IT Compliance Journal

PRACTICAL, ACCESSIBLE INFORMATION FOR COMPLIANCE PROFESSIONALS

VOLUME 2, NUMBER 2, FALL 2007

Although businesses have invested billions in firewalls, intrusion detectors, intrusion prevention systems, and other defense mechanisms, the US has witnessed more than 300 breach disclosures since the passage of California's Breach Disclosure law.

IN THIS ISSUE

ITCi
IT Compliance Institute™

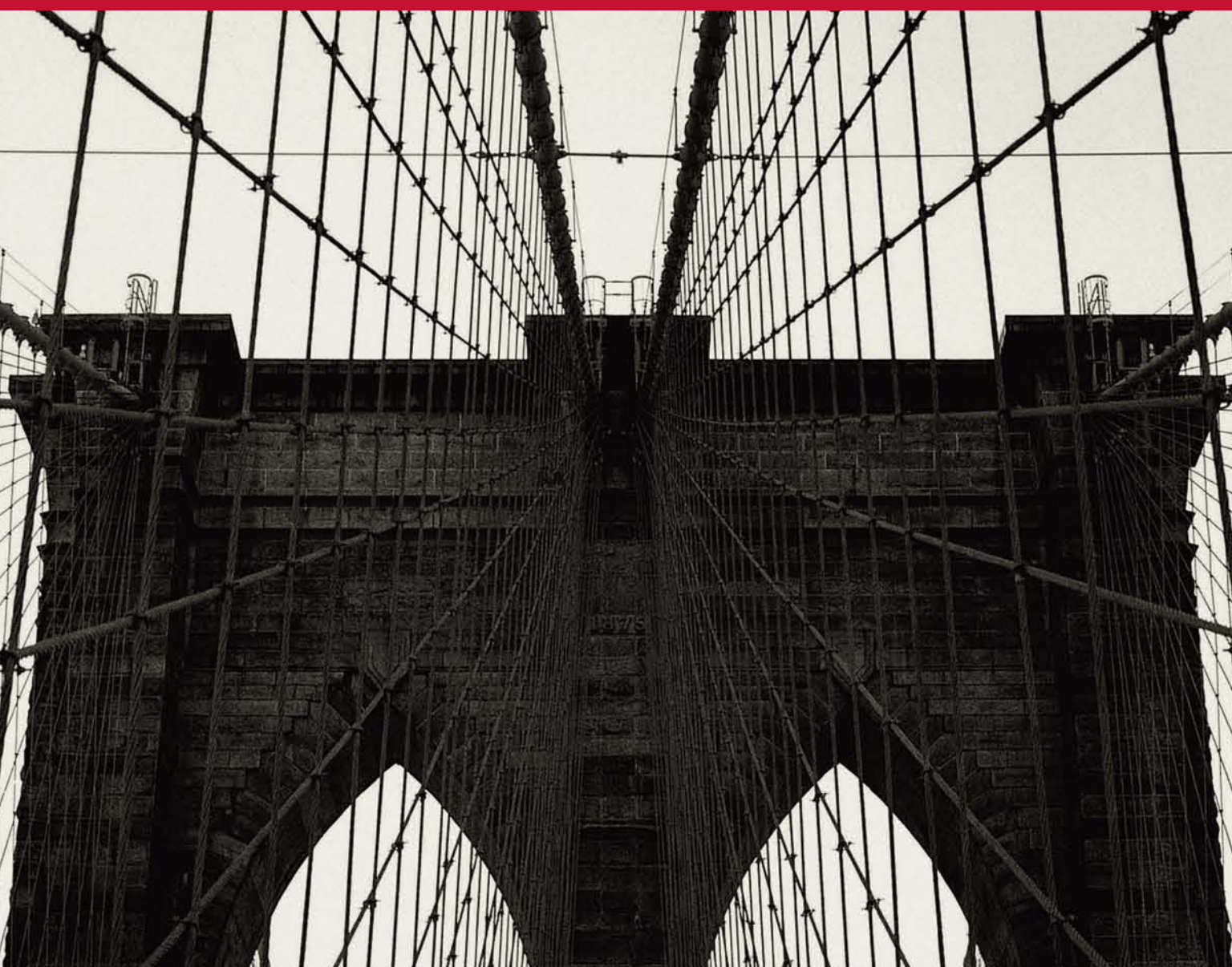
Enterprise data. Aligned.

