IBM Security

Risk and Compliance Management

Enterprise risk and compliance management

IBM Security Solutions enable new business models and help manage compliance across the enterprise

Contents

Executive summary

On a smarter planet, one that is more instrumented, interconnected and intelligent, security plays a vital role in the enterprise. The more data and information organizations make available to their audiences, the greater the risk. As a result, a new set of needs has emerged. Security must be smart security, enabling trust between organizations and their customers, partners, employees and others, and protecting critical information, applications, systems and services. But that’s just the beginning.

Smart security must be there to help organizations capitalize on new and promising models for doing business. For example, federated relationships enable organizations to more freely share information and to collaborate with each other in a highly connected environment. Federation can be challenging because the more connected an organization is, the more vulnerable its systems are to compromise. Smart security is also needed to support new business models such as cloud computing, in which resources are managed outside the boundaries of traditional organizations and their security infrastructures. To take advantage of new opportunities on a smarter planet, organizations must have the assurance that their critical resources are secure and protected—no matter who has access to them, or where they are.

New ways of doing business expand the need to help organizations manage risk across the environment. Today's regulators require compliance with a growing number of standards to protect the privacy and integrity of sensitive data, and organizations must have the right security in place to do so as cost-effectively as possible. However, compliance with these standards doesn't guarantee secure systems: Organizations must also be proactive in assessing and managing risk across their systems.

Proper security controls and best practices play a vital role as organizations work towards reducing complexity, cutting costs and ensuring compliance. Therefore, to enhance security, risk and compliance solutions should be implemented as part of an Integrated Service Management approach. This approach helps make security an integral part of the business process, rather than an add-on, and helps organizations achieve visibility, control and automation across business and IT assets.

Spending more to meet growing compliance demands

Today, there are thousands of regulations governing various organizations in the U.S.—and more are on the way all the time, particularly for highly regulated industries such as banking and financial services. The U.S. Government budget for 2010 calls for expenditures on regulatory activities of $55.8 billion for the fiscal year, up from $53.6 billion in the previous fiscal year, with actual outlays likely to be higher than the budget estimates. Regulatory spending is projected to grow by 4.2 percent in 2010 over the previous year, and staffing at federal regulatory agencies is budgeted to increase 2.3 percent.[1]

Just as the federal government is spending more on regulatory activities, private enterprise is spending more to comply with regulations. One report projects that spending by U.S. companies on governance, risk and compliance will grow to $29.8 billion in 2010, up nearly 4 percent over the previous year[2]—nearly double the amount companies were projected to spend back in 2005.[3] And that doesn't even take into account what is being spent worldwide to comply with U.S. regulatory requirements. Companies have had dedicated regulatory compliance budgets for years now, and as each year passes, the resources needed to comply with ever-multiplying regulations and industry requirements continue to escalate.[4] These regulatory requirements are a response to real and serious threats to corporations and to individual private data from malicious people and organizations who would misuse this data.

And there is no finish line in this race to comply: It is an ongoing, cyclical process that requires continual diligence and focus. Unfortunately, maintaining compliance doesn't always ensure a secure system. Organizations must be wise about how they approach fulfilling compliance mandates so as not to waste time and money. It is the combination of proactively assessing and managing risks in the environment that can not only meet compliance needs, but also enable an organization to pursue new business models aimed at cutting costs and improving service. According to one study, companies who have moved far past basic ad hoc processes to top-level optimization enjoy higher revenues, profits and customer retention levels—and spend less annually on regulatory compliance—than those in the early stages of compliance spending.[5]

Finding smart risk solutions to meet the challenge

Successfully managing risk in rapidly changing regulatory and operational environments is difficult. It requires smart risk solutions that demonstrate new and innovative ways of measuring, modeling and applying risk-related information. Smart risk management is about collecting better information, using it more quickly and more effectively, and minimizing the need for human interaction in routine events. Thus the same intelligence and interconnectedness that make risk and compliance management so challenging also offer the best hope for meeting the challenge:

- A smart enterprise is instrumented, enabling information management and control at a granular level, and allowing organizations to sense threats and to respond quickly and precisely.
- A smart enterprise's systems are built on interconnected data that enables innovation, advances straight through processing and delivers a single source of the truth.
- A smart enterprise enables the rapid, intelligent analysis of a vast mix of structured and unstructured data to improve insight and enable informed judgment.

To stay one step ahead of the challenge of risk and compliance management today, smart enterprises are working to optimize their ability to know and manage their risk exposure, across lines of business, across the globe, and in real time.

