that must be supported with real-time information and must also be documented or at least be traceable by an auditor.

CHALLENGES/OPPORTUNITIES

In the future, enterprises will want to make obligatory compliance initiatives part of a financial opportunity to gain increased business efficiency, risk mitigation, and cost containment. From an IT product perspective, there will be a natural product progression to a broader governance platform that enables automated business processes. Additionally, these platforms will support internal process controls, automation of the internal controls, risk management, reporting, and governance.

The ability to respond to broader areas such as information transparency, security, risk visibility, and business process design will be impacted by applications and the network that supports these applications. Enterprises will need to make sure they not only can achieve risk and compliance goals but also can monitor and report the status of the enterprise risk and compliance efforts and the status of the IT infrastructure. The same tools and approach can be utilized to give the enterprise the business transparency and communication tools it needs, within and across its extended borders. Its empowered users quickly make the best possible decisions, armed with real-time and contextual business analytics. This shift in conducting business at the speed of change will drive the next wave of business agility and accelerated business innovation.

Network solutions can enable this goal with relative ease and economy. Vendors will embed compliance and risk capabilities in the next generation of IT solutions, when it makes sense, to close gaps in information transparency, security, and business process rigor.

Additionally, the cost of compliance will impact the uptake of GRC IT solutions. Vendors will be pressed to show how they maximize the IT cost and value of the enterprise compliance and risk effort. They will need to invest the time to determine where the ROI lies and is measurable.

CONCLUSION

GRC and business process change efforts and corresponding IT solutions entail detailed integration with the network as it provides rapid event correlation and notification of events along with contextual business analytics. The right combinations of IT solutions yield information that informs process improvements. Vendors hoping to support GRC and true accelerated business innovation efforts will need to look at IT efforts that help organizations achieve the following:

- Enable applications to "cross-talk" for real-time internal controls, report creation, and risk identification
- Consolidate network usage policy enforcement for infrastructures that adapt to ongoing compliance requirements
- Control and avoid the loss (or leakage) of intellectual property
- Create easy-to-control security platforms for provisioning, single sign-on, and authentication of users that also provide security barriers
- Enable collaborations between people and processes that support governance and risk initiatives
- Use IT so that it becomes a monetary factor that will drive down the cost of compliance and enable risk mitigation as a cost benefit

At this point in the GRC solutions development cycle, most vendors do not offer a comprehensive solution. Partnerships between application, network, and device vendors will provide evolving and more comprehensive solutions. Vendors that create affordable IT portfolios and viable and understandable governance and risk processes stand to gain traction with enterprises that are looking to go beyond HIPAA or Sarbanes-Oxley compliance into operational or financial risk realms as well as take on the bigger challenge of executing business process change and accelerated business innovation. Networks will be a contributing IT factor in helping enterprises achieve this goal. The Cisco SONA product can be an important infrastructure path that users can take to address growing compliance and business innovation needs.

Copyright Notice