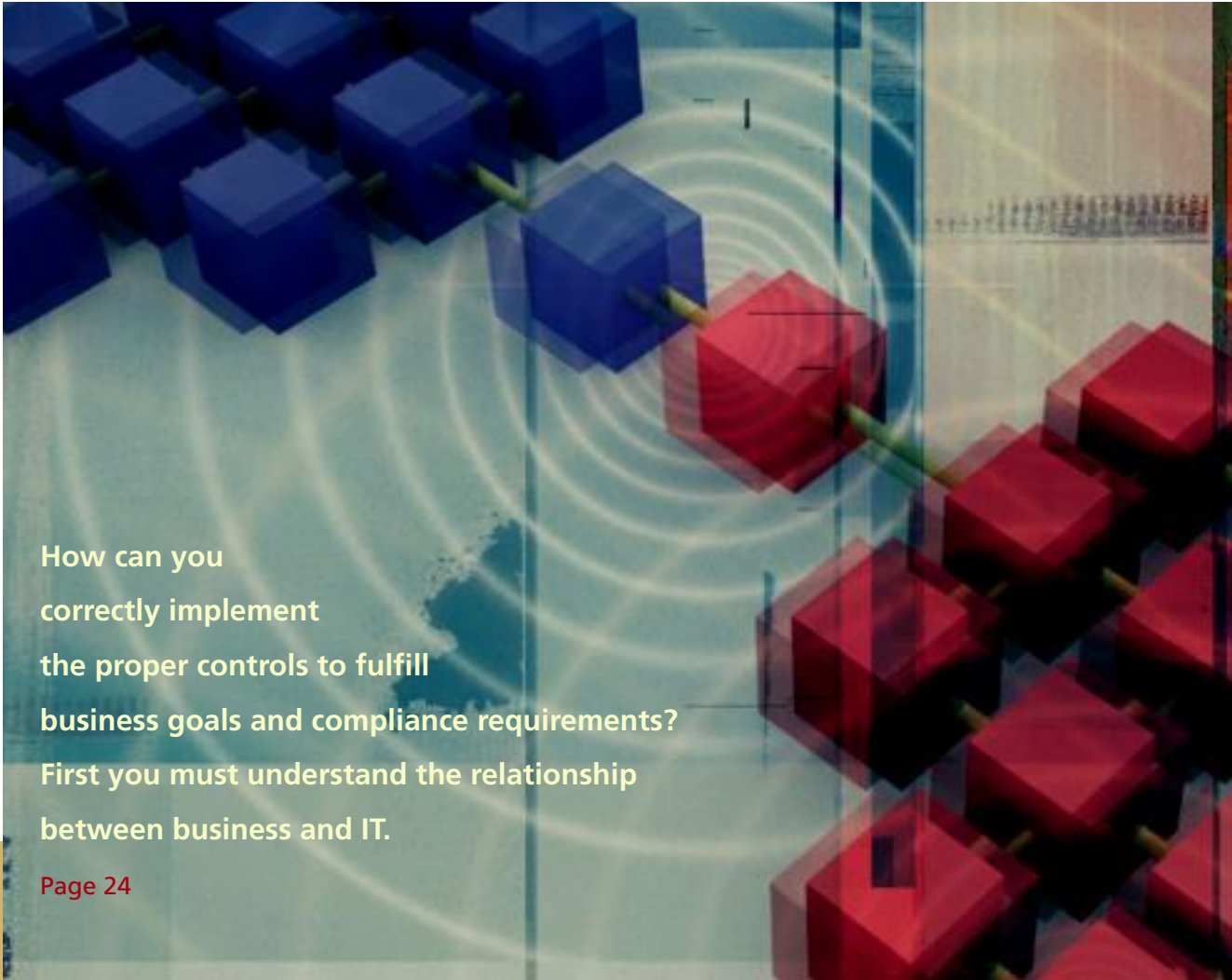


# IT COMPLIANCE JOURNAL

PRACTICAL, ACCESSIBLE INFORMATION FOR COMPLIANCE PROFESSIONALS

VOLUME 1, SPRING 2006

An abstract graphic featuring a grid of blue and red cubes. A single red cube is highlighted with concentric white circles radiating from it, suggesting a focal point or a signal. The background is a light blue gradient with faint grid lines.

How can you  
correctly implement  
the proper controls to fulfill  
business goals and compliance requirements?  
First you must understand the relationship  
between business and IT.

Page 24

## IN THIS ISSUE

Privacy, Network Security, and the Law 7  
**Robert J. Scott**

Governance: A Business Intelligence Best-Practice Case Study 15  
**Beth Leonard**

A Best-Practices Approach to Leveraging Control Frameworks  
for Compliance and Risk Management 21  
**R. Andrew Brice, CISA, CISSP**

Perfect Pitch: Aligning Compliance, Risk, and Business Intelligence 30  
**Linda L. Briggs**



## Dramatically reduce the time, effort and resources spent on IT compliance.

Are you increasingly burdened by multiple regulatory compliance mandates and associated audit and reporting efforts? **Scalable's IT compliance management solutions** enable organizations in multi-regulatory environments to cost-effectively achieve, demonstrate and maintain IT compliance through:

- **Automated traceability** of regulatory standards to controls and audit evidence
- **Single, rationalized policy and control framework** that addresses SOX, NERC CIP, GLBA, HIPAA, FISMA, ISO 17799 and other mandates/standards
- **Comprehensive IT compliance evidence repository** that aggregates across evidence sources and types; attestation, awareness, assessments and system checks

Scalable's award-winning **Command Center** product streamlines key IT compliance processes.

Let **Scalable Software** provide you the services and capabilities needed to cost-effectively achieve, demonstrate and maintain IT compliance.

Call **877.763.7248 X4023** to learn more and schedule a demo of our award-winning **Command Center** product.

**website:** [www.scalable.com](http://www.scalable.com)  
**email:** [info@scalable.com](mailto:info@scalable.com)

2929 Allen Parkway, Suite 1400 Houston, TX 77019



**SCALABLE**  
SOFTWARE

IT Compliance & Asset Management

## Table of Contents

5 ITCi Research Director Perspective

6 COMSTATs

A compilation of key compliance statistics from the past year

7 Privacy, Network Security, and the Law

State privacy rules that currently guide business practices;  
Federal privacy bills under consideration.

**Robert J. Scott**

15 Governance: A Business Intelligence Best-Practice Case Study

A sophisticated BI program addresses governance challenges and  
generates a two-year ROI of 700 percent.

**Beth Leonard**

21 A Best-Practices Approach to Leveraging Control Frameworks for  
Compliance and Risk Management

A logical road map IT managers can use to address compliance  
challenges—and justify compliance investments.

**R. Andrew Brice, CISA, CISSP**

30 Perfect Pitch: Aligning Compliance, Risk, and Business Intelligence

Breaking compliance and risk management efforts into manageable  
chunks and measurable metrics can simplify the picture.

**Linda L. Briggs**

36 Compliance Bibliography

**IT COMPLIANCE INSTITUTE**

5200 Southcenter Blvd., Suite 250  
Seattle, WA 98188  
Phone: 206.246.5059 Fax: 206.246.5952  
<http://www.itcinstitute.com>

**EDITORIAL AND RESEARCH DIRECTOR** Cass Brewer

**GENERAL MANAGER** Meighan Berberich

**DIRECTOR OF MARKETING** Michelle Johnson

**V.P., BUS. TECH. GROUP & NEW BUS. DEV.** Ellen Hobbs

**ART DIRECTOR** Deirdre Hoffman

**GRAPHIC DESIGNER** Bill Grimmer

**EDITOR** Huan Do

---

**1105 MEDIA**

Corporate Headquarters: 9121 Oakdale Ave. Ste. 101,  
Chatsworth, CA 91311, [www.1105media.com](http://www.1105media.com).

**PRESIDENT & CEO** Neal Vitale  
[nvitale@1105media.com](mailto:nvitale@1105media.com)

**CFO** Richard Vitale  
[rvitale@1105media.com](mailto:rvitale@1105media.com)

**EXECUTIVE VP** Michael J. Valenti  
[mvalenti@1105media.com](mailto:mvalenti@1105media.com)

**DIRECTOR OF IT** Jerry Fraizer  
[jfraizer@1105media.com](mailto:jfraizer@1105media.com)

**DIRECTOR OF CIRCULATION AND DATA SERVICES**  
Abraham Langer [alanger@1105media.com](mailto:alanger@1105media.com)

**DIRECTOR OF WEB OPERATIONS** Marlin Mowatt  
[mmowatt@1105media.com](mailto:mmowatt@1105media.com)

**DIRECTOR OF PRINT PRODUCTION** Mary Ann Paniccia  
[mpaniccia@1105media.com](mailto:mpaniccia@1105media.com)

**CONTROLLER** Janice Ryan  
[jryan@1105media.com](mailto:jryan@1105media.com)

**DIRECTOR OF FINANCE** Paul Weinberger  
[pweinberger@1105media.com](mailto:pweinberger@1105media.com)

**CHAIRMAN OF THE BOARD** Jeffrey S. Klein  
[jklein@1105media.com](mailto:jklein@1105media.com)

---

**ADVERTISING SALES** Drew Seifried  
[dseifried@itcinstitute.com](mailto:dseifried@itcinstitute.com), 206.246.5059, ext. 123

---

List Rentals: 1105 Media, Inc. offers numerous e-mail, postal, and telemarketing lists targeting business intelligence and data warehousing professionals, as well as other high-tech markets. For more information, please contact our list manager, Worldata, at 800.331.8102 or [www.worldata.com](http://www.worldata.com).

Reprints and E-prints: PARS International, [1105reprints@parsintl.com](mailto:1105reprints@parsintl.com).  
Phone: 212.221.9595, Fax: 212.221.9195

© Copyright 2006 by 1105 Media, Inc. All rights reserved. Reproductions in whole or part prohibited except by written permission. Mail requests to "Permissions Editor," c/o IT Compliance Journal, 5200 Southcenter Blvd., Ste. 250, Seattle, WA 98188. The information in this journal has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been reviewed for accuracy, there is no guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors, new developments in the industry and/or changes or enhancements to either hardware or software components. Produced in the USA. Product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.



## About ITCi

### OUR MISSION

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance, corporate risk management, and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today's regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi's primary goal is to be a useful and trusted resource for IT professionals accountable for privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

ITCi sponsors a variety of programs and offerings, including a worldwide membership program, weekly e-newsletter, educational online and live events, an in-depth research program, the Unified Compliance Project, and many others.

### OUR MEMBERS

ITCi supports a diverse member community composed of CIOs, CTOs, IT managers, analysts, consultants, and compliance specialists from around the world. Our members enjoy unrestricted access to ITCi research and analysis, white papers, and the Unified Compliance Project, as well as discounts on ITCi conference and summit registrations.

## ITCi CORE PROGRAMS

### ITCi Research & Analysis

ITCi supports, develops, and distributes regular research to keep our members up to date on the technology impact of government regulations, as well as trends within the vendor community. ITCi's research network provides timely updates on new regulations, industry trends, emerging technologies, peer case studies, and compliance best practices based on primary research and interaction with our members. This information is delivered via our Web site, e-newsletters, Member alerts, ComplianceWEB Webinars, and ComplianceINSIGHT white papers.

### ComplianceNOW E-newsletter

ComplianceNOW, distributed weekly and written by the experts in the field, features news and analysis on revised, new, and emerging regulations that impact IT professionals across all geographies and vertical markets. ComplianceNOW is a timely resource that provides insights, best practices, and recommendations that help IT management and staff address the complex issues surrounding their role in regulatory compliance.

### Unified Compliance Project

The Unified Compliance Project (UCP) is a collection of resources designed to help IT managers simplify, standardize, and align complex compliance initiatives. The UCP includes white papers, Webinars, and the largest free regulatory crosswalking resource available to IT and compliance managers today. By focusing on

commonalities across regulations, standards-based development, and simplified architectures, the UCP supports a strategic approach to IT compliance that reduces cost, limits liability, and leverages the value of compliance-related technologies and services across the enterprise.

### ComplianceWEB Events

As part of our ongoing commitment to research, we regularly produce IT Compliance-related Webinars. This body of research and analysis comprises our ComplianceWEB Event Series.

ComplianceWEB events generally occur on a monthly basis, and feature an ITCi staff moderator and an expert speaker for the event's featured topic. Past events include: "Five Critical Factors in Defensible Information Security Policies," "Ten Pitfalls to Avoid in PCI Security Standard Compliance," "Compliance Dashboards: Integrating Governance and Performance Metrics," and many more.

### ComplianceINSIGHT White Papers

ITCi periodically produces research-oriented white papers that delve deeper into compliance topics. The ComplianceINSIGHT White Paper series is a growing body of research that represents an extremely popular and highly downloaded resource for our audience.

Past ComplianceINSIGHT papers cover specific regulations such as Sarbanes-Oxley and HIPAA, as well as overarching strategic themes, such as defensible policies and compliance intelligence.

### ITCi Conferences & Summits

We believe that face-to-face interaction is a vital part of continued education and growth in any occupation, which is why we convene compliance professionals for live events at different locations throughout the country.

Our most recent event, the Unified Compliance Summit, was held in Las Vegas and received high marks from attendees across the board. Additional events are planned for 2006 and 2007; [join our mailing list](#) to stay informed of developments.