Addressing risk and compliance with the IBM Security Framework

As organizations work to create infrastructures that are both secure and dynamic, they face new imperatives to manage risk end-to-end across security domains. The key to managing risk in a dynamic infrastructure is to develop a foundational set of security controls that make it possible to deliver services with agility and speed—while keeping down the costs of managing, administering and operating the security infrastructure.

To this end, IBM has created a comprehensive security framework, based on:

- Control Objectives for Information and related Technology (COBIT) a globally accepted framework for governance based on industry standards and best practices.[6]
- Code of practice for information security management (ISO/IEC 27002:2005), an international standard establishing guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.[7] This standard contains best practices of control objectives and controls in 11 areas of information security management.
- IT Infrastructure Library® (ITIL®) providing a comprehensive, consistent and coherent best practice framework for IT service management and related processes.[8]

From a security standpoint, the integration of these processes and best practices allows organizations to make sure they are functioning properly within a set control limit, to deliver the services that are expected or mandated in an increasingly interconnected and complex world.

The overall foundation of the IBM Security Framework consists of security governance, risk management and compliance, supporting common policy, event handling, and reporting. Key components of the IBM Security Framework include:

- People and identity – ensuring that the right people and systems have access to the right assets at the right time.
- Data and information – protecting critical data in transit and at rest.
- Application and process – ensuring application and business services availability and security.
- Network, server and endpoint – staying ahead of emerging threats across IT system components.
- Physical infrastructure – leveraging digital controls to secure events in the physical world.

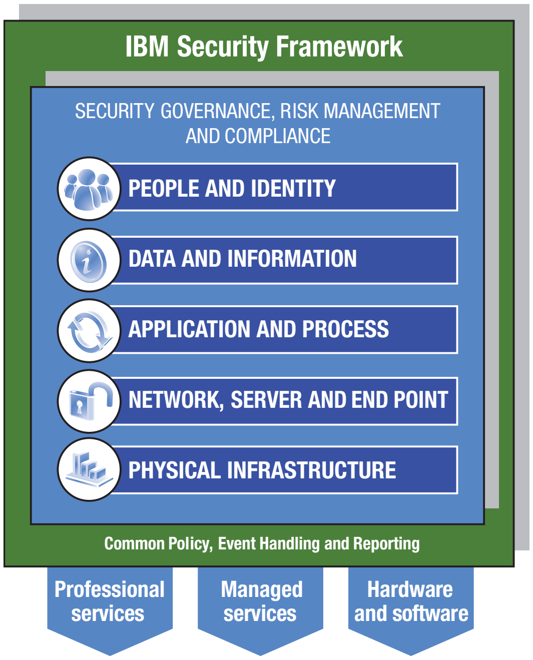

Figure 1: The security framework developed by IBM provides a foundation for managing risk end-to-end across enterprise security domains.

IBM helps enterprises apply this security framework, in whole or in part, through a combination of hardware, software and services. IBM's solutions for enterprise risk and compliance management within this framework are comprehensive and flexible; they can be tailored to unique enterprise requirements to appropriately manage risk and help demonstrate compliance to regulators.

IBM Security Solutions for enterprise risk and compliance management

IBM offers a comprehensive portfolio of security solutions for enterprise risk and compliance management, which help meet the challenges of securing systems in an increasingly instrumented, interconnected and intelligent organization. These offerings deliver a full range of capabilities that address the people, process and information risks in enterprise environments. To ensure the environment is functioning properly within a set control limit across business and IT assets, proper visibility, control, and automation is needed. Implementing risk and compliance management solutions in an Integrated Service Management approach can enhance security by building it as an integral part of the business process, rather than an add-on. IBM Security Solutions, implemented with an Integrated Service Management approach, can deliver the visibility, control and automation required to enable successful business growth on a smarter planet.

IBM solutions for enterprise risk and compliance management secure the enterprise end to end, across identities, data and information, applications, processes, and infrastructure. Automated risk management capabilities are part of each offering, to close the loop from controls and management to audit and compliance. By establishing an integrated compliance management mechanism throughout these offerings, IBM solutions help to ensure consistent compliance across platforms.

This paper describes specific IBM software solutions for helping you assess and manage risk across the enterprise.