You dedicate huge resources to enterprise applications like Oracle,® PeopleSoft,® JD Edwards,® Siebel.® And every year they grow in size and complexity — increasing maintenance challenges. Now you can take back control with Princeton Softech Optim.™ Optim gives you the ability to align application data management to performance goals. Optimizing results, mitigating risk and controlling the cost of every IT investment — servers, software, storage, networks and people. Is this heaven? No, it's the power of Enterprise Data Management.

Learn more at princetonsoftech.com.

princeton softech

The Power of Enterprise Data Management



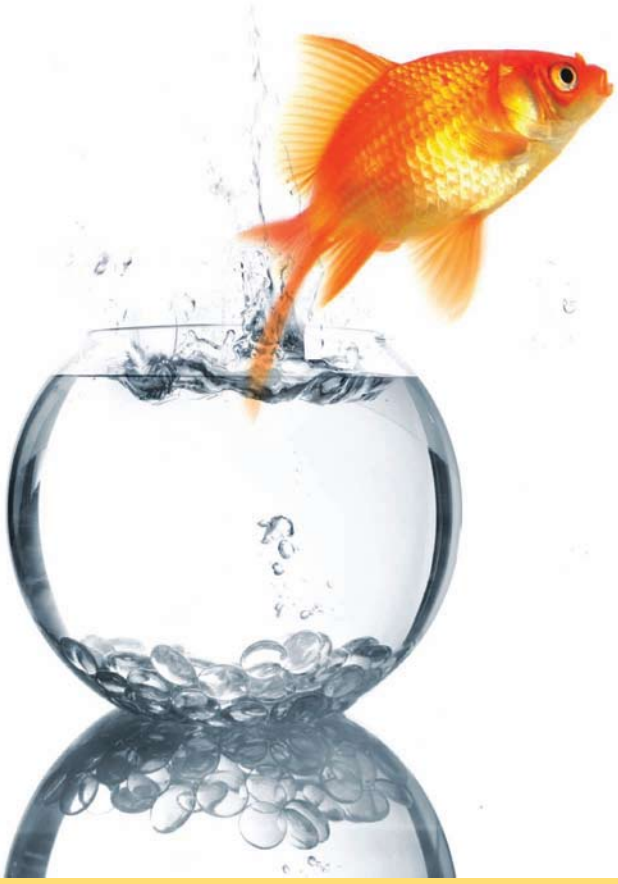
IT COMPLIANCE JOURNAL

VOLUME 2, NUMBER 2, FALL 2007

Table of Contents

ITCi
IT Compliance Institute™

PCI COMPLIANCE GOT YOU SWIMMING IN CIRCLES?



Don't Be Confined by a File Monitoring Tool – Breakout with Solidcore

Solidcore is the first and only solution to provide real-time detective *and preventative controls* for continuous compliance. We'll help you get compliant fast and stay there automatically. Join the leading companies – including 2 of the Fortune 10 – who have adopted Solidcore's integrated approach to change control. Our real-time control technology scales to the largest distributed environments... and from today's PCI needs to whatever's next, from SOX to ITIL.

Visit our website to read our PCI whitepaper or call us to see what Solidcore's change control technology can do for you.

solidcore®

Email: sales@solidcore.com
Web: http://www.solidcore.com
Tel: 888.210.6530

IT Compliance Journal

www.itcinstitute.com

GENERAL MANAGER Geoff Bridges
DIRECTOR OF MARKETING Michelle Johnson
EDITORIAL AND RESEARCH DIRECTOR Cass Brewer
DIRECTOR OF EDUCATION John Rapp
EDITOR Huan Do
ART DIRECTOR Deirdre Hoffman
GRAPHIC DESIGNER Bill Grimmer

1105 MEDIA

PRESIDENT & CEO Neal Vitale
CFO Richard Vitale
SR. VP, HUMAN RESOURCES Michael J. Valenti

VP, FINANCIAL PLANNING & ANALYSIS William H. Burgin
VP, FINANCE & ADMINISTRATION Christopher M. Coates
VP, AUDIENCE MARKETING & WEB OPERATIONS Abraham M. Langer
VP, INFORMATION TECHNOLOGY Erik A. Lindgren
VP, PRINT & ONLINE PRODUCTION Mary Ann Paniccia

CHAIRMAN OF THE BOARD Jeffrey S. Klein

REACHING THE STAFF

Editors can be reached via e-mail, fax, telephone, or mail. A list of editors and contact information is at www.itcinstitute.com.