### Regulations Database

The ITCi Regulations Database is a unique resource, available only to ITCi members, that holds the most comprehensive online repository of regulation descriptions, IT-centric analysis of statutory impact, and key compliance dates. Together with timely articles, vendor resources, and topical alerts, the Regulations Database rounds off one of the most useful and informative Web sites addressing compliance-related technology issues.

### www.ITCinstitute.com

ITCi's Web site serves as a central source for all ITCi education, research, and community interaction. It features news, research and analysis, best practices, case studies, white papers, Webinars, information about ITCi and industry events, the Unified Compliance Project, a vendor directory, and much more.





# IT Compliance Conference

WASHINGTON, D.C., OCTOBER 2–4, 2006

[www.ITCinstitute.com/dc06](http://www.ITCinstitute.com/dc06)

Attend the IT Compliance Conference and explore the major IT issues that underlie compliance, risk management, and governance programs. Leave with concrete recommendations for building sustainable compliance programs that deliver real business value.

## Learn To:

- Reduce complexities and streamline your IT compliance activities
- Leverage technology solutions across the enterprise to meet complex regulatory requirements
- Save money and reduce costs by capitalizing on previously hidden efficiencies
- Effectively design, align, and control your compliance solutions

## Who Should Attend:

- CIOs/CTOs
- Chief compliance officers
- Chief security officers
- IT directors and managers
- Compliance managers
- CFOs/financial officers

# ITCi Research Director Perspective

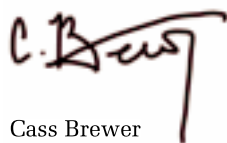
Who can you trust when it comes to compliance advice?

This is a question that we at ITCi ask ourselves every day. Seldom in history has the business world seen such a froth of hype and hysteria as compliance has generated over the last three years. As it turns out, massive budget infusions, vague guidance, and the threat of jail time for failure are a fairly perfect formula for information chaos.

Not that compliance is itself chaotic. Antifraud and risk management regulations like Sarbanes-Oxley and Basel II are purgative responses to a demonstrable history of creative and negligent accounting. Electronic administration rules such as Gramm-Leach-Bliley, HIPAA, and FISMA address the need for IT management in industries flush with both sensitive information and unruly information systems. And privacy and security regulations, such as the EU Data Protection Directive and US state privacy laws, confront the queasy reality that personal rights and identity can be stolen as easily as personal information.

The processes, policies, and technologies that lie at the core of compliance with these regulations are also rational. Complexity can be deconstructed, implementation demonstrated, best practices documented, and control objectives modeled. In fact, we at ITCi regularly see this rational potential fulfilled by our members and other compliance practitioners, regulators, auditors, and vendors. But we've also seen that the success and practical knowledge gained through these endeavors is too often hidden from the people who really need it.

Providing an accessible venue for brutally practical information on how the people responsible for compliance and risk management succeed is the primary goal of the IT Compliance Journal. We have vetted each paper in this, our inaugural issue, to ensure it provides coherent, intelligent, and unbiased research and insight. We learned a lot in compiling this issue, and we hope you'll find it at least as useful as we do—a little bit of concrete amid the chaos and froth. If you have feedback on the Journal or its topics, please feel free to write us at [editor@itcinsitute.com](mailto:editor@itcinsitute.com).



Cass Brewer  
Editorial and Research Director  
IT Compliance Institute

# COMSTATs

A compilation of key compliance statistics  
from the past year.

Percentage of material weaknesses in internal controls that can be mitigated through IT, as reported by Gartner: **97**

Portion of compliance budget used for Sarbanes-Oxley compliance, according to a recent study by AMR Research: **22 percent**

Percentage of large enterprises that regularly experience application downtime due to application infrastructure failure: **73**

Total estimated damages resulting from **identity theft: \$5 billion** for individuals and **\$48 billion** for businesses

Percentage of US business organizations expect to increase their IT spending over the next three years: **60**

Percentage of budget used for general SEC compliance, document retention requirements, and security and privacy compliance, respectively: **13, 12, and 7**

Number of high-tech jobs that were created in 2005: **125,000**

Portion of Internet files that contain piggybacked spyware: **1 in 20**

Percentage of enterprises that have suffered a cyber attack: **54**

Percentage of organizations that use centralized reporting capability and metrics to describe their current security posture: **89.5**

Number of corporate earning restatements, due to SOX, through October, 2005: **971**

Total projected number of new high-tech jobs in 2006: **217,000**

Percentage of these that contain potentially damaging code, with the greatest accumulation being found in game and celebrity sites: **14**

Odds that the cost of these attacks exceeded \$100,000: **1 in 5**

Estimated number of identity theft or fraud victims, according to the Federal Trade Commission (FTC): **10 million**

Increase in total incidents of malware: **48 percent**

Percentage of **fraud** perpetrators who were **employed** by the victim firm, in North America: **60**

Number of projected total of restatements for 2005: **1,200**

Predicted total compliance spending in 2006: **\$27.3 billion**

Percentage of incidents that allowed outside access to the infected machine: **42**

Odds that a Web site will attempt to load spyware onto a visitor's machine, based on random visits to 20 million Web sites: **1 in 62**

Chance that those perpetrators were **senior managers: 1 in 4**

Decrease in compliance with HIPAA privacy rules in last year: **6 percent**

Drop in cost of Sarbanes-Oxley compliance for larger firms in 2006: **44 percent**

Portion of incidents that resulted in stolen information: **34 percent**

Odds that the IRS has audited or will audit a company in 2005 and 2006: **1 in 5**

Rise in percentage of financial fraud over the last two years: **22**

Percentage of malware that included a keylogger: **16**

Percentage of cyber-attack cases in which damages exceeded \$500,000: **11**



# Privacy, Network Security, and the Law

Robert J. Scott

In the four years since California passed SB 1386, many states have followed suit and enacted similar privacy legislation. This article briefly explores various state privacy rules that currently guide business practices. It also looks at Federal privacy bills currently under consideration, any of which could supersede state requirements and thereby impact corporate security priorities.

## RELATED REGULATIONS

California Senate Bill (SB) 1386

15 USC §1700

Notification of Risk to Personal Data Act (NRPDA) [Pending]

## INTRODUCTION

In the four years since California passed the groundbreaking privacy law SB 1386, many states have followed suit and enacted similar legislation. Many of the regulatory requirements are similar across states; however, the various laws contain somewhat disparate definitions of “personal information.” They also provide for different types of notification after a security breach. This article briefly explores the requirements and variances of state statutes. It also looks at several Federal privacy bills currently under consideration by Congress. Although it is unclear which, if any, of the pending bills will be passed as a national security breach notification law, the requirements of any Federal privacy legislation would supplant existing state laws. In other words, businesses would be required to adapt their practices to the new Federal requirements.

## OVERVIEW OF STATE LEGISLATION

### Definition of Personal Information

The primary element of the privacy breach notification statutes in the various states is the definition of personal information. Generally, any business that possesses the personal information of a resident of a particular state must notify the resident if his or

her personal information has been obtained by an unauthorized individual. Obviously, to determine whether a breach must be reported, it is critical to determine whether information obtained by a hacker qualifies as personal information under specific state statutes.

For instance, in California, personal information includes a person’s first name or first initial and last name, along with one of the following unencrypted pieces of information:

- Social Security number
- Driver’s license number or state identification number
- Account number, credit card number, or debit card number, combined with any password, security code, or access code<sup>1</sup>

The definitions of personal information in Connecticut, Delaware, Florida, Illinois, Louisiana, Minnesota, Montana, Nevada, New Jersey, Rhode Island, Tennessee, Texas, and Washington are identical to California’s definition.<sup>2</sup> Although Indiana’s and Ohio’s definitions of personal information are also identical to California’s definition, the notification statutes in these

states apply only to state agencies.<sup>3</sup> Private businesses are not required by Indiana or Ohio statutes to report security breaches.

Several states include more information in the definition of personal information than California. For example, Arkansas' statute specifies medical information, as well as the items enumerated in the California definition of personal information.<sup>4</sup> Georgia's and Maine's definitions include the data components identified in California's statute, as well as account passwords or other personal identification numbers or access codes, and any items that, even without the first and last names are sufficient to allow an unauthorized person to attempt identity theft.<sup>5</sup> North Carolina's statute also expands the California definition to include passport numbers, debit card numbers, digital signatures, any other numbers or information that can be used to access a person's financial resources, biometric data, and fingerprints.<sup>6</sup> North

On the other hand, businesses generally cannot reduce their reporting onus by requiring customers to waive their notification rights when they sign service contracts. Most privacy breach notification laws stipulate that any attempt to waive the statutory obligations is void, as against public policy. For more information regarding the other components of the state statutes, refer to Figure 1.

### **Notification after Personal Information**

#### **Has Been Breached**

Most of the states that have passed privacy legislation have also followed California's lead when describing the type of notice required for security breaches. The vast majority of states allow written notice or electronic notice provided in accordance with 15 USC § 7001. If the person or business providing the notice demonstrates that the number of affected persons exceeds 500,000 or that the cost of notice would exceed \$250,000, notice may be provided via

electronic mail, via a posting on the person's or business' Web site, or via publication in major statewide media.

Five states—Delaware, Maine, Montana, North Carolina, and Pennsylvania—allow notification

**Businesses generally cannot reduce their reporting onus by requiring customers to waive their notification rights.**

Dakota recognizes date of birth, mother's maiden name, identification numbers assigned by employers, and digital signatures.<sup>7</sup> In New York, "personal information" is defined as "information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." New York requires notification when public information is obtained in conjunction with a Social Security number; driver's license or state identification number; or account number, credit card number, or debit card number, in combination with an associated security code or password.<sup>8</sup>

Businesses that maintain personal information on behalf of clients can significantly reduce both the risk of incurring security breaches and the burden of reporting breaches by encrypting sensitive data. Of the 23 states that have security breach notification laws, only five require notification of a breach of encrypted data.<sup>9</sup>

via telephone, with varying degrees of restriction. For instance, Maine requires companies to maintain a log of telephone notifications; Pennsylvania allows telephonic notice only if the customer can reasonably be expected to receive the notice and it is given in a clear, conspicuous manner; and North Carolina requires that contact be made directly with the affected person.

### **PENDING FEDERAL LEGISLATION**

#### **The Notification of Risk to Personal Data Act**

The proposed Notification of Risk to Personal Data Act (NRPDA) was introduced in the Senate on June 28, 2005 by Senator Jefferson Sessions [R-AL].<sup>10</sup> The bill, which has been approved in committee and is not before the entire Senate, is the legislation currently pending in the Senate that is most like the California statute. The bill would preempt all the state notification laws and require notification if companies experienced a breach of sensitive personal information

FIGURE 1: STATE STATUTES

State	Time to Notify Consumers of a Breach of Personal Information	Civil Penalties for Failure to Promptly Notify Customers of Breach	Private Right of Action	Exemption for Encrypted Personal Information	Exemption for Criminal Investigations or Information Publicly Available from Government Entities	Exemption for Immaterial Breaches (Typically Defined as No Reasonable Likelihood of Harm)
Arkansas	Most expedient time possible, without unreasonable delay	•		•	•	•
California	Most expedient time possible, without unreasonable delay		•	•	•	
Connecticut	Immediately			•	•	•
Delaware	Immediately, in the most expedient time possible, without unreasonable delay	•	•	•	•	
Florida	Without unreasonable delay	•		•	•	
Georgia	Most expedient time possible, without unreasonable delay			•	•	
Illinois	Most expedient time possible, without unreasonable delay		•	•	•	
Indiana	Without unreasonable delay			•	•	
Louisiana	Most expedient time possible, without unreasonable delay		•		•	•
Maine	Most expedient time possible, without unreasonable delay	•		•	•	
Minnesota	Most expedient time possible, without unreasonable delay	•		•	•	
Montana	Without unreasonable delay	•		•	•	
Nevada	Most expedient time possible, without unreasonable delay	•	•*	•	•	
New Jersey	Most expedient time possible, without unreasonable delay			•	•	•
New York	Most expedient time possible, without unreasonable delay	•				
North Carolina	Without unreasonable delay	•	•		•	•
North Dakota	Most expedient time possible, without unreasonable delay			•	•	
Ohio	Most expedient time possible, but not later than 45 days	•			•	•
Pennsylvania	Without unreasonable delay	•		•	•	
Rhode Island	Most expedient time possible, without unreasonable delay	•	•	•	•	•
Tennessee	Most expedient time possible, without unreasonable delay		•	•	•	
Texas	As quickly as possible	•			•	
Washington	Most expedient time possible, without unreasonable delay		•	•	•	•

\* The privat

that resulted in a significant risk of identity theft to any individual. Notification would have to be made as expeditiously as possible and without unreasonable delay.

NRPDA's definition of sensitive personal information differs slightly from that of most states. According to the bill, "sensitive personal information" includes an individual's first and last name; their address or telephone number; and their Social Security number, driver's license or state identification number, financial account number, credit or debit card number, and any required security or access code or password. Like many state laws, NRPDA excludes publicly available information and encrypted information from its definition of sensitive personal information. Similarly, notification is not required if it would impede a civil or criminal investigation.

Under NRPDA, notice could be issued in writing; by telephone or e-mail; or, under certain circumstances, as a posting on the Internet or media alert. If more than 1,000 individuals are affected, companies would also be required to tell consumer credit reporting agencies how many individuals had been impacted and how those individuals would be notified.