IBM Tivoli Security Management for z/OS: Next-generation mainframe security

The increased complexity and scope of mainframe operations, coupled with the limited availability of skilled mainframe personnel, present challenges for managing an organization's most secure platform. Growing data volumes, the necessity to share information that resides on the mainframe, and the obligation to monitor access control—even for the systems' privileged users—can generate great expense and complex security issues. Organizations require a mainframe solution that can securely automate audit, alert, and monitoring capabilities while enhancing the mainframe's ability to be the hub of enterprise security.

In today's large enterprise, many mission-critical applications are likely to reside on IBM System z® mainframe computers. IBM helps enable the mainframe to operate as an enterprise security hub with an end-to-end mainframe security solution that provides security policy enforcement, effective user management, threat monitoring and other risk and compliance management-related capabilities.

IBM enhances risk management and compliance by establishing and enforcing security policies based on specific enterprise security requirements. Organizations can proactively enforce security policy compliance on Resource Access Control Facility (RACF®), prevent internal security errors, identify noncompliance security commands, and issue alerts in response to high-risk security commands.

Tivoli Security Management for z/OS® provides more effective user management and simplified security administration to help increase efficiency and reduce errors in tasks associated with risk and compliance management. For example, administrators can test security configuration changes without affecting production, proactively identify potential conflicts between multiple RACF databases, and manage users, groups, roles, permissions and policies from a single interface.

Through comprehensive, continual monitoring for threat incidents, Tivoli Security Management for z/OS can detect changes to established baselines and find evidence of abuse of privileges, reducing the risk of insider threats. IBM's solution also includes capabilities such as cross-platform log collection, sophisticated data analysis, and prepackaged reporting across operating systems, applications and databases to help facilitate demonstration of compliance with government and industry regulations and standards.

Tivoli Security Management for z/OS supports all currently supported versions of the IBM z/OS operating system, as well as subsystems such as CICS® that enterprises depend on. This reduces the effort associated with upgrading to a new release of z/OS, making it easier to manage risk and compliance in a nondisruptive manner.

Through the combined security capabilities IBM provides—RACF, System z mainframe security and other IBM enterprise security solutions—organizations can establish an enterprise security hub on which to centralize and standardize security management and security policy across the enterprise. The hub can provide capabilities for risk and compliance management such as life-cycle identity management, access control policies, federated identity management, and compliance monitoring and reporting capabilities.

Tivoli Security Management for z/OS is part of the zSecure family of products, which includes offerings that add additional auditing and risk management capabilities to CA TopSecret and CA ACF/2, as well as to RACF.

IBM privileged identity management solutions: Defense against insider threats

While protecting IT systems from external harm is crucial, especially when traditional boundaries are blurred by the need to share and collaborate with other organizations, it's important to remember that the threat to systems can also come from within the enterprise—in the form of privileged users. These are the individuals who use IT systems, applications and data to do their jobs on a daily basis, who have access to sensitive information and assets, and who often are highly capable technology users. Because they are entrusted with such broad access to IT systems, these insiders may represent the biggest threat to data integrity and privacy in an organization. In fact, a 2007 study indicates that approximately 69 percent of security incidents originate with employees and former employees.9 Whether intentional and malicious, or innocent and accidental, these incidents can cause serious harm, and enterprises must guard zealously against them.

Obviously, the answer to managing the risk associated with privileged users is not to limit access; for administrators, LOB managers and others, broad access is essential. The answer is to ensure an appropriate level of visibility into their actions and to have both policies and processes in place to quickly respond to problems and potential problems. IBM Security Solutions can help protect the enterprise in this way, with capabilities for managing access to systems and applications by enforcing user rights, using real-time behavior tracking to spot problems, and providing real-time alerts to resolve threats quickly.

Another key benefit of IBM privileged identity management solutions is the ability to maintain control and accountability of privileged identities as virtual machines proliferate, data center consolidations advance, and cloud computing matures.

The IBM Tivoli Access Manager family of solutions enables organizations to establish an effective, automated system to manage privileged user access to operating systems, e-business applications and other critical systems. Once that is in place, solutions such as Tivoli Security Information and Event Manager can be used to automatically monitor user behavior, identify problems and report on user activities. This makes collected user activity monitoring information actionable, particularly with regard to demonstrating compliance with internal policies and regulatory requirements that are associated with privileged-user issues. Tivoli Security Information and Event Manager also provides near-real-time alerting capabilities. Information on suspicious activities can be routed to a correlation engine for further analysis and action.