E-mail: e-mail is routed to individuals' desktops. Please use the following form: firstinitiallastname@1105media.com. Do not include a middle name or middle initials.

Telephone: The switchboard is open weekdays 8:30 a.m. to 5:30 p.m. After 5:30 p.m. you will be directed to individual extensions.

Renton Office 425.226.9126; Fax 425.687.2842

Corporate Phone 818.734.1520; Fax 818.734.1528

ADVERTISING SALES Lesley Schwartz
lschwartz@1105media.com, 425.277.9196

Reprints and E-prints: PARS International, 1105reprints@parsintl.com.
Phone: 212.221.9595, Fax: 212.221.9195

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, Merit Direct at 914.368.1000 or www.meritdirect.com.

About ITCi

ITCi IT Compliance Institute™

OUR MISSION

The IT Compliance Institute (ITCi) strives to be a global authority on the role of IT management in corporate compliance, risk management, and governance. ITCi helps organizations navigate today's complex regulatory environment, turning compliance responses into capital opportunities.

Providing extensive research, news, tools, and education for the IT compliance community, ITCi is a useful and trusted resource for compliance professionals. We are one of the few independent compliance analysts who provide a cross-industry, cross-regulatory, and global perspective on topics ranging from anti-fraud controls to technical security, privacy, records management, compliance unification, technology frameworks, and effective IT auditing. To serve our diverse member community, ITCi covers these topics through an array of publications and programs, including a worldwide membership program, publications, compliance reference databases, live and online educational events, the Compliance Convergence Initiative, and more, as described below.

OUR MEMBERS

ITCi supports a diverse member community composed of CIOs, CTOs, IT leaders, auditors, risk management and business executives, consultants, and compliance specialists from around the globe. Our members gain unrestricted access to most ITCi resources, as well as discounts on ITCi-hosted events and interactive tools.

continued on page 6

LEGAL DISCLAIMER

When assessing any legal matter, do not rely solely on materials published by third parties, including the content in this publication, without additionally seeking legal counsel familiar with your situation and requirements. The information contained in the *IT Compliance Journal* is provided for informational and educational purposes and does not constitute legal or other professional advice. Furthermore, any applicability of any legal principles discussed in this paper will depend on factors specific to your company, situation, and location. Consult your corporate legal staff or other appropriate professionals for specific questions or concerns related to your corporate governance and compliance obligations.

ITCi makes every effort to ensure the correctness of the information we provide, to continually update our publications, and to emend errors and outdated facts as they come to our attention. We cannot, however, guarantee the accuracy of the content in this publication, since laws change rapidly and applicability varies by reader.

The information in this publication is provided on an "as is" basis without warranties of any kind, either expressed or implied. The ITCi disclaims any and all liability that could arise directly or indirectly from the reference, use, or application of information contained in this publication. ITCi disclaims any liability, whether based in contract, tort, strict liability, or otherwise, for any direct, indirect, incidental, consequential, punitive, or special damages arising out of or in any way connected with access to or use of the information in this publication.

ITCi does not undertake continuous reviews of the Web sites and other resources referenced in this publication. We are not responsible for the content published by other organizations. Such references are for your convenience only.

POLIVEC

it all starts with one compliance initiative

...and management needs the latest technologies, courtesy of the IT pros, to make sure that they finish the job.

Regulatory compliance, governance, risk management. The vast majority of senior executives and board members know that they're extremely important. But few of those same executives know just where to start, or that powerful IT solutions have emerged to give them firm control of compliance risks and costs. The Polivec GRC platform lets you start with the most important department or regulation and extend control across the company the way you want and when you want. For a copy of our informative 2007 Executive Survey on Compliance, visit www.polivec.com/policy

POLIVEC™

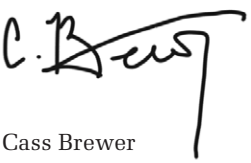
ITCi Research Perspective

It's been a brutal year on the security front. A constant stream of laptop losses, employee malfeasance, and data breach reports has crossed the newswire, adding up to more than 165 million compromised records as of this printing. Meanwhile, after several false starts, both HIPAA and PCI authorities have gotten serious about enforcement. In March, the US Health and Human Services Department rocked the healthcare community by initiating its first HIPAA audit. And VISA defied expectations in September by refusing to defer again the PCI deadline, despite broad evidence that many merchants couldn't comply. The message to management is clear: Get your house in order, because if the bad guys don't get you, the good guys will.