The most significant differences between the state security breach laws and NRPDA are the enforcement provisions. Violations of NRPDA would be enforced by the "functional regulator"; that is, the regulating entity for the type of agency or business that violated NRPDA's provisions. For example, if an insurance agency violated NRPDA, the state insurance authority would enforce the provisions; if an air carrier failed to comply, the Secretary of Transportation would be the functional regulator. State attorneys general could also bring actions in federal court for violations of NRPDA. Individuals whose information was affected by a data breach would be barred under NRPDA from seeking legal remedy.

### **The Identity Theft Protection Act**

The proposed Identity Theft Protection Act (ITPA) is currently pending in the Senate.<sup>11</sup> It was introduced on July 14, 2005 by Senator Gordon Smith [R-OR] and is scheduled for debate at the time of this writing. The ITPA expressly preempts all state and local laws governing security breach notification. The current

version of the bill would require that, when a breach was discovered, a covered entity notify the Federal Trade Commission (FTC). Under some circumstances, it would also require notification of credit reporting agencies and affected consumers.

Within the bill, "covered entity" is defined as "a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization that acquires, maintains, or utilizes sensitive personal information."

The bill's definition of "sensitive personal information" in the ITPA is similar, but not identical to, California's definition. Sensitive personal information is described as an individual's name, address, or telephone number, combined with one or more of the following pieces of information:

- Social Security or other taxpayer identification number
- Financial account number, credit card number, or debit card number, combined with the required security code, access code, or password
- State driver's license identification number or state resident identification number

Unlike the state laws, ITPA would require companies to notify various agencies based on the number of individuals affected by a data breach. If 1,000 or more individuals were affected by a breach, the covered agency would have to report the breach to the FTC and all of the consumer credit reporting agencies. If fewer than 1,000 individuals were impacted and if the covered entity determined that the breach did not create a reasonable risk of identity theft, the covered entity would be required to report the breach to the FTC, but not to the consumer reporting agencies.

Regardless of the number of people affected, covered entities would also be required to notify consumers of the breach if there was a reasonable risk of identity theft. Notification pursuant to this provision would have take place in the most expedient manner practicable, but not later than 45 days after the date the breach was discovered by the covered entity.

To determine whether there was a reasonable risk of identity theft, covered entities would need to consider a number of factors. The proposed legislation requires covered entities to evaluate whether the compromised data contained sensitive personal information usable by an unauthorized third party and whether the data was in the possession and control of an unauthorized party likely to commit identity theft. The notice provisions related to consumers are very similar to state requirements: a written or electronic notice and substitute notice under certain circumstances.

Like the majority of state laws, ITPA would not require covered entities to notify consumers of a breach if that notification would materially impede a civil or criminal investigation or threaten national security. ITPA would be enforced by the FTC, as well as other relevant federal agencies (e.g., the Securities and Exchange Commission would have power to enforce the ITPA with respect to broker/dealers). Although civil penalties are allowed by ITPA, the law provides no private right of action.

### **The Personal Data Privacy and Security Act**

The Personal Data Privacy and Security Act (PDPSA) is also currently pending in the Senate. It was introduced on September 29, 2005 by Senators Arlen Specter [R-PA], Russell Feingold [D-WI], Dianne Feinstein [D-CA], and Patrick Leahy [D-VT].<sup>12</sup> The bill has been sent by the committee to be considered by the entire Senate. The PDPSA would not apply to financial institutions, entities covered by HIPAA or the Gramm-Leach-Bliley Act, or any business that qualifies for exemption under the Safe Harbor provision. The Safe Harbor provision exempts businesses that provide protection equal to industry standards, as identified by the FTC.

All other agencies or business entities engaged in interstate commerce that used, accessed, transmitted, stored, disposed of, or collected sensitive personally identifiable information, would be required to notify any resident of the United States whose information had been, or was reasonably believed to have been illicitly accessed or acquired. This notification would

have to be provided without unreasonable delay. According to PDPSA, sensitive personally identifiable information is defined as an individual's first name or first initial, their last name, and:

- A non-truncated Social Security number, driver's license number, passport number, or alien registration number
- Two of the following:
  - Home address or telephone number
  - Mother's maiden name
  - Complete birth date
- Fingerprint, voiceprint, retina or iris image, or any other unique physical representation
- A unique account identifier, electronic identification number, user name, or routing code, in combination with any associated security code, access code, or password

**Businesses would not have to follow the notification provisions if a risk assessment indicated no significant risk of harm to the individuals.**

Additionally, sensitive personally identifiable information could include a financial account number, credit card number, or debit card number, "in combination with any security code, access code, or password that is required for an individual to obtain money, goods, services, or any other thing of value."

The notification provisions would not apply to government agencies that could certify in writing that notification might hinder an investigation or cause damage to national security. Businesses would not have to follow the notification provisions if a risk assessment indicated no significant risk of harm to the individuals represented by the compromised data. Moreover, businesses would be required to notify the Secret Service of the results of a risk assessment without unreasonable delay but not later than 45 days after a breach. Businesses would also be required to notify the Secret Service of their intent to invoke the



risk-assessment exemption. The Secret Service would have 10 days to compel businesses to provide notice.

Businesses required to disclose security breaches under the PDPSA would have to provide individual notice and media notice. The individual notice requirements would be satisfied by providing written notice, telephone notice directly to the affected individual, or e-mail notice if the individual consented to receive such information through the e-mail channel. Additionally, if more than 1,000 individuals stood to be impacted by the breach, the agency or business would need to notify all consumer credit reporting agencies.

The agency or business would need to give notice of the security breach to the Secret Service if the number of individuals affected exceeded 10,000, if the breached database contained sensitive personally identifiable information of more than 1,000,000 individuals, if the breached database was owned by the federal government, or if the sensitive personally identifiable information was that of federal government employees or contractors.

Like the ITPA, the PSPDA would preempt all state laws requiring security breach notifications. The proposed legislation expressly prohibits private causes of action for injuries related to security breaches, but it does provide for civil penalties in actions instituted by the Attorney General.

#### **The Financial Data Protection Act**

The proposed Financial Data Protection Act (FDPA) was introduced on October 6, 2005 by Representative Steven LaTourette [R-OH] and 14 co-sponsors.<sup>13</sup> This bill has not made it out of the House committee. Most bills do not progress from committee to the entire House. If passed, this legislation would also preempt all state security breach notification laws.

The FDPA would amend the Fair Credit Reporting Act, requiring consumer reporters to investigate potential breaches of sensitive personal information. The bill defines “consumer reporter” as “any consumer reporting agency or financial institution or any person which, for monetary fees, dues, on a cooperative

nonprofit basis, or otherwise regularly engages in whole or in part in the practice of assembling or evaluating consumer reports, consumer credit information, or other information on consumers.”

Under the bill, sensitive financial personal information includes a financial account number combined with an associated access, security, or biometric code or other password or personal identification information. It also includes an individual’s first and last name, address or telephone number, and either a Social Security number, driver’s license or identification number, or taxpayer identification number.

If the breach could result in substantial harm or inconvenience to any consumer to whom the information related, the consumer reporter would be required to promptly notify:

- The Secret Service
- The appropriate regulatory agency
- Any entity that owned or was financially obligated on an account that might be subject to unauthorized transactions as a result of the breach
- Each national consumer reporting agency, if the breach involved 1,000 or more customers
- Any appropriate critical third party

Consumer reporters would also have to provide notice to consumers if there is a breach that results in a reasonable probability that personal information may be misused. This notice must be made without unreasonable delay. If requested, the consumer reporter must provide free credit monitoring services to consumers for six months. Consumer reporters could delay notice if notice would impede a current civil or criminal investigation. The functional regulatory agencies would be responsible for enforcement of the FDPA.

#### **The Data Accountability and Trust Act**

The proposed Data Accountability and Trust Act (DATA) was introduced on October 26, 2005 by Representative Clifford Stearns [R-FL] and eight cosponsors.<sup>14</sup> It is currently under review by committee and would preempt state laws.

DATA would require any person or company engaged in interstate commerce to report a breach of security to every individual whose personal information was acquired by an unauthorized source, notify the FTC of the breach, place a conspicuous notice on its Web site, and notify the financial institution that issued the individual's breached account (if applicable). Notification could not follow unreasonable delay. The company could notify individuals of the breach in writing or via electronic mail, and the proposed law would also allow substitute notification if certain criteria were met.

For purposes of DATA, personal information is defined to include an individual's first and last name and any one of the following:

- Social Security number
- Driver's license number or other state identification number
- Financial account number, credit card number, debit card number, and any required security code, access code, or password

This proposed legislation would require that the company also provide a free copy of the exposed individuals' credit reports from at least one major credit reporting agency.

The FTC would enforce violations of DATA. Although the bill would preempt state notification laws, it specifically excludes from preemption actions based on state trespass, contract, and tort laws as well as other state laws relating to acts of fraud. In other words, if this legislation were enacted, individuals might be able to seek redress under state law for injuries resulting from unauthorized disclosure of their personal information.

#### **THE NEW STANDARD OF CARE—HOW TO AVOID LIABILITY**

Security breaches can be costly. In the past several months, the FTC has investigated and sanctioned several companies for lapses in security involving customer information. For instance, Superior Mortgage Company was accused of misrepresentation by the FTC after the agency found that reportedly encrypted data

was actually decrypted before the company transmitted it via e-mail to its headquarters.<sup>15</sup> Superior Mortgage agreed to refrain from making misrepresentations and submitted to FTC monitoring for 10 years.

The retailer DSW was sanctioned for storing unencrypted files that were easily accessed using a commonly known user name and password. DSW agreed

This proposed legislation would require that the company also provide a free copy of the exposed individuals' credit reports from at least one major credit reporting agency.

to implement comprehensive security measures and submit to FTC compliance monitoring for 20 years.<sup>16</sup>

ChoicePoint, a data warehousing company, agreed to pay \$15 million in fines and restitution and allow 20 years of monitoring after it provided sensitive personal information to subscribers who did not have a permissible purpose.<sup>17</sup>

Based on the current state laws it is clear that businesses should, at the very least, ensure that all names, addresses, account numbers, and other personal information of consumers is encrypted. This will minimize the risk that the business will have to notify consumers or law enforcement agencies should a breach occur. Until federal legislation is enacted, businesses must also be aware of the different requirements of various state laws governing the protection of data. Companies should regularly consult with attorneys regarding requirements in the relevant jurisdictions. Ensuring compliance with the statutes governing the storage of information will also decrease the risk of liability.

Although many state laws do not allow private causes of action based on the security breach laws, other claims based on breach of contract, misrepresentation, or negligence might not be precluded. For example, consumers in many states can file lawsuits against

companies whose security was breached, claiming that the companies negligently stored or protected the information. In addition to being diligent about data protection, companies should also to review their contracts and sales materials to ensure that, in addition to meeting statutory requirements, they are also fulfilling all of the promises they have made to customers regarding data protection.

## CONCLUSION

Until federal legislation creates a uniform standard and possibly prohibits private causes of action for security breaches or notifications thereof, businesses must constantly familiarize themselves with the ever-evolving notification requirements for each state in which they do business. With diligent efforts, companies can reduce the possibility of liability for breaches in security.

## NOTES

1. Cal. Civil Code, § 1798.82(e)
2. Connecticut General Statutes § 36a-701b(a); 6 Delaware Code § 12B-101, Florida Statutes § 817.5681(d)(5); 815 Illinois Compiled Statutes § 530/5; Louisiana Revised Statutes § 51:3073(4); 10 Maine Revised Statutes § 1347(6); Minnesota Statutes § 325E.61(e); Montana Statutes § 30-14-1704(4)(b); Nevada Revised Statutes § 603A.040; New Jersey Statutes § 56:8-161; 73 Pennsylvania Statutes § 2302; Rhode Island General Laws § 11-49.2-5(c); Tennessee Code § 47-18-2107(a)(3); Texas Business & Commerce Code §§ 48.002, 48.103; Washington Revised Code § 19.255.010(5)
3. Indiana Code § 4-1-11-3; Ohio Revised Code § 1349.19(A)(7)
4. Ark. 4-110-103
5. Georgia Code § 10-1-911(5), 10 Maine Revised Statutes § 1347(6)
6. North Carolina General Statutes §§ 75-61(10), 14-113.20(b)
7. North Dakota Statutes § 51-30-01(2)(a)
8. New York General Business Law § 899-aa(1)(a)-(b)
9. Louisiana, New York, North Carolina, Ohio, and Texas have enacted statutes that require notification, even if the personal information data is encrypted
10. Notification of Risk to Personal Data Act, S.B. 1326, 109th Cong. (2005)
11. Identity Theft Protection Act, S.B. 1408, 109th Cong. (2005).
12. Personal Data Privacy and Security Act, S.B. 1789, 109th Cong. (2005)
13. Financial Data Protection Act, H.R. 3997, 109th Cong. (2005)
14. Data Accountability and Trust Act, H.B. 4127, 190th Cong. (2005)
15. In the Matter of Superior Mortgage Corporation, FTC Docket No. C-4153 (December 14, 2005)
16. In the Matter of DSW, Inc., FTC Docket No. C-4157 (March 7, 2006)
17. United States v. ChoicePoint, 1:06-CV-0198 (N.D. Ga. 2006)

## AUTHOR BIO

Robert J. Scott is the managing partner of the legal and technology services firm Scott & Scott, LLP. Contact him at [rjscott@scottandscottllp.com](mailto:rjscott@scottandscottllp.com).