IBM Tivoli Security Information and Event Manager: Optimized compliance efforts

Security information and event management (SIEM) can help optimize security and compliance efforts by combining real-time management with monitoring and reporting. IBM Tivoli Security Information and Event Manager brings together the two major aspects of SIEM—a real-time management dashboard for incident management and an information analysis dashboard for assessment of policy compliance—to provide a comprehensive foundation for managing risk and compliance. With these two capabilities working together, organizations can centralize log collection and event correlation across the enterprise, as well as leverage an advanced compliance dashboard to link events and user behavior to corporate policies.

The robust enterprise audit dashboard provided by Tivoli Security Information and Event Manager allows chief information security officers and auditors to obtain a single view of all relevant activities in the enterprise. At a glance, they can see how much activity has been logged and compare user profiles with information being accessed. The enterprise audit dashboard also helps view policy violations over time and leverage log databases to meet different reporting and compliance requirements.

To facilitate compliance with specific regulations, the IBM solution also includes a range of management modules, each of which provides extremely detailed help including:

- An asset classification template showing information, people and assets that are affected, using the vocabulary employed by the regulation.
- A policy template that measures event data against a custom policy that governs who should have access to regulated information and how much they should be able to do with it.
- A report center that draws on the asset classification and policy templates to provide dozens of relevant compliance reports geared to a specific regulation or best practice.

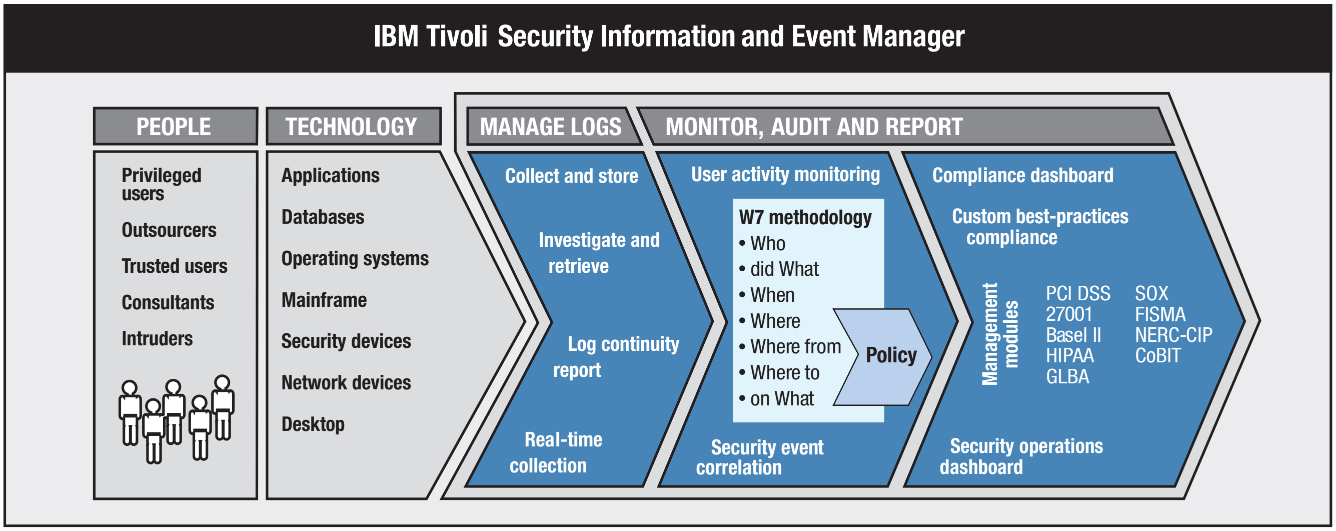

Figure 2: IBM Tivoli Security Information and Event Manager provides a comprehensive foundation for addressing SIEM requirements.

Guardium software from IBM: Database risk and compliance management

The quest for cost-effective enterprise risk and compliance solutions that provide both real-time security and fine-grained auditing extends to database environments, where stand-alone appliances can be used to enforce policies without significant impact on performance.

Guardium real-time database monitoring and security for enterprise applications enables organizations to secure their critical enterprise data by proactively identifying unauthorized database activities. It also includes auditing and compliance capabilities to simplify compliance and data privacy processes. And unlike many database auditing solutions, Guardium covers the z/OS operating system platform, providing complete database coverage. It creates fine-grained audit trails without impacting performance or stability, unifies monitoring for multiple platforms, and assures separation of duties by operating outside the database as an independent network appliance.