Access management, application security, and encryption remain hang-tough security gaps. Each represents a management issue as well as a technology challenge. Access management is a phenomenally complex issue, requiring both sweeping policy changes and scrupulous attention to scads of events. Application security requires a sea change in the way software is planned and developed. And encryption poses serious technical challenges, as well as a managerial headache.

This issue of the Journal touches on many of these issues, from Ted Ritter's analysis of two major information security standards to Arshad Noor's proposal for a simplified encryption key-management approach. On a different note, Mary Ann Reichard's control framework for e-discovery touches on another information management risk that is neither abated by nor unrelated to information security issues. And, finally, Peter Gallinari's paper reminds us that sometimes the good guys can also be the bad guys.

We hope you find this Journal informative and useful. As always, we hope you will contact us with your questions and feedback. Just drop us a line at my e-mail address, below.



Cass Brewer
Editorial and Research Director
IT Compliance Institute
cbrewer@itcinstitute.com

About ITCi

continued from page 3

OUR CORE PROGRAMS

Compliance Convergence Initiative (CCI)

The CCI is a new, open project by and for the compliance community. The project develops resources to support the planning, standardization, and harmonization of compliance-related IT initiatives across the enterprise. As a living repository of expertise and experience from managers who deal with compliance issues every day, the CCI supports more efficient and effective compliance, governance, and risk management efforts.
www.itcinstitute.com/cci

CCI Project Wikis

As part of the CCI, ITCi supports two wiki projects that allow compliance professionals to get, share, and discuss key resources. The CCI Policy Wiki project is a repository of public and contributed IT policy templates that support corporate compliance efforts. The CCI GRCpedia is a library of terms and concepts related to governance, risk management, and compliance. Both resources are free and contributions are welcome.
www.itcinstitute.com/cci

White Paper Library

ITCi's White Paper Library holds a wealth of information about best practices for addressing regulatory challenges. White papers are produced by ITCi and by carefully selected vendor partners to address the specific concerns of our audience. Past topics have included Sarbanes-Oxley and HIPAA, as well as overarching strategic themes such as defensible policies and compliance intelligence.
www.itcinstitute.com/wp

ComplianceWEB Webinars

ComplianceWEB Webinars bring industry experts live to your desktop for an hour of in-depth exploration into the tools, topics, and technologies that facilitate regulatory compliance. Vendor participation is kept to a minimum to ensure that each event is an educational opportunity and not an hour-long sales pitch. Webinars are archived on our Web site for playback at any time.
www.itcinstitute.com/events

IT Audit Checklist Series

The IT Audit Checklist Series provides practical guidance for IT, compliance, and business managers on preparing for successful internal audits. In addition to helping managers understand what auditors look for and why, IT Audit Checklists can also help managers proactively complete self-assessments of their operations, identifying opportunities for system and process improvements that can be performed in advance of an actual audit.
www.itcinstitute.com/checklist

IT Compliance Conferences

ITCi offers a variety of educational and networking events dedicated to helping professionals solve the complex challenges of systems management for corporate governance, risk control, and compliance. National conferences and regional boot camps offer unique expert presentations, workgroups, and peer networking opportunities that expose professionals to best practices, experience-based advice, and frank dialogues that have direct and immediate application to real-world IT compliance challenges.
www.itcinstitute.com/conference

IT Compliance Journal

This academic-style journal offers practical information on how the people responsible for compliance and risk management implement effective and sustainable processes, policies, and technologies. Each issue features expert insight into emerging trends and leading compliance practices, key compliance statistics from the past year, and a directory of critical research in compliance, risk management, and governance.
www.itcinstitute.com/journal

ComplianceNOW E-Newsletter

ComplianceNOW, written by the leading experts in the field and delivered to your inbox weekly, 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 executives and managers with the complex issues surrounding their role in regulatory compliance.
www.itcinstitute.com/compliancenow.aspx

Regulations Database

The ITCi Regulations Database covers more than 100 local, national, and international regulations. Entries include regulation summaries, key compliance dates, and IT impact. Search by regulation name, or define search criteria such as industry, region, and company type to view a list of applicable regulations.
www.itcinstitute.com/db

COMSTATs

A compilation of key compliance statistics from the past year.