# Governance: A Business Intelligence Best-Practice Case Study

Beth Leonard

When a corporate IT assessment revealed that business and IT efforts were severely hampered by lack of clear, stable governance structures, the company developed a sophisticated BI program to address its challenges. The program generated a two-year ROI of almost 700 percent and became a testing and learning ground for developing and executing a corporate governance process.

## RELATED REGULATIONS

Sarbanes-Oxley Act

Telecommunications Act of 1996 (US)

The Communications Act 47 USC § 151 et seq.

### THE BUSINESS PROBLEM

The idea of business “governance” first began to emerge back in the mid-1990s, as companies sought ways to better utilize technology for business process improvement and competitive advantage. The company described in this case study identified governance as one of the key enablers for aligning its business and IT domains in order to accomplish that goal. The company’s recognition of the importance of governance first surfaced in an IT strategic planning study and was initially identified and tested as a critical success factor to its business intelligence (BI) program. The company’s implementation of BI governance, while not without challenges, would clearly be considered a governance best practice today.

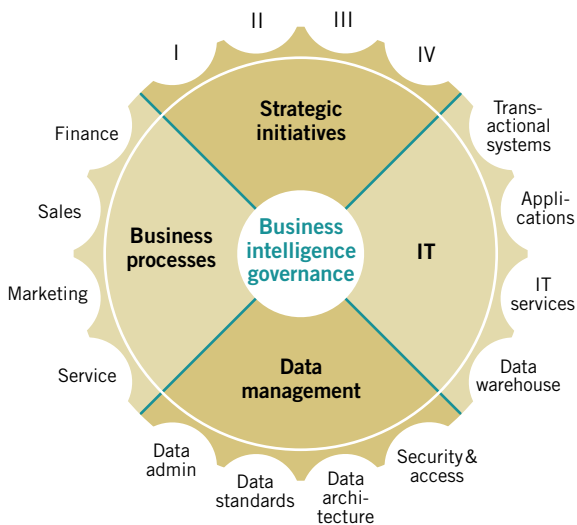
The following statement describes one of the outcomes of the IT assessment undertaken by the company: “IT efforts are severely hampered by lack of clear, stable governance structures.” The report went on to describe the current state as follows:

- Unclear roles and responsibilities. This results in poor decision-making, lack of accountability, lack of business domain buy-in, and insufficient sharing of data and solutions across the organization.

- Ineffective processes to communicate strategic business opportunities to IT. This limits IT’s ability to understand business needs and be proactive. It limits business’s ability to understand IT constraints. Together, this insufficient planning generates a backlog of requirements, obsolete infrastructure, and discouraged users.
- Complex, ineffective funding process. Business has little knowledge or control of IT priorities and investments. Lack of cross-functional coordination results in ineffective use of resources. The annual funding process does not quickly adapt to changing business needs and priorities.
- Limited value tracking and results reporting. Ineffective feedback mechanisms and lack of formal measurement systems convey neither benefits achieved nor drive accountability. Executive sponsorship, continuous improvement, and change management opportunities are lost.

The executive mandate was clear: “Fix it.” At the time, this company was still in the very early stages of planning its first data warehouse (DW). The BI program took on a microcosmic character of the larger corporation and IT department. It became the corporate

**FIGURE 1: BI GOVERNANCE VIEWS—  
THE CORPORATE BIG PICTURE**



testing and learning ground for developing and executing a governance process.

### THE DESIRED STATE

The first step was to define BI governance and establish the goals. A BI governance team composed of the BI program director and middle managers from the business units crafted a definition similar to the one below:

Governance is the decision-making and oversight process that prioritizes investments, allocates resources, and monitors results to ensure the business intelligence (BI) program is aligned with corporate objectives, produces desired business actions and behaviors, and creates value.

The team then outlined the following BI governance goals:

- Link all BI projects to strategic corporate initiatives and IT value drivers
- Provide BI capabilities that reach multi-functions for multi-purposes
- Ensure user adoption
- Deliver tangible value, on-time and on-budget
- Develop business insights and manage for continuous improvement

### THE ACTION PLAN

The BI governance team launched a five-step execution plan.

#### 1. Position BI governance as a core management competency

This step required demonstrating how BI governance fit into the big corporate picture and then defining data as a strategic business asset. The team used the company's budgeting process as a model. The corporate budgeting process engaged executives from across the business and IT functions at strategic roundtables to set priorities, allocate budget dollars, track program results against business case projections, and identify and resolve issues.

BI governance used and enhanced this roundtable model to fit BI specific requirements. BI governance needed to take a broader perspective than the strategic roundtables, each of which focused on a specific initiative and associated processes, organizations, programs, and technology. BI governance aligned its program and prioritized its projects against all strategic initiatives, as well as existing processes and their ongoing needs for business analytics.

A key issue was how to balance the plethora of business needs with the rigor and constraints of IT. The team had to prioritize data and applications delivery to optimize their strategic benefits while satisfying the greatest number of users at a time. In making data available to users for reporting and analysis, the BI team also had to consider data management issues, such as corporate data standards and source-system data quality. In other words, the BI program had the potential to touch every strategic initiative, every business process, many of the IT systems, and much of the corporate data. The scope and complexity of its task required the BI governance team to understand and influence the corporate big picture. Governance was the linchpin to coordinate the requirements and constraints of the information demand-and-supply chain.

#### 2. Establish joint business and IT decision-making and oversight

The BI governance team recognized that their operating model needed to represent the varied interests from



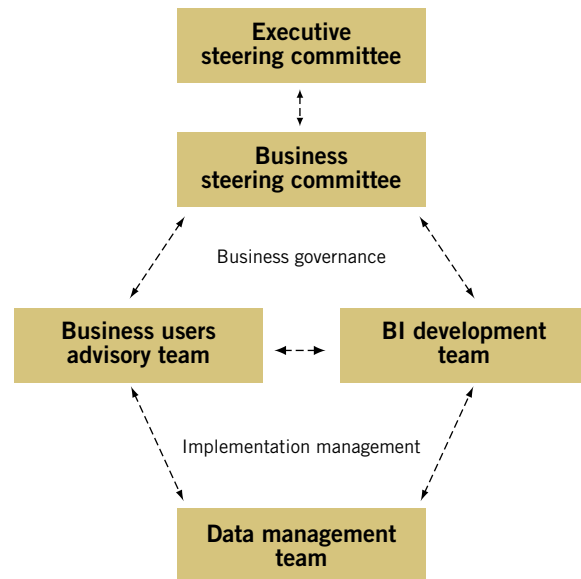
the business processes, IT, and data management. The team needed to operate and interact at multiple levels of the organization—executive management, middle management, and work groups. As such, BI governance could not exist on an organization chart. It was not a hierarchy, but an interaction system. The team developed a governance system in which the decision-making bodies functioned as three-legged stools. This arrangement created an interactive and mutually supportive relationship of checks and balances between the business steering committee, business users advisory team, the BI/DW development team, and the data management team.

The governance bodies met quarterly to make decisions on the application portfolio, share insights from data analysis and business actions, and receive performance reports. They met monthly to review project status, identify issues, and discuss options for resolution. They used subteams to work through details and bring back recommendations. Roles and responsibilities, knowledge categories, and skill sets were defined for each team member. BI governance responsibilities were included in job descriptions and performance commitments. Individuals were further incented to participate through both internal recognition and cash bonuses, based on program achievement. It became highly prestigious to be selected to sit on the BI governance team.

The Business steering committee was composed of vice presidents and senior directors from the major business functions—marketing, sales, product development, finance, strategic planning, and IT. Their job was to approve project funding, monitor project status, and remove roadblocks. They set policy, communicated program value, and championed culture change.

A business users advisory team was designed to represent the interests of the end users and support the steering committee. These subject matter experts were directors and managers whose primary job was to carry out tactical execution of strategic initiatives in their departments. In this role, they were directly linked to corporate strategy, responsible for explaining performance indicators, and keenly aware of information gaps and user needs. They reported

FIGURE 2: BI GOVERNANCE TEAM



directly to senior executives and therefore played an important advocacy role as influencers and change agents for the BI program.

The BI development team established a close working partnership with the business users advisory team by assigning a business analyst to each individual. Together, the teams defined the BI program vision, processes, and success metrics—essentially the governance mechanisms. They collected user input for candidate applications, developed business cases, and prioritized the pipeline of work requests. They aided the decision-making work of the business steering committee by advocating for the users and managing the inputs and outputs associated with the governance mechanisms.

The data management team was a working member of the BI development team. Data management team members performed functions such as data administration, data modeling, data profiling, and metadata management. The team included data stewards from both business and IT. This team also worked across the IT organization and the source systems in data error detection and correction. The data management team played a key role in resolving “data gaps” for the BI program. Resolution

sometimes required significant process change or legacy system enhancement. In one case, the team corrected inconsistencies in a decades-old definition of “telephone access line.” Their work resulted in changing the way business processes used “access line”

During the first portfolio review, the BI governance team was able to consolidate nearly 50 standalone projects for a development cost savings of \$10 million.

data for forecasting equipment expansion, servicing customer accounts, and reporting revenues. In another example, the team established data quality processes that affected the assignment of customer identifier codes used to indicate members of the same household. They boosted accuracy of customer identifier codes used for direct mail campaigns from less than 60 percent to more than 80 percent.

### **3. Implement a BI portfolio management approach to investment**

The BI governance team created a new method with its portfolio approach to BI investment and resource management. Their message was that BI would be managed as an ongoing program and not as a project. This fundamental principle established a foundation for collecting, evaluating, and prioritizing business needs according to predefined criteria. These criteria included strategic importance or criticality, financial value, reach or quantity of users impacted, dependencies, and do-ability. Application requests were broken into short, iterative projects of three to four months. Business cases were developed for each request and actual results were tracked against projected costs and benefits. The portfolio was reviewed quarterly and reprioritized, when necessary, to reflect changing business needs.

In addition to being a prioritization tool for the BI governance team, the portfolio was also an input mechanism to the annual budgeting cycle. The

portfolio was subdivided into three budget categories: new development, maintenance and enhancement, and program infrastructure. Maintenance and infrastructure costs were distributed across business functions.

New development costs were assigned to the primary requesting organization, with some allocation to secondary beneficiaries.

Managing by portfolio provided all stakeholders an opportunity to advocate for their needs and to understand exactly how the funding decisions would be made. The portfolio provided a plan that enabled IT to coordinate resource availability and determine skill sets

in advance. It provided business users with advance knowledge of where their needs stood in the queue. And it reduced overall development and maintenance costs by consolidating duplicate projects. During the first portfolio review, the BI governance team was able to consolidate nearly 50 standalone projects for a development cost savings of \$10 million.

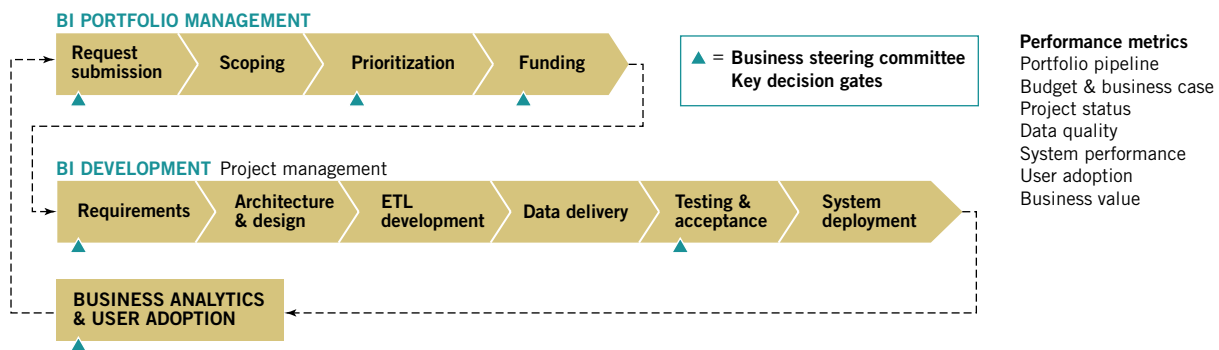
### **4. Use a gated decision-making process**

The BI governance team identified critical decision points in the program cycle that they called “gates.” They reviewed program status at each gate to make a “go/no go” decision about whether the project should move forward and whether additional resources should be invested.

Decision gate reviews provided a forum for addressing issues and problems before they became show stoppers. Each decision gate also carried performance metrics, which the team used to track and report program success. At each gate the team had the opportunity to review the program and its individual projects within the context of an ever-changing business and technical environment. They continually assessed both short-term and long-term value propositions.

Decision gates fell into three categories: the application portfolio, the development project, and user adoption. The team established a predefined set of criteria that an application or project needed to meet to pass through the gate. For example, if a

FIGURE 3: BI GOVERNANCE DECISION GATES



request for application development entered the portfolio pipeline, to pass the first gate it would have to be linked to a strategic initiative or offer a compelling value proposition (e.g., revenue, cost reduction, productivity, customer intimacy). It would also need an executive sponsor willing to fund development. To pass the second gate, the request would undergo a scoping process to determine the feasibility of investing in development. The team would assess whether data and technology existed to support the application. If not, could it be acquired and at what cost? Would there be resource impacts? Was the request practical, in terms of dependencies and timing? Could the request be accomplished in project intervals of three to four months?