Guardium database monitoring and security features a workflow automation application that streamlines the compliance workflow process, transforming database security lifecycle management from an error-prone, time-consuming activity that is performed periodically to a continuous, automated process that efficiently supports risk and compliance goals. The software:

- Provides a single set of policies and reports across the entire infrastructure, without the need to configure each database server or install new software.
- Stores both the audit trail and the results of oversight in a repository that cannot be modified, even by privileged users.
- Tracks the results of electronic sign-offs and escalations.
- Manages the regular distribution of compliance reports across the enterprise.
- Enables proactive, real-time response to security incidents and policy violations, rather than offering only after-the-fact analysis of static log data.
- Provides automated compliance reporting and workflow automation to reduce IT workload.

Guardium can also be used to automate any repetitive task. For example, periodic scans can be scheduled to autodiscover sensitive objects that may have been added or moved from previous locations—and the resulting information can be used to automatically update all appropriate policy groups for such objects.

IBM Tivoli Data and Application Security: End-to-end protection of enterprise data

As data volumes continue to increase and data-sharing remains a vital part of doing business, today's enterprise faces a growing risk of data loss. Data volumes are currently doubling every 18 to 24 months, complicating efforts to provide secure storage of enterprise data.[10] And applications have become a primary attack point for data security breaches. With the increasing complexity of today's composite applications, combined with ongoing efforts to make them more accessible to users who need to share information, an organization's data is more vulnerable than ever. Data loss incidents have the potential to dramatically impact the enterprise, with consequences ranging from easily quantifiable effects on the bottom line to less measurable, but equally damaging, effects such as loss of public goodwill.

Tivoli Data and Application Security helps organizations protect data and applications by providing auditable access controls, enabling fine-grained control of user privileges and centralizing management of data encryption keys. It provides end-to-end protection of sensitive data in enterprise storage systems, databases and within critical applications, helping support regulatory compliance initiatives and improving data and application reliability.

IBM Tivoli Data and Application Security offers the following key features:

- Fine-grained management of user privileges, from the application level to the operating system level.
- Centralized entitlement and security policy management and enforcement—for fine-grained authorization and data-level access control.
- Centralized management of encryption keys—for both tape and disk storage.
- Comprehensive and automated user activity monitoring and reporting.
- Centralized, automated compliance reporting and log management customized to address a wide variety of regulations and industry standards, such as Payment Card Industry Data Security Standard (PCI DSS), Basel II, Sarbanes-Oxley (SOX) and ISO 27002.

The data and application security solution can help organizations manage risk by preventing unauthorized access to or use of sensitive data that can lead to data breaches or compliance violations. At the same time, it can help facilitate data sharing among internal and external collaborators, including through Web-based services.

IBM Rational AppScan Enterprise Edition: Testing for Web application vulnerability

Testing and reporting on the security of Web applications is an increasingly important part of risk and compliance management for any enterprise engaged in e-business. The challenge for many organizations in this regard is to scale application scanning across the enterprise while still maintaining centralized control of vulnerability data. To meet this challenge, IBM offers IBM Rational® AppScan® Enterprise Edition, a Web-based multiuser application security solution for testing teams that need to perform vulnerability assessments in a centralized fashion. Capabilities of the software include advanced application scanning, remediation capabilities, executive security metrics and dashboards, and key regulatory compliance reporting.

IBM Rational AppScan Enterprise Edition features a scalable enterprise architecture that enables centralized scanning of multiple applications simultaneously. It works by traversing a Web application, analyzing and testing it for security and compliance issues, and then generating actionable reports. The software can detect embedded malware and links to malicious or undesirable sites in Web applications, reducing the risk that an enterprise's sites will infect visitors' systems or redirect them to dangerous online destinations. Once the scanning process identifies a security vulnerability, the software provides intelligent fix recommendations to ease the remediation process. It also performs continuous monitoring and aggregation of metrics to ensure remediation and trend improvement over time. Sophisticated dashboards and flexible reporting views provide enterprise-wide visibility into risks and remediation progress. Seamless integration with quality assurance (QA) testing tools and code scanning devices further simplifies security testing and remediation by QA and development teams.

To demonstrate compliance with regulations governing the security of enterprise systems, the software comes with more than 40 out-of-the-box security compliance reports including reports for the PCI DSS, ISO 27001 and ISO 27002 security standards, and industry-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and the Basel II accord.

IBM Security Services: A comprehensive approach to end-to-end risk management

IBM Security Services provides the industry's broadest and most innovative portfolio of security services, which enable customers to effectively manage risk while optimizing security investments. By offering a variety of services across all domains of the IBM Security Framework—risk compliance management; data and information; application and process; network, server and end point; and physical infrastructure—IBM Security Services drives improved integration, time to market and time to value for enterprises.