Corporate cost to US businesses each year due to spam: **$71 billion**

Cost spent per employee annually to identify and delete the spam: **$712**

Average cost per lost record due to a information security breach: **$90 to $305**

Cost per record for discovery, response, and notification for data breach: **$50**

Value of lost employee productivity per lost record: **$30**

Percentage of US respondents who believe electronic healthcare records would be more efficient than a paper-based system: **72**

Percentage of survey respondents who believe the benefits of electronic records, such as better care in emergencies and reduction in medical errors, outweigh any potential privacy risks: **73**

Percentage of data breaches that result from the loss of off-network equipment: **70**

Percentage of companies that lack effective controls for managing removable devices: **43.3**

Percentage of corporations that have experienced a data breach: **85**

Percentage of organizations that experienced a data breach and reported a loss in customers: **74**

Percentage of these that faced potential litigation: **59**

Percentage of audit and compliance managers who believe their IT counterparts lack the knowledge of risk and compliance issues to collaborate on identity and access management: **65**

Percentage of IT pros who state audit and compliance managers lacked sufficient technical expertise to collaborate: **42**

Number of clicks per month that internet users make to risky Web sites: **550 million**

Percentage of major e-commerce Web sites that have common flaws that put users' data at risk: **80**

Percentage increase in the number of external regulatory investigations for US lawyers: **49**

Percentage increase in the number of investigative requests from regulators for international law firms: **47**

Number of ranking levels the US fell over the last year in an annual comparison of nations' network readiness for information and communications technology by the World Economic Forum: **6**

Rank held by Denmark, which was cited for its use of electronic services, its regulatory structure, and its telecommunications environment in the benchmark report: **1**

Percentage of fee increase by top audit firms since 2001: **345**

Median total auditor costs in 2006: **$2.7 million**

Median total auditor costs in 2001: **$1.4 million**

Total fees paid to auditors in fiscal 2006: **$10.5 billion**

Cost of Sarbanes-Oxley compliance for companies with revenue of less than $1 billion in 2006: **$2.8 million**

Percentage at which the cost of SOX compliance for these companies has risen since 2003: **171**

Cost of SOX compliance for firms with revenue higher than **$1 billion: $12.4 million**

Percentage at which the cost of SOX compliance for these firms has increased since 2003: **54**

Number of convictions made by federal prosecutors in corporate fraud cases since 2002: **1,236**

Number of these that were CEOs or other senior-level executives: **419**

Percentage of enterprises that are not leveraging IT governance procedures to reduce the financial risk of lost or stolen data: **90**

Rate of likely data breaches for companies lacking compliance and IT governance procedures: **Once every three years**

Rate of likely data breaches for companies with proper IT compliance controls: **Once every 42 years**

Sources for COMSTATs are listed on page 39.

ISO is more focused on higher-level and management practices, while NIST tends to delve more deeply into tactical, organizational issues. Together, the two standards provide a comprehensive approach to risk management for IT assets.

Reaching Out to Protect Within: Comparing and Contrasting ISO 27001/27002 and NIST Special Publication 800-Series Information Security Standards

TED RITTER, CISSP

RELATED GUIDANCE

- ISO 27001
- ISO 27002
- NIST 800-Series
- FISMA

One of the greatest challenges CIOs face is justifying information security spending. Successful security is measured by what doesn't happen, as opposed to what does. How much is enough security? What is necessary, as opposed to sufficient or excessive? How does cost-of-control factor into the risk profile? There are no uniform answers to these questions. All management can do is implement accepted best practices and hope that they are both necessary and sufficient to successfully protect the enterprise in a cost-effective manner.

Unfortunately, hope is not a plan, so organizations look to standards bodies for guidance on security best practices. But choosing a best-practices standard or framework to follow is its own challenge. There are many of them and many factors to evaluate, including the standards' similarities to existing organizational practices, costs, complexity, supporting documentation, and—assuming there might not be a single, one-size-fits-all solution that is right for any given organization—even how a standard aligns with other standards.