The user adoption gate provided both a current view of BI usage and a feedback loop to identify future opportunities. What percentage of the targeted audience was actually using the application? What was their satisfaction index? Was the application delivering the data and technical performance expected? What were the business actions taken and insights derived? Did the application produce the benefits forecasted by the business case? What needed to be improved in the BI program?

The decision-gate approach utilized the variety of skills, knowledge, and interests of the BI governance team as it addressed multiple business and technology issues. It ensured that the steering committee remained focused on overarching business issues rather than being dragged into technical details and development-

cycle tasks. Subcommittees were used to provide input and act as subject matter experts, work through the details of issues, bring forth recommendations, and advocate for the interests and needs of their particular areas. Clear distinctions were made between governing and managing, or stated another way, between doing the right things versus doing things right.

### 5. Communicate the BI governance implementation roadmap

The BI governance team recognized that they were introducing a new way of working to the company and undertaking the role of change agents. They also recognized that change is fundamentally a social process requiring open, consistent, and ongoing communications. To accomplish this, the team built and published their governance plan, or implementation roadmap, and regularly communicated progress throughout the corporation. The roadmap covered the following categories:

- Purpose and scope
- Organization—committees, members, roles and responsibilities, and schedules
- Process and decision gates
- Performance measures
- Escalation and exceptions policies
- Templates, tools, and materials
- Communications plan

The governance roadmap communicated to stakeholders what the governance process was, how

it would work, how success was defined, and who was involved. It mapped out a very tactical set of activities to be developed and introduced over the course of a year. The roadmap essentially became the BI governance team's "performance commitment" to the corporation.

## RESULTS

The BI governance team created a highly interactive partnership between the business and IT domains and across the stakeholder groups. They established a 360-degree governance feedback loop that ran from planning to execution, results analysis, and sharing insights. This learning environment advanced organizational knowledge and subsequently translated into improved business processes and new initiatives. The governance structure and decision-making processes created a clear path of accountability for delivering results.

Within two years the BI program was managing multiple projects in parallel and releasing a deliverable every 4 to 6 weeks. Projects were consistently on time and on budget. The collaborative decision-making process enabled the company to leverage BI to automate inside sales processes, reengineer product development, and align capital expenditures with target market opportunities. When the company tallied the results of its BI program, the two-year ROI was nearly 700 percent—a tangible result that they attribute to the strength of good governance.

## LESSONS LEARNED

- Governance encompasses more than policies, rules, and standards. It must also deal with the social system, or behavioral side, of decision-making—relationships, interactions, attitudes, thinking, and learning.
- Governance cannot be defined by organization or hierarchy. It blends people and functions from across the corporation into a dynamic and interconnected teaming model based on common goals and collaboration.
- Governance needs to be actively designed. It doesn't just happen. The very process of design enables the team to build commitment, cement

relationships, and think through BI processes and decision-making scenarios.

- Governance design should reflect a top-down view of enterprise needs. This ensures executive sponsorship and maintains the right decision-making focus at the appropriate management level. It creates linkages to strategy, processes, corporate data management, and IT.
- Governance is about leadership and change management. It takes vision, requires clear communications, manages expectations, and demands accountability. It also takes time to change the way people think and work and to institutionalize a new process.

### BIO

Beth Leonard is a consultant at Baseline Consulting. Prior to joining Baseline, Beth worked for Fortune 100 companies as executive sponsor of business intelligence and data warehousing programs, where she implemented BI governance, led marketing departments, and directed strategic initiatives such as CRM. Contact her at [bethleonard@baseline-consulting.com](mailto:bethleonard@baseline-consulting.com).

# A Best-Practices Approach to Leveraging Control Frameworks for Compliance and Risk Management

R. Andrew Brice, CISA, CISSP

This article provides a best-practices approach by which IT managers can illustrate the value of IT control activities for business and compliance. Addressing strategy, solutions, and resources, this approach includes a logical roadmap by which IT managers can address not only compliance challenges, but also the formidable hurdles of communicating the need for compliance investments to business stakeholders.

## RELATED REGULATIONS

Sarbanes-Oxley Act

Basel II Revised  
International Capital  
Framework

Gramm-Leach-Bliley Act

US Code—Title 12:  
Banks and Banking

IT job descriptions have traditionally been defined by specific IT control objectives and activities. Individuals' contributions were generally quantified and measured over the course of a year and those measurements were translated into activity-related reports and metrics used within the IT environment to illustrate progress.

More recently, complex “best practices” frameworks have emerged to effectively organize IT control objectives and their associated activities into hierarchical models. Of course, no law actually mandates the use of a control framework; however, the increasing acceptance of CobiT and other IT-oriented frameworks externally validates IT responsibilities within an organization. In the IT industry, this is familiar to those involved in operations, auditing, and consulting.

Indeed, business needs drive the implementation of IT frameworks. As business and technology functions grow, they tend to integrate. The resulting interdependence promotes greater transparency in business processes, and increases the value of both IT and business process.

The Internet is one of the best examples of this type of technology evolution. Originally, it was developed for military purposes; later, it was used to share information within the educational community. Today, more than 30 years later, people can use the Internet to open bank accounts, pay bills, buy concert tickets, and even make long-distance phone calls. The Internet is an example of a purpose-built technology that—under the influence of time, technological development, and market pressures—developed into a system with far more business value and utility than its original plan envisioned.

The same type of technology evolution can be fostered in business as well. Fortunately, many companies are now realizing more business value from their IT investments. By implementing a best practices framework that considers IT activities, annual business objectives, and job descriptions, companies can obtain many benefits, including:

1. Leveraging years of individuals' experience in developing IT best practices



2. Creating a picture of value within a commonly accepted and recognized framework
3. Reducing or eliminating the duplication of IT design and implementation efforts involved in addressing new compliance and regulatory initiatives

Like the Internet in the 1990s, the evolution of the IT industry requires clearer integration and connection of its activities with business interests. This paper presents a particular best practices (BP) strategy for achieving this goal. This BP approach has the potential to dramatically increase the transparency between IT activities and business goals.

Why, what, and how are the three cornerstones used in the BP approach to measure and map IT activities to the business. There is a clear relationship between the three. *Why* is the reason for the IT activity. *What* represents the actions that need to be performed. *How* represents the steps, products, or services that facilitate those actions.

#### **WHY?**

One of the first questions you should ask about any proposed IT effort is “Why?” Identifying the business rationale for an IT activity helps identify and clarify the primary driver and benefit of IT efforts.

Accordingly, it’s reasonable to ask why a best practices approach should be adopted. In addition to the benefits already mentioned, the BP approach illustrates the benefits of fulfilling compliance with external laws and regulations, such as Sarbanes-Oxley (SOX) reporting requirements. Tying relevant IT activities to a comprehensive IT control framework intrinsically addresses internal audit expectations. It also creates business value, since standardized control efforts, based on best practice frameworks, can generally be leveraged and reused, thus averting duplication of effort.

An increasing number of vendors are proactively “mapping” products and services to IT frameworks. Within the next few years, product and service mapping to IT frameworks could actually become standard. Vendor solutions that integrate widely recognized best practice frameworks will not only

enable vendors to more easily define their value to business and compliance managers, but also ease the burden of solution implementation and process integration for IT operations.

Finally, there are likely to be benefits specific to your situation. Consider these questions:

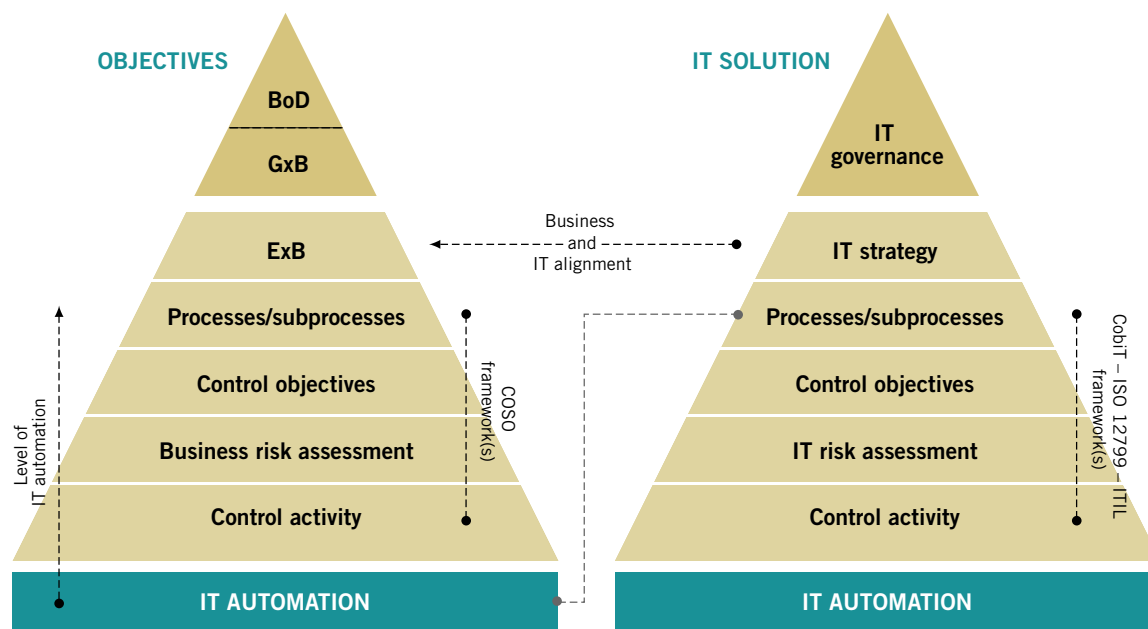
- What IT activities will meet SOX or other external compliance requirements?
- What IT activities will meet internal auditors’ expectations?
- How can you leverage current internal or external compliance efforts?
- How can you ensure thorough consideration of job requirements?
- If you’re a vendor or consultant, how can you use best practices concepts to better illustrate that your products or services are providing value to your clients?

The answers to these questions will point to value opportunities and ways in which a best practices approach to compliance can substantially reduce the costs while increasing ancillary benefits.

#### **WHAT?**

Which controls should be in place to address compliance and the other business goals? There are many papers, standards, and frameworks available that can help you determine which controls you should consider (see Compliance Bibliography, page 36). Adopting (or developing) an anchor framework of standardized IT controls is a sound business and IT practice.

One of the first questions you should consider when evaluating the use of a best practices framework is whether your organization will benefit more by adopting an established framework and modifying it to suit organizational needs, or whether it would be more efficient to develop a customized solution from scratch. Both options have unique advantages and costs. The option selected should reflect the size and complexity of the organization, the availability of implementation resources, managerial expertise, and so on.

**FIGURE 1: BUSINESS OBJECTIVES AND IT SOLUTIONS**

The following is a sample list of commonly adopted IT control frameworks. Although some are more comprehensive than others, each can serve as a structured checklist of what to consider and cover within the organization:

- Control Objectives for Information and related Technology (CobiT)
- International Standards Organization (ISO/IEC 17799:2005)<sup>6</sup>
- IT Infrastructure Library (ITIL)<sup>7</sup>
- Microsoft Operational Framework (MOF)—based on ITIL
- Capability Maturity Model Integration (CMMI)
- Standard of Good Practice (SoGP)
- National Institute of Standard and Technology (NIST)

The BP approach discussed in this paper focuses on CobiT. With its close ties to SOX, broad scope, and target audience of business, managers, users, and auditors, CobiT is a logical framework for compliance efforts. SOX requirements alone have increased the popularity of CobiT, which correlates directly to the COSO Enterprise Risk Management framework. Since COSO is explicitly recommended by SOX regulators,

CobiT has naturally become the most widely adopted IT framework for SOX compliance.

If you are already using another framework, such as the ISO17799 or ITIL and you want to use CobiT, don't worry: these standards are not incompatible. CobiT's publisher, the Information Systems Audit and Control Association (ISACA), provides mapping and relationship information between CobiT and other popular IT control frameworks. Mapping CobiT controls to other implemented frameworks within your company is a fundamental efficiency with many downstream benefits, such as the elimination of redundant and incompatible development and processes and the ability to consistently implement standardized control processes to meet emerging compliance or risk-management goals.

How do compliance and regulatory requirements relate to CobiT and other IT frameworks? Most regulatory requirements involve a request from an auditor, compliance officer, or legal department to ensure that proper controls are in place. Frameworks such as CobiT act as control checklists that you can use to meet regulators' expectations. Moreover, since frameworks provide a standardized list of control

objectives, they can help you cross-reference internal and external regulatory requirements. Finally, because many frameworks offer more robust processes than are required by any given law, they can increase your compliance coverage and ability to meet current and future regulatory requirements.

### HOW?

How can you correctly implement the proper controls to fulfill business goals and compliance requirements? To properly address this question, you must first understand the relationship between business and IT.

On the business side, processes are defined to achieve the business plan, objectives, and goals. IT helps business units achieve their goals. As business relies more heavily on IT, it is the responsibility of IT to build transparency and value into business systems. Yet the risk associated with the business goals generally remains the responsibility of business. To address this risk and maintain a balance between business needs and the value associated with an IT solution, IT risk management is increasingly recognized as a key part of the larger risk-management picture. Pragmatic IT risk mitigation options provide a more precise IT solution to support business needs without over-engineering.

A pragmatic IT risk mitigation option can be reached using a defined and implemented IT risk management approach. Such an approach will ensure consistency across the IT organization, whatever its size, location, or cultural challenges.

Where should IT risk management begin? Again, business can either adopt an established framework for managing IT risk or build their own customized framework from scratch.