The IBM Security Services portfolio includes Professional Security Services, to help assess, plan and implement security solutions; Managed Security Services such as managed firewall services, in which IBM manages security for the enterprise from the cloud; and Cloud Security Services such as Web URL filtering or security event log management.

In the area of risk and compliance management, offerings from IBM Security Services can help enterprises meet three key business challenges: satisfying regulatory compliance requirements, understanding and managing risk, and implementing appropriate policies and controls. Services offerings to address these challenges include:

- Security policy planning and development.
- Security risk assessments.
- Security health checks.
- Security workshops.
- Information security framework development.
- Enterprise security architecture development.
- Privacy services.
- PC security assessments.

These offerings benefit the enterprise in several ways, from helping set a baseline for compliance by assessing compliance posture against leading regulatory and industry standards, to developing an appropriate and effective framework for risk and compliance management. IBM Security Services leverages best-of-breed products from both IBM and other leading security vendors who are IBM Select Partners.

Why IBM?

As a leading security company, IBM works with our clients as a trusted partner in delivering security products and services in which our research, leading-edge technologies, consulting expertise, implementation experience, and world-class support for IT security solutions are consolidated and linked together – where security becomes inherent in the design of your IT services environment. We help our clients address the complexity, cost and compliance issues of ensuring security for a smarter planet. IBM is in an ideal position to assess our clients' security needs, provide solutions, and ensure that those solutions are successfully implemented:

- We have the skills – IBM has X-Force® to understand and remediate threats, and thousands of researchers, developers, consultants and subject matter experts on security initiatives.
- We know how – We have consulted on and implemented thousands of security projects, so we have the practical expertise in best practices, processes, and ROI, and we care about our clients' success.
- We get the big picture – IBM provides end-to-end solutions, from security strategy and governance to security across mainframes, desktops, networks, pervasive computing and more.
- We know our customers' industries – IBM has wide industry expertise and tailors security solutions to industry vertical challenges, including securing business processes.
- We live it – We manage security and privacy for our 400,000 employees worldwide, and our services teams manage more than 7 billion security "events" for clients every day.
- We can prove it – IBM has been providing IT security for over 30 years. We have over 200 security references and more than 50 published case studies.
- We have an ecosystem – IBM has a large Business Partner community that complements and implements our solutions.
- We can help you choose – IBM Security Services assessors can provide a list of IBM and non-IBM products to assist clients in creating the best solution for your environment.

For more information

To learn more about how IBM can help your organization develop a security posture that better serves your business goals by effectively managing risk and compliance, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/security.

IBM Corporation Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
March 2010
All Rights Reserved

Use of the information herein is at the recipient’s own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice. References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

[1] deRugy, Veronique, and Melinda Warren, “Regulators’ Budget Report: Expansion of Regulatory Budgets and Staffing Continues in the New Administration,” Mercatus Center, George Mason University, October 2009. http://mercatus.org/publication/regulators-budget-report

[2] Tucci, Linda, “Governance, risk and compliance spending to grow in 2010,” SearchCompliance.com, December 1, 2010. http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html

[3] D’Antoni, Helen, “Security Conforms to Regulatory Compliance,” Information Week, August 29, 2005. www.informationweek.com/news/securityshowArticles.jhmtl?articleID=170100825

[4] “64% of Companies Have Dedicated Regulatory Compliance Budgets, According to META Group Study,” Business Wire, July 26, 2004. www.thefreelibrary.com/64%25+of+Companies+Have+Dedicated+Regulatory+Compliance+Budgets,...-a0119745130

[5] Greiner, Lynn, “Compliance spending offers benefits besides security,” Network World, August 12, 2008. www.networkworld.com/news/2008/081108-compliance-spending-offers-benefits-besides.html

[6] For more information about COBIT, go to www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

[7] For more information about ISO/IEC 27002:2005, go to www.iso.org/iso/catalogue_detail.htm?csnumber=50297

[8] For more information about ITIL, go to www.itil-officialsite.com/home/home.asp

[9] The Global State of Information Security 2007, a Joint Research Project of CIO and CSO in partnership with PricewaterhouseCoopers. www.pwc.com/en_BE/be/publications/state-of-infsecurity-pwc-07.pdf

[10] “Data Volume is Becoming Unmanageable, Say Executives,” Government Technology News Report, August 5, 2008. www.govtech.com/gt/articles/385068

♻ Please Recycle