For example, one best-practice option is the internationally accepted information security standards from the International Organization for Standardization (ISO). The current series of ISO security standards has evolved over the past 12 years to become a well thought-out, well laid-out, and widely accepted set of security best practices, including ISO 27001 and ISO 27002. Over the same time period another set of security best practices has been developed by a US government agency, the National Institute of Standards and Technology (NIST). The NIST 800-Series of Special Publications (SP 800) is now the standard for security for US federal government agencies, third-party providers of services to agencies, and business subject to federal legislation, including HIPAA.

FIGURE 1 COMPARISON OF ISO 27002 PDCA AND NIST SDLC APPROACHES

Fundamentally, the two standards are similar. Unlike the widely implemented ISO security standards, however, NIST is generally ignored outside of the relatively small realm of federal agencies and their contractors. This is an unfortunate twist of exposure and perception—and a product of the managerial tendency to seek a single best-practice reference. But within a broader perspective, the two standards are well aligned; both supplementary and complementary to each other. The ISO standard is generally geared towards higher-level, management practices, while NIST guidance explores more tactical, organizational issues. Taken together, the two standards can provide a comprehensive approach to risk management for IT assets. Each could be used to support the implementation of the other, and collectively they could form the backbone of a comprehensive, sustainable, and defensible global information security practice.

It's time organizations removed their regulatory blinders and started looking at outward to better protect within.

A HIGH-LEVEL VIEW OF ISO 27002 AND NIST 800-SERIES STANDARDS

Both NIST and ISO standards indicates a security process: ISO recommends a "plan, do, check, act" (PDCA) process, while NIST prescribes a systems development lifecycle (SDLC) approach involving initiation, development, acquisition/implementation, operation/maintenance, and disposal. Figure 1 compares the two processes.

There is clear overlap between the two standards, and their recommendations are relatively well aligned. Of the two models, the NIST model is more closely aligned with conventional system planning and development cycles. In contrast, the ISO PDCA approach is more oriented toward systems that are already in production. However, the bottom line is that both models provide a structure with which information security managers may successfully plan, implement, operate, and monitor a risk-based security solution.

Both standards leave a lot of room for interpretation. Depending on your perspective, this could be both good and bad. Room for interpretation allows some flexibility and a level of reasonableness that isn't found with more prescriptive standards. Unfortunately, it also engenders confusion, since explicit practices that are not stated can be of greater concern than stated guidance.

Critical Success Factors

Both ISO and NIST standards define numerous success factors. In general, ISO guidance tends to be high-level and generic, with an emphasis on communication and cooperation. By contrast, NIST guidance tends to be more tactical, with an emphasis on individual responsibility, team-member competence, and cooperation between members of the IT organization. In reality, both sets of guidance are of value, however, since successful risk management requires strategic planning, strong communications, support, project management, execution and follow-through.

TABLE 1 TOP 10 CRITICAL SUCCESS FACTORS INDICATED BY ISO 27002 AND NIST 800-SERIES STANDARDS

SUCCESS FACTOR	COMMENTS
1 Information security policy is tied to the objectives of the business (Source: ISO)	Information security must be discussed in business terms; otherwise, it's impossible to measure the success or failure of the policy in relation to the success or failure of the business
2 The organization develops and follows a risk-management approach and framework consistent with the organizational culture (Source: ISO)	Different organizations approach and solve problems in different ways. The information culture is rarely discussed in NIST documentation, but it must be considered, regardless of whether the organization is private or public
3 The organization obtains and shows visible support and commitment from all levels of management (Source: ISO)	Management must show ongoing visible support for the information security plan through written and verbal means
4 Senior management is committed to the information security plan and committed to fund information security management activities (Sources: ISO, NIST)	If senior management does not support the information security project, the project will fail—or, at best, limp along until there is a change in senior management. NIST and ISO offer little funding guidance; however ISO pertinently observes, "Action to prevent nonconformities is often more cost-effective than corrective action."
5 The IT team provides full support and participation (Source: NIST)	The IT team bares the brunt of the work associated with the assessment, audit, and remediation aspects of information security programs. Constant communication is critical to achieve and maintain buy-in by team members.
6 The risk assessment team must be competent (Sources: ISO, NIST)	The team involved in the risk assessment must have the expertise needed to effectively assess systems, identify risks, and provide cost-effective solutions to mitigate risks
7 Effective marketing and distribution of information security guidance to all parties promotes awareness (Source: ISO)	Security guidance, standards and polices must be distributed and sold to all managers and employees. A given security plan might be world-class, but is destined for failure without a successful internal sales and marketing effort.
8 The organization provides appropriate security awareness training to members of the user community (Source: NIST)	When users understand the implications of their actions and their power to impact security effectiveness, acceptance of the security plan is greatly enhanced
9 The organization establishes an effective information security incident-management process (Sources: ISO, NIST)	ISO and NIST both define incident response as a critical component of risk management. NIST SP 800-53 defines incident response in the IR section of controls; ISO 27002 §13 is dedicated to incident response.
10 The organization develops its own guidelines specific to its own needs (Source: ISO)	Both ISO and NIST standards underscore the need to tailor any security plan to the unique requirements of the organization