The IT risk management methodology used in the BP approach is based on the framework for Management of Risk<sup>5</sup> (MoR), developed by the UK Office of Government and Commerce (OGC)<sup>6</sup>. It is a model to guide business and IT managers through the proper identification, acceptance, mitigation, and monitoring of risks to the business. Within the OGC methodology, the nine stages of risk management are:

1. Define a framework
2. Identify the risks
3. Identify probable risk owners
4. Evaluate the risks
5. Set acceptable levels of risk
6. Identify suitable responses to risk
7. Implement responses
8. Gain assurances about effectiveness
9. Embed and review

The first stage, defining an IT control framework, includes identification of relevant standards and policies. This is where IT control frameworks can be leveraged to your advantage.

All nine stages of the OGC risk management methodology are integrated and described in more detail through the execution of a roadmap that is also integral to the BP approach. This roadmap, designed and developed by R. Andrew Brice, can ease the transition from theoretical risk-management concepts to practical application. It is organized into five phases, each containing specific activities. Figure 2 illustrates each phase and its execution within the roadmap.

The roadmap has five phases: identification, cross-reference, risk analysis, risk mitigation, and evaluation.

### PHASE 1: IDENTIFICATION

#### Step 1: Identify the organization and its business goals, objectives, and processes

Mapping and illustrating the value of IT to business depends on your ability to link IT control activities and relevant business goals. CobiT 4.0 provides a list of 20 business goals, categorized and linked to IT goals and processes, that you can use as a template or foundation for your own mapping efforts.

Although mapping business goals might seem to be overly complex or inconsequential, it is, in fact, important to use CobiT's list or an equivalent list to identify your business goals or objectives. Compliance and risk management require seamless

**FIGURE 2: THE BP APPROACH ROADMAP**

Phase 1 Identification	Phase 2 Cross-reference	Phase 3 Risk Analysis / Assessment	Phase 4 Risk Mitigation	Phase 5 Evaluate Results / Value Mapping
Identify the organization and business goals, objectives, and/or processes.	Execute cross-reference mapping to all identified frameworks and standards.	Perform a high-level risk assessment / self assessment and record initial results as a benchmark for maturity measurement.	Identify potential risk mitigation options (e.g. products or services).	Review IT risk mitigation options with the business.
Identify the relevant framework(s).	Execute cross-reference mapping to all identified compliance initiatives.	Review assessment results and identify probable business and IT owners.	Identify all associated costs for each mitigation option.	If accepted, initiate a project to implement the selected IT risk mitigation option.
Identify the relevant control practices or activities.	Execute cross-reference mapping to all identified IT roles/areas.	Based on risk results, perform a detailed risk analysis to include asset impact, risk realization cost, and acceptable level of risk.	Identify any residual risk.	Map the value associated with the IT activity back to the organization and business goals or objectives.
			Compare costs associated with risk mitigation options against "risk realization" costs to identify TCO/ROI.	Review the relevance of the IT control activity to the cross-references for frameworks and compliance.

communication between IT and business stakeholders; a list makes it easier for IT to communicate with business stakeholders when discussing risks and their respective mitigation options. This map of controls and business goals is both the entry point of IT's collaboration with business and the end point of IT's effort to translate its control activities in terms of business value.

**Example**—CobiT's Business Goal 14, "Compliance with external laws and regulations."<sup>1</sup>

### Step 2: Identify relevant IT control framework(s)

IT best practice framework(s) are often used as a checklist of considerations and coverage in compliance and risk management efforts. Although many businesses build their own frameworks, established frameworks such as CobiT offer the advantage of providing external validation for IT control decisions. Frameworks also enhance control efforts centered around processes that are known to need improvement.

The use and consistent reference to best practice frameworks helps discussions between IT and business stakeholders move from subjective discussions to more proactive planning that directly addresses internal audit issues and concerns.

**Example**—CobiT 4 is a best-practices framework for IT controls

### Step 3: Identify relevant IT control practices or activities

CobiT 4.0, released in 2005, includes 214 IT control objectives. When a specific function or activity is recognized by the risk management team, IT can identify relevant control activities by reviewing CobiT's control objectives. If the organization relies on a best practice framework other than CobiT or identifies a compliance issue, a specific role, or a responsibility that CobiT doesn't consider, identifying relevant control activities can be achieved through the cross-reference activities described in Phase 2.

**Example**—Protection of sensitive data is a major concern for most compliance initiatives. This translates into information security responsibilities. One of the most important responsibilities for information security is access control. CobiT 4.0 describes this business objective and its relevant control activity as:

CobiT Process DS5: Ensure System Security  
Control Objective DS5.3: Identity Management  
Control Activity: Define, establish and operate an identity (account) management process

### PHASE 2: CROSS-REFERENCE

#### Step 1: Execute cross-reference mapping to identified frameworks and standards

The custodians of the various frameworks and standards available today are realizing the benefits of aligning

disparate frameworks and standards with each other. For example, the 214 control objectives defined in CobiT 4.0 cover a broad spectrum of activities that align, more or less, with many of other frameworks and standards, such as ISO 17799, the HIPAA Security Standard, and the Payment Card Industry Data Security Standard (PCI DSS). Mapping disparate frameworks into a single comprehensive framework helps the organization consistently implement and leverage all of its mapped controls. This is especially important if the organization has adopted and implemented one framework, but wants to incorporate components of another.

**Example**—ISACA’s free publication “Aligning CobiT, ITIL, and ISO 17799 for Business Benefit,” available on the organization’s Web site,<sup>3</sup> provides one example of a framework cross reference. Additionally, the BIT-map Web site<sup>4</sup> offers a free matrix mapping of CobiT 3 and 4 to the ISO 17799 security standard, versions 2000 and 2005. Combined, these two documents provide a traceable path to several of the most popular framework and standard control activities.

#### **Step 2: Execute cross-reference mapping to all identified compliance initiatives**

The list of compliance initiatives seems to be growing. For the IT-related compliance needs of your organization, several sources should be involved in identifying the requirements. Because compliance initiatives can involve laws as well as regulatory requirements, consultation with a legal representative is always important. External IT compliance expertise should also be sought.

**Example**—Many companies have legal departments or representatives dedicated to evaluation of compliance initiatives affecting the organization. The IT Compliance Institute<sup>8</sup> (ITCi) provides an excellent forum for information and expertise.

#### **Step 3: Execute cross-reference mapping to all identified IT roles and business areas**

Organizations should clarify roles and responsibilities, then map or cross-reference them to the list of relevant control objectives. This activity is dependent on the user, organization, and specific needs and in most situations, subjective results occur.

**Example**—A responsibility matrix based on CobiT 4.0 can be used, either by extracting the information from the framework document, or by downloading a free version from BIT-map.<sup>4</sup> Either resource can reduce the amount of time IT managers spend mapping roles and business areas to control requirements.

### **PHASE 3: RISK ANALYSIS/ASSESSMENT**

#### **Step 1: Perform a high-level risk analysis/self-assessment and record initial results**

The primary objective of this activity is to prioritize areas of organizational need. Some organizations already have an established risk-analysis process that includes self-assessment questionnaires distributed on a routine basis. These self assessments are normally based on user input; however, they are still a valuable source of information that can help compliance and risk management teams set appropriate priorities.

**Example**—A Web-based self-assessment questionnaire can be used to accurately distribute, authenticate, record, and aggregate responses. Several products are currently available, including some standalone products, such as the Symantec Compliance Assessment Tool,<sup>9</sup> available for small to midsize organizations.

#### **Step 2: Review results and identify probable owners**

Determining ownership of risk and control objectives is one of the most challenging areas that business and IT managers must address. The increasing scope and number of compliance initiatives are helping organizations to bridge this gap, however, as many laws (and auditors) required companies to identify and record process owners.

**Example**—Unfortunately, there is no application that magically determines ownership of risk and control objectives. If no other information is available, organizations can start by documenting roles and responsibilities, followed by a review of organizational charts.

#### **Step 3: Prioritize high-risk areas and perform a more detailed risk assessment**

The goal of a detailed IT risk assessment is to more



accurately determine business risk by qualifying or quantifying the risk associated with IT support activities. Traditional methods for IT risk cover threats, vulnerabilities, and asset value. More progressive methods include another component: the probability or activity of a risk being realized.

Traditional methods for IT risk cover threats, vulnerabilities, and asset value. More progressive methods include the probability of a risk being realized.

**Example**—Compliance or risk teams

can identify IT risk by evaluating four variables. For example, the formula for evaluating the total IT risk for unauthorized access to sensitive data would be:

1. Threat: the potential threat to the business and IT systems supporting an identified business process
2. Vulnerability: the vulnerability associated with IT systems supporting an identified business process
3. Asset: assets located on the vulnerable IT systems
4. Probability or activity: the likelihood that a threat will manifest or the identification of an existing activity that poses a threat

#### PHASE 4: IT RISK MITIGATION

##### Step 1: Identify potential risk mitigation options (e.g. products or services)

Once you have determined the risk to the IT systems supporting a business process, the next step is to identify and evaluate your options for mitigating that risk. The objective of any risk mitigation option is to execute one or more controls to reduce the risk. A risk mitigation option can be a combination of products, services, policies, procedures, or even education and training.

**Example**—Risk mitigation should be mapped to the same control framework that is the foundation of risk assessments, process ownership, and other compliance and risk activities. Following the CobiT example, this mapping would look like:

CobiT Process DS5: Ensure system security

Control Objective DS5.3: Identity management

Control Activity: Define, establish, and operate an identity (account) management process

Option: Identity manager software solution

##### Step 2: Identify all associated costs for each mitigation option

Once mitigation options have been identified, the IT manager should identify all costs associated with each option—especially products or services.

**Example**—Calculate the initial cost of the product or service, implementation, and training. Include all reoccurring costs for maintenance agreements, annual administration, and location.

##### Step 3: Identify any residual risk

Even when the quality of a product or service that mitigates risk is high, some residual risk may remain. This residual risk is normally low and largely depends on the nature and capabilities of the selected risk-mitigation option.

**Example**—By using the identity manager software solution, all properly requested user access can be processed with controls in place. However, this does not guarantee that a user will not bypass the process. This outlying possibility represents residual risk.

##### Step 4: Compare costs associated with risk mitigation option against risk realization costs to identify total cost of ownership (TCO) and return on investment (ROI)

Organizations should calculate whether the cost of mitigating the risk outweighs the cost the business will incur if the risk is realized. Calculating TCO is a time-tested method for providing business with risk-mitigation option costs. Documenting the business case for the solution is another best practice. When it is possible to quantify the value of the business risk, the business case should include a section defining the ROI of the solution.

**Example**—When corporate reputation is on the line, many companies choose to incur a high cost associated with implementing a risk mitigation option. To calculate the ROI of a risk-mitigation solution, IT managers should consider:

1. Risk assessment cost: Using survey results, an actual cost per incident can be calculated. According to recently published reports, for example, unauthorized data access has an average cost of \$60,000 per incident.
2. Risk mitigation value: How much a given solution might reduce risk can be determined. This might be expressed as a percentage.
3. Risk mitigation cost: The implementation cost of the identified solution is added to the annual cost of licensing and maintenance. For the ROI calculation, you should subtract the risk mitigation cost from the risk assessment cost.
4. Return on investment: Using business case modeling, compliance and risk teams or managers can identify the breakeven point of a solution's value by calculating the initial and annual risk mitigation costs over a three- to five-year period. Additionally, you can compare this to the risk assessment cost over the same period.

## PHASE 5: EVALUATE RESULTS AND VALUE

### Step 1: Review IT risk-mitigation options with the business

One advantage of developing a business case for risk-mitigation options is the ability to more easily communicate your needs and rationale to business managers. The business case is an important tool in establishing a common area of understanding between business and IT practices.

**Example**—In a hypothetical company, the average cost associated with each incident of unauthorized data access is \$60,000. The initial cost of implementing a risk mitigation option is approximately \$100,000, with annual maintenance costs of \$20,000. The business case should illustrate

a breakeven point of two years with a return of \$40,000 from the third year on.

### Step 2: Initiate implementation project based on selected IT risk-mitigation option

When the business concurs with IT's assessment that a particular risk-mitigation option is indicated, IT can turn its focus to implementation.

**Example**—There are many well-established project management approaches, including the PRINCE (PRojects IN Controlled Environments) methodology.<sup>10</sup>

### Step 3: Map the value associated with the IT activity back to the organizational and business goals

To illustrate the value of the IT activity to business managers, it is essential to trace the IT activity through your chosen best-practice framework to its associated business goals and, finally, to organizational objectives.

**Example**—A complete lineage of organizational objectives to IT activity might look like this

Organizational Objective: Client satisfaction and reputation

Business Goal: Compliance with external laws and regulations

Process CobiT DS5: Ensure system security

Control Objective DS5.3: Identity management

Control Activity: Define, establish, and operate an identity (account) management process

Option: Identity manager software solution

### Step 4: Review the relevance of the IT control activity to the cross-references for frameworks and compliance

To illustrate the added value of leveraging current compliance investments, IT managers must identify similar, relevant control activity requirements within additional compliance initiatives.

**Example**—Adding compliance alignment opportunities to the lineage might look like this:

Organizational Objective: Client satisfaction and reputation

Business Goal: Compliance with external laws and regulations

Process CobiT DS5: Ensure system security

Control Objective DS5.3: Identity management

Control Activity: Define, establish, and operate an identity (account) management process SOX, HIPAA, and GLBA relevant

#### **AUTHOR BIO**

R. Andrew Brice has worked and consulted with US and International organizations since 1991. In Credit Suisse Group, he has served as the Chief Information Security Officer (CISO) and currently as the Head of IT Risk and IT Security Risk Control.

#### **CONCLUSION**

The BP approach can be used to successfully illustrate the value of an IT control activity, as defined in best practice, for business and compliance. It can be leveraged to increase the value of a current compliance investment by proactively addressing the issue at the source instead of on a compliance by compliance approach. Additionally, this approach can provide a solid foundation to successfully address the challenges faced when communicating the need for a project, a product or a service to the business and other management, especially to gain acceptance and funding where needed.

#### **END NOTES**

1. Control Objectives for Information and related Technology (CobiT), <http://www.itgi.org>
2. IT Governance Institute, <http://www.itgi.org>
3. Information Systems Audit and Control Association (ISACA), <http://www.isaca.org>
4. BIT-map, <http://www.bit-map.com>
5. Management of Risk (MoR) from the Office of Government Commerce (OGC), <http://www.ogc.gov.uk>
6. ISO 17799, <http://www.iso.org>
7. IT Infrastructure Library (ITIL), <http://www.ogc.gov.uk>
8. IT Compliance Institute (ITCi), <http://www.itcinstitute.com>
9. Symantec Compliance Assessment Tool, [http://www.veritas.com/Vrt/offfer?a\\_id=18972](http://www.veritas.com/Vrt/offfer?a_id=18972)
10. The PRINCE2 Project Management Method, <http://www.prince2.com/>

# Perfect Pitch: Aligning Compliance, Risk, and Business Intelligence

Linda L. Briggs

Increasingly complex business and IT processes and expanding compliance scope can be overwhelming. Breaking compliance and risk management efforts into manageable chunks and measurable metrics can simplify the picture. By using a business intelligence (BI) approach to compliance, companies can conquer apparently insuperable compliance demands and support core business goals in the process.

## RELATED REGULATIONS

Sarbanes-Oxley Act

Gramm-Leach-Bliley Act

Basel II Revised International Capital Framework

Federal Information Security Management Act (FISMA)

Bestselling author Anne Lamott, in a book offering advice to would-be writers, tells a story from her childhood in which her brother struggles at the kitchen table with a school paper due the next day. Overwhelmed by the task at hand, a report on birds, and realizing that he should have started months earlier, he sinks head into hands. “Bird by bird, buddy,” calmly counsels his father. “Just take it bird by bird.”

That advice could easily apply to IT compliance managers, as well—so often moored to their desks, heads buried in hands, overwhelmed by what looms ahead as they struggle to make regulatory compliance something other than a costly and repetitive yearly struggle and an endless corporate cost center.

Surely, compliance, taken as a whole, is overwhelming. Even addressing compliance goals as discrete projects is unwieldy. But understanding compliance control by control, impact by impact, metric by metric, allows companies to put compliance efforts in perspective—not only of corporate governance, risk management, and compliance goals, but also of broader business goals.

The corporate compliance outlook improves considerably when companies begin to connect the dots that link compliance, risk management, and business awareness. Clearly, risk and compliance are closely tied. “Faced with stiff penalties regarding the integrity of financials,” Forrester Research analyst Michael Rasmussen writes in regard to risk and compliance management, “executives are requiring that risk and compliance be consistently managed within defined levels of risk tolerance.... The only way to combat potential litigation is through increased control and oversight.”<sup>1</sup>

Many CIOs are only now starting to question the quick fixes their companies initially implemented to meet compliance obligations. Many IT point solutions and quick fixes that suited corporate purpose in year one of Sarbanes-Oxley (SOX) compliance, for example, now look inconsistent, expensive, and impossible to maintain. Efficient compliance management depends on resolving these challenges. Simplification and standardization of IT initiatives that support compliance is one major step. And in the bigger

picture, companies must find ways to turn the overlap between compliance, risk management, and business awareness into a competitive advantage.

If there's a silver lining to the cloud that compliance has cast over the business landscape in the past four years, it might be this: companies that figure out how to intelligently meet compliance obligations can create an actual competitive advantage, simply because they'll be a distinct minority. And IT can play an important role in that process.

### COMPLIANCE AND RISK MANAGEMENT

There are many kinds of risk exposure: risk of loss of financing, of creditor failure, of operational failure, of unfavorable market shifts, and more. Increasingly, compliance is also seen as a special subset of risk management. And IT is both strategically and tactically integrated into both risk management and compliance.<sup>2</sup> The IT department itself is subject to risk and compliance. Moreover, IT is an enabler for corporate risk management, since it supplies the functional foundation for many risk monitoring and management activities.

Companies are taking a more structured approach to enterprise risk and compliance management for many reasons. According to Rasmussen, "Facing increased compliance obligations, a dynamic business and IT environment, fragmented risk and compliance projects, and exposure to tort and criminal liability, organizations are seeking a formalized approach to managing enterprise risk and compliance."

Another factor driving organizations toward better risk and compliance management is a realization of the inconsistent approach toward compliance common in many companies. "Risk and compliance management has been fragmented throughout organizational silos," Rasmussen writes, "resulting in a duplication of technologies and efforts with inconsistent approaches, measurement, and reporting."<sup>3</sup>

### GETTING IT TOGETHER

Although many businesses are focused on SOX because of its complexity, immediacy, and penalties, many global regulations are placing new demands on IT departments. Non-compliance risks are raised

by Basel II, Gramm-Leach-Bliley, and SEC rules for financial institutions, HIPAA for companies that deal with health care information, and the USA Patriot Act (USAPA) and payment-card industry standards for many companies that process consumer transactions.

In fact, according to Ross Armstrong, a senior research analyst at Info-Tech Research Group, "the Patriot Act's requirements directly affect IT departments that never before had to worry about compliance at any meaningful level."<sup>4</sup> This is because USAPA empowers the FBI to subpoena any US company at any time to produce business records. Unfortunately, without a framework for compliance and risk management, Armstrong writes, few companies are currently able to comply with such a request—despite the fact that compliance requirements for SOX and USAPA are remarkably similar.

Combining the many complex regulatory requirements into a single holistic compliance view is the focus of the IT Compliance Institute's Unified Compliance Project (UCP, <http://www.itcinstitute.com/ucp>) and other efforts that cross-reference regulatory requirements and IT frameworks. These efforts focus on similarities rather than differences between compliance needs, such as the heavy overlap Armstrong points out between SOX and USAPA. The goal is to help companies to reduce costs, limit liability, and leverage spending on compliance-related technologies across the enterprise. The UCP supports this goal by working to reconstruct complex corporate regulations into a more holistic IT compliance view.

Other projects and companies also help to reduce risk by framing compliance as a single sweeping endeavor, rather than disparate efforts. IBM, for example, has been working on a risk and compliance framework for several years. The project, announced in 2004, creates a taxonomy made up of hundreds of regulations, covering both US and European data privacy measures. In an interview last year, IBM's Frederik Soendergaard-Jensen, who heads up the company's risk and compliance software business, pointed out that, since most companies need to address multiple compliance laws, "buying by regulation isn't a cost-effective [approach]." He encourages companies to look at the

regulations they face overall, then work compliance management into the existing business infrastructure.

#### THE STRATEGIC ROLE OF BUSINESS INTELLIGENCE IN COMPLIANCE EFFORTS

For most organizations, integrating compliance into business processes is a daunting task, akin to tuning a car engine while racing down the highway. Since compliance requirements can alter, overlap, or even directly contradict some business processes, simply adding compliance as a new layer to employee responsibilities is seldom successful.

Instead, a thorough understanding of hierarchical objectives, policy components, and related procedures

and privacy. The application of BI principles to compliance practices is called, for the purposes of this paper, *compliance intelligence*.

According to Ted Frank, head of the Technology Group within a consortium of companies called the Open Compliance and Ethics Group (OCEG, <http://www.oceg.org>), most companies recognize that risk management and compliance are linked. OCEG, whose charter is to promote effective governance, risk and compliance management, has participation from over 30 percent of the Fortune 500. Still, Frank notes, “It surprises me [that] a very small percentage [of companies] ask the question about business intelligence.”<sup>5</sup>

Compliance requirements can alter, overlap, or even directly contradict some business processes; simply adding compliance as a new layer to employee responsibilities is seldom successful.

“The challenge of making compliance more efficient, more effective, and less risky,” agrees Lee Dittmar, a principal with Deloitte Consulting, “is just the other side of the coin of improving internal capabilities and turning data into information, then getting that information to the right place at the right time.... Doesn’t that sound a lot like business intelligence?”

is a prerequisite of compliance integration. This allows companies to map compliance processes to existing business processes and integrate or consolidate overlapping processes, where they exist.

Measurement and reporting are also prerequisites of successful compliance integration. Managers must understand how well compliance activities are working during the period when processes are being developed, during process changes, and on an ongoing basis.

Over the past decade, business intelligence (BI)—essentially, the collection and analysis of business information—has become a common strategic component in many organizations. As BI technologies have evolved and BI processes have gained mainstream acceptance, so too has an understanding of its importance, at least within more agile and market-responsive companies. Only recently, however, have companies begun to see BI’s potential benefits in regard to risk management, compliance, and even IT security

Take SOX as an example. To ensure financial-reporting compliance, companies must monitor thousands of business activities—including controls, communications, and transactions—that occur on a daily basis. Many of these activities are also part of core business functions. Analyzing the raw data on business activities lets companies discover important trends, identify risky outliers to regulated processes, and monitor the effectiveness of new policies and strategic directives. Using a BI approach to compliance goals helps a company understand how compliance impacts business performance, where compliance and core business processes overlap, and how information management practices can support both.

Another specific example of the overlap of BI, risk management, and compliance is key risk indicators (KRIs). While BI focuses on key performance indicators (KPIs), many of these same metrics can be understood in terms of risk—effectively acting as KRIs that could be measured and reported very similarly to the way



that KPIs are. The number of errors associated with a particular process, for example, could be a KPI or KRI, particularly if the errors were associated with a financial reporting process or another materially relevant activity. Other examples of KRIs might be the number of lawsuits filed in relation to a process, percentage of malicious traffic (viruses, etc.) on a network, number of recognized policy breaches by employees, or number of major accounts lost.

As with KPIs, KRI data can be sliced and diced in any number of ways that help the business identify a course of response. KRI reporting should be timely and accessible to appropriate managers. Perhaps more than KPIs, however, KRIs should be documented and tied to accountability—tied to controls, staff roles, and business objectives.

Once companies begin to build on the link between BI and compliance, BI becomes an asset in compliance. Following BI principles can help companies provide the sort of rapid response that compliance often mandates, for example. A tight analytical perspective on specific compliance metrics helps a company understand how and where a regulatory change will impact existing processes. This perspective also provides more rapid and accurate notice when a compliance process works, changes, or breaks down entirely.

### THE CHALLENGE OF RAPID CHANGE

The rapidly evolving regulatory landscape calls for a flexible compliance approach. Companies must be able to respond quickly, while continuing to work toward sustainable, long-term compliance strategies. BI, with its emphasis on data and analytics that help companies quickly recognize environmental changes and measure their adaptive performance in response, can be extremely useful in measuring compliance success.

Some of the largest companies with the most at stake in terms of compliance, are starting to see the link and move accordingly. “I see two things happening in the market,” says OCEG’s Frank. “Large, complex companies are recognizing that the investment they’re making in managing financial reporting risk or privacy risk... must be leveraged across the board, across other areas of risk. Their boards are demanding it.”

Also, Frank notes, companies are starting to automate controls in an attempt to make manual processes more system-oriented. “The level of debate and the interest in the market for enterprise technologies to tackle [compliance] is at a fever pitch. [Compliance software] is becoming a unique and distinct category of software, and [is] starting to be viewed as a mission-critical asset.”

A BI development with specific automation potential for compliance efforts is the move toward “right-time” BI.<sup>6</sup> Businesses are increasingly using BI analytics to reduce the time between business events and business responses. This trend holds promise for any change management effects and particularly benefits in regard to SOX section 409, which mandates real-time reporting of material events.

### COMPLIANCE DASHBOARDS

One BI-associated tool that can aid in measuring timely compliance efforts is performance dashboards. Compliance-specific dashboards can be customized to fit the business, then used to summarize and present compliance information efficiently. Dashboards can be tailored to present relevant information—and only relevant information—to interested parties at various levels in the company, ranging from line-of-business managers, upward through middle management, to the CEO. A properly calibrated dashboard can arrange the data to present various views and depths of information, as appropriate—a tremendous real-time tool in compliance management.

According to a new book on dashboards by Wayne Eckerson of The Data Warehousing Institute (TDWI),<sup>7</sup> a good performance dashboard is built on a business intelligence and data integration infrastructure, using a multilayered approach. A good dashboard lets a wide variety of users drill down into the performance metrics they need to manage their individual portions of the business.

Used correctly, performance dashboards can alert users to the sorts of out-of-bounds conditions—such as spikes or anomalies in KRIs—that should be flagged, not just for business intelligence, risk, and business performance management, but for compliance as well.

Well-conceived and integrated dashboards that display the right level of information to the right users, and that are based on a solid business intelligence infrastructure, can greatly augment compliance intelligence.

#### EXCEL AGGRAVATION

Forrester Research analyst Keith Giles estimates that, while about 70 percent of business workers use Excel spreadsheets, only 10 percent use BI. That's a problem, particularly in financial reporting—specifically, a company's ability to document reporting controls, ensure consistent reporting, and recognize materially relevant events when they occur.

The single version of the truth that a well-constructed BI system can give managers is often undermined by the nemesis of out-of-control spreadsheet use. Deemed critical by masses of business managers but a huge headache to IT—and compliance

The “single version of the truth” that a well-constructed BI system can give managers is often undermined by the nemesis of out-of-control spreadsheet use.

managers—spreadsheets are almost never tied into an analytical infrastructure via transaction engines. That makes spreadsheets a compliance nightmare that can undermine a company's efforts to link BI and compliance. In his book, Eckerson calls the unmined mass of spreadsheet data “spreadmarts”—spreadsheets or individual databases that function as data marts, with their own data, metrics, and rules.

“Centrally defined metrics and a single version of corporate information,” are key to making BI effective, Eckerson says. If dashboards don't work from the system of record—if they draw information from other databases within the company—then they're working at cross-purposes to compliance intelligence. Given the distorted data this situation produces, organizations cannot comply or compete.

#### MANAGEMENT BUY-IN

Compliance spending is huge and will continue to be so for at least several more years. In March, AMR Research predicted that, in 2006, total spending on compliance will hit \$27.3 billion. Twenty-two percent of those dollars, or \$6 billion, will be spent on SOX compliance. Spending will continue to climb in 2007, AMR predicts, with companies spending \$28 billion on compliance initiatives.

One upside to all the focus on compliance is the boost to IT budgets. In particular, the pitch for compliance software is, to put it bluntly, easier to sell to management these days. Also, executives are more likely to invest in risk management solutions—a hot topic in itself lately—when an argument can be made that ties those solutions to SOX or other compliance efforts, as well.

Compliance budgeting is an opportunity for IT managers to select products that offer not just short-term compliance fixes, but long-term solutions with benefits for risk management and business performance, with compliance as a byproduct.

In working toward compliance intelligence, IT can also make the argument to upper management that better BI tools result in more confident managerial attestations. Solid, customized reports that summarize various aspects of the business from different levels and angles are great selling tools to a CFO, CEO, and board of directors. With good enterprise BI tools producing solid information, IT can assure management that its attestations on compliance are correspondingly solid.

Management support means more than additional spending dollars. It's also deemed critical by analysts for moving compliance forward, strategically. According to Rajeev Rawat and Claudia Imhoff,<sup>8</sup> it's crucial that IT managers and CIOs secure the support of senior management when seeking resources to retool the enterprise for compliance and competitive advantage. IT must demonstrate, they say, that it has evolved from its limited, technology-focused past to

a new strategic role that focuses on the needs of the enterprise and on making IT a competitive advantage.

#### STEPS FOR MOVING TOWARD COMPLIANCE INTELLIGENCE

Here's blunt advice from Ted Frank, head of the Open Compliance and Ethics Group: "If you don't think you need a business plan and a strategy for dealing with regulatory compliance, you're crazy. You've got to do it." Frank advises that companies start by formally defining risk within the context of a strong business plan. "If you have that, BI becomes an inherent piece of the puzzle."

But like Anne Lamott's brother and his bird report, too many companies are frozen in place, overwhelmed by the task ahead and desperate for deadline extensions. This is an area where small, steady steps can make marked progress.

Rather than too granularly identifying risk, for example, compliance teams should start with the most obvious risks and work outward from there. Compliance initiatives are an opportunity to fix many of the information flow problems within an organization, but data management is a complex endeavor that can't be done all at once. "Put into place what the [biggest] risks are, what information [you] need to know when they occur, the alerts and query capabilities, and the monitoring information you want on an ongoing basis," suggests Deloitte's Ditmar. Compliance teams can feed that information to decision makers and those who govern the organization. That's a start.

Above all, don't forget the critical role of IT in driving compliance intelligence. By helping the company select the right tools, including long-term compliance products with BI overtones, and compliance dashboards, IT can help steer its company's overall compliance strategy—as it should. By understanding and fostering the links among compliance, BI, and risk, IT assures its perpetual seat at the corporate leadership table.

#### NOTES

1. Michael Rasmussen, Forrester Research, Inc., "Trends 2005: Risk and Compliance Management"
2. Michael Rasmussen, Forrester Research Inc., "Trends: IT's Role in Enterprise Risk Management," April 27, 2005
3. Michael Rasmussen, Forrester Research Inc., "Trends 2005: Risk and Compliance Management," Analyst Corner, [www.csoonline.com](http://www.csoonline.com)
4. Ross Armstrong, "Compliance is Now Everyone's Concern," Info-Tech Research Group, <http://www.infotech.com>
5. Ted Frank is also CEO of Axentis, a vendor that offers governance, risk management, and compliance products and services
6. Claudia Imhoff, "Three Trends in Business Intelligence Technology: Perfect Storm or Perfect World?", Business Intelligence Network, April 2006, <http://www.b-eye-network.com>
7. Wayne W. Eckerson, *Performance Dashboards: Measuring, Monitoring and Managing Your Business*, John Wiley and Sons, New Jersey, 2006
8. Rajeev Rawat and Claudia Imhoff, "Compliance for the Agile Enterprise. Retooling IT for Compliance: Secure Resources and Tools to Plan, Evaluate, Test and Deploy," Business Intelligence Network, March 2005, <http://www.b-eye-network.com>

#### BIO

Linda L. Briggs is a contributing editor for the IT Compliance Institute. Based in San Diego, she writes about technology in corporate, education, and government markets. You can contact her about this and other articles at [lbriggs@lindabriggs.com](mailto:lbriggs@lindabriggs.com).

# Compliance Bibliography

Key research in compliance,  
risk management, and governance  
from 2005 and 2006.

## ANTIFRAUD AND FINANCIAL REPORTING COMPLIANCE

- **Corporate Governance Survey Key Findings**  
*The Business Roundtable*

Very few firms expect compliance costs to rise in 2006.

Abstract: <http://www.itcinstitute.com/info.aspx?id=24799>

Full report: <http://tinyurl.com/ppxlf>

- **AMR Research Reports Compliance Spending Will Reach \$27.3B in 2006**  
*AMR Research*

SOX is only the tip of the compliance-spending iceberg, says recent study. The anti-fraud act accounts for only 22 percent of compliance spending.

Abstract: <http://www.itcinstitute.com/info.aspx?id=24388>

Full report: <http://tinyurl.com/oq3gh>

- **IRS Improves Enforcement and Services in 2005**  
*US Internal Revenue Service (IRS)*

The IRS is auditing more companies than ever. The rate is now one in five, more than double what it was three years ago.

Abstract: <http://www.itcinstitute.com/info.aspx?ID=22583>

Full report: <http://tinyurl.com/lfmn5>

- **Global Economic Crime Survey 2005**  
*PricewaterhouseCoopers*

Despite new regulations, financial fraud is on the rise, and internal audits are not the first line of defense. In North America, senior managers were behind nearly a quarter of identified fraud cases.

Abstract: <http://www.itcinstitute.com/info.aspx?id=22117>

Full report: <http://tinyurl.com/mqfxn>

- **Sarbanes-Oxley Section 404 Costs and Implementation Issues: Survey Update**  
*CRA International*

More efficiency, less documentation should make the difference in the coming year of implementation

Abstract: <http://www.itcinstitute.com/info.aspx?id=22115>

Full report: <http://tinyurl.com/rpj78>

- **Restatements—Traversing Shaky Ground**  
*Glass, Lewis & Co*

The number of restatements in 2005 nearly doubled, thanks to SOX compliance and emboldened auditors.

Abstract: <http://www.itcinstitute.com/info.aspx?id=22114>

Full report: <http://tinyurl.com/n2zud>

## SECURITY AND DATA PROTECTION COMPLIANCE

- **Information Security Breaches Survey 2006**  
*PricewaterhouseCoopers on behalf of the UK Department of Trade and Industry (DTI)*

Abstract: Many UK businesses lack a security-aware culture. Security expenditure is either low or targeted at the wrong risks. New technologies such as flash drives, iPods, and smart phones pose significant future risk.

Full report: <http://tinyurl.com/odb7v> (PDF)

- **Internet Security Threat Report: Volume IX**  
*Symantec*

Trojans, phishing, and botnets are up; virus mass-attacks down. Cybercrime trends toward more targeted, profitable, low-key attacks.

Abstract: <http://www.itcinstitute.com/info.aspx?id=24387>

Full report: <http://tinyurl.com/qnuqd>

- **Accounting for Internet Malice**  
*Top Layer*

More than half of companies have suffered cyber attacks. One in five exceeds \$100,000 in damages, driving up security spending.

Abstract: <http://www.itcinstitute.com/info.aspx?id=23417>

Full report: <http://tinyurl.com/qzx73>

- **A Crawler-based Study of Spyware on the Web**  
*Alexander Moshchuk, Tanya Bragin, Steven D. Gribble, and Henry M. Levy, Department of Computer Science & Engineering, University of Washington*

Five percent of Internet files contain spyware code. The silver lining: drive-by attacks are falling out of vogue.

Abstract: <http://www.itcinstitute.com/info.aspx?id=23415>

Full report: <http://tinyurl.com/n9djm> (PDF)

- **Enforcement Activities of the FTC Under the Truth In Lending Act, the Consumer Leasing Act, the Equal Credit Opportunity Act, and the Electronic Fund Transfer Acts During 2005**  
*US Federal Trade Commission (FTC)*

Abstract: <http://www.itcinstitute.com/info.aspx?ID=22845>

Full report: <http://tinyurl.com/ov3ws>

- **Sophos Security Threat Management Report 2005**  
*Sophos*

Trojans surpass worms as cyber-criminals seek income rather than thrills. Attacks by malware grew by 48 percent in 2005.

Abstract: <http://www.itcinstitute.com/info.aspx?id=22116>

Full report: <http://tinyurl.com/oghzb>

- **The SANS 2005 Information Security Salary & Career Advancement Survey**  
*SANS Institute*

Higher degrees, certifications, and communications skills are still worth having.

Abstract: <http://www.itcinstitute.com/info.aspx?ID=22580>

Full report: <http://tinyurl.com/rxgoj>

## STAFFING, STAFF MANAGEMENT, AND SALARIES

- **They're Hiring in Techland**  
*BusinessWeek Online*

The high-tech job market has come back to life after the post-bubble trough, despite rampant out-sourcing.

Abstract: <http://www.itcinstitute.com/info.aspx?ID=22843>

Full report: <http://tinyurl.com/o8aok>

- **Tech Wages Hit Highest Level in Five Years During Fourth Quarter of 2005**  
*Yoh*

SAP consultants top the list of record pay increases.

Abstract: <http://www.itcinstitute.com/info.aspx?id=23416>

Full article: <http://tinyurl.com/lam6r>

## LEADERSHIP AND STRATEGY

- **Future looks rosy for corporate IT spending**

Most business leaders foresee expanding IT budgets.

Abstract: <http://www.itcinstitute.com/info.aspx?id=24801>

Full report: <http://tinyurl.com/qsy6p>

- **Gartner Survey of 1,400 CIOs Shows Transformation of IT Organisation is Accelerating**  
*Gartner*

Survey finds that IT departments must turn their attention to business issues rather than technical matters.

Abstract: <http://www.itcinstitute.com/info.aspx?ID=22844>

Full report: <http://tinyurl.com/mhq5g>

## HEALTH IT AND HIPAA

- **Survey Finds Backsliding on HIPAA Privacy Compliance**

*American Health Information Management Association (AHIMA)*

Lack of resources and management interest appear to be the culprits.

Abstract: <http://www.itcinstitute.com/info.aspx?id=25815>

Full report: <http://tinyurl.com/l7ndm>

- **U.S. Healthcare Industry HIPAA Compliance Survey Results: Winter 2006**

*Healthcare Information and Management Systems Society /Phoenix Health Systems*

Long-term benefits of HIPAA are starting to appear, although some serious compliance issues remain.

Abstract: <http://www.itcinstitute.com/info.aspx?id=23866>

Full report: <http://tinyurl.com/s4lu3> (PDF)

**Note on URLs:** To make referent URLs more accessible to our readers, we have used a generic URL-shortening service, <http://tinyurl.com>.

---

# Write for the IT Compliance Journal

If you can offer solid insight into the complex IT issues related to regulatory compliance, we want to hear from you. The IT Compliance Journal is a biannual publication dedicated to the presentation of unbiased, experience-based information on compliance-related strategies, best practices, technologies, and processes. The *Journal's* goal is to educate compliance and IT professionals about an array of options and disciplines they can use to support the development of compliant, well-governed, and risk-resilient organizations. Acceptable proposals must offer useful, practical, and expert-level advice for their topic. We are especially interested in solution-oriented case studies.

Articles should focus on either best practices or mistakes to avoid in compliance efforts, or present a case study of a compliance challenge successfully solved. Case studies must include hard metrics that illustrate solution success. You are also welcome to submit manuscripts on other topics of interest to compliance and IT managers. If your proposal for a

paper or presentation is accepted, an ITCi editor will contact you with additional information about fair compensation, the publishing schedule, and additional editorial opportunities.

For guidance on topics or clarification on ITCi's submission guidelines, please write [editor@itcinstitute.com](mailto:editor@itcinstitute.com) or visit <http://www.itcinstitute.com/display.aspx?id=202>.