FIGURE 2 TYPICAL RISK-BASED APPROACH TO INFORMATION ASSURANCE

Table 1.0 is a consolidation and compilation of success factors taken from both ISO and NIST documentation. There are many more factors for success noted in the guidance than are listed in the table, but the table presents the top 10 factors, based on analysis of both standards.

A RISK-BASED APPROACH

Both ISO and NIST define a risk-based approach to security management. Both focus on assessing the potential impact on information confidentiality, integrity, and availability (CIA) as the basis for all security discussions. Figure 2 depicts the basic risk management process followed by both standards.

As previously noted, ISO is more focused on higher-level and management practices, while NIST tends to delve more deeply into tactical, organizational issues. Together, the two standards provide a comprehensive approach to risk management for IT assets. All six steps noted in Figure 2 are critical for successful risk management, and at each step there is significant overlap of ISO and NIST guidance.

Two steps in which integration of the guidance offers significant benefit are defining the scope of the project (Figure 2, Box 1) and selecting appropriate security controls for risk treatment (Figure 2, Box 4). While success of these two steps won't guarantee overall project success, failure at either step almost certainly guarantees project failure. Therefore, anything that might be done to increase success at either step increases the likelihood of success of the entire project.

The next section discusses these two areas more specifically and explores how the integration of ISO and NIST guidance offers significant value to a Chief Information Security Officer (CISO) or compliance officer attempting to implement either standard.

Definition of Scope and Control Selection

Scope definition involves the establishment of boundaries for and classification of the IT environment and its assets. A well-defined boundary supports well-defined risks and vulnerabilities, which lead to well-defined risk treatments, and so on. Conversely, poorly defined boundaries set the stage for a difficult and high-risk risk management process. ISO offers a high-level starting point for scope definition by providing excellent guidance on defining risk management boundaries in relation to the business:

> Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope. (Source: ISO 27002, 4.21.a)
>
> The scope of a risk assessment can be either the whole organization, parts of the organization, an individual information system, specific system components, or services where this is practicable,

The concept of a security accreditation boundary is not unique to NIST. Although certification and accreditation are never explicitly mentioned in ISO 27002, they are implied as a component of the ISMS audit. NIST dedicates a document, NIST SP 800-37[2] "Guide for the Security Certification & Accreditation of Federal Information Systems to describing the C&A process. This guide provides excellent value to CISO and Compliance Officers attempting ISO compliance.

> realistic, and helpful. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3[1] (Guidelines for the Management of IT Security: Techniques for the Management of IT Security). (Source: ISO1779:2005, 4.1)

NIST also defines management of risk in relation to the enterprise; however NIST's unit of measurement for defining boundaries is the "System."

> System Characterization—focus on accreditation boundaries and establish ownership. (Source: NIST SP 800-30, 3.1)

In both standards, boundary decisions are left to the discretion of the authorized officials. Again, this lack of specificity provides opportunity for both flexibility and confusion. It places more pressure on officials to establish boundaries, while at the same time it gives them flexibility to define boundaries in highly tailored ways. For government agencies, a system is usually defined by mission or application; for example, a personnel management application and all of its associated servers, workstations, and employees access might be considered a single "system." Systems might also be designated by security classification, location, or operating system. A small agency might have just one system.

Commercial organizations define ISMS boundaries using similar criteria, although ISO provides less guidance than NIST on this issue. For government networks, system boundaries are directly tied to system classification. NIST's Federal Information Processing Standards Publication (FIPS) 199[3] and SP 800-60[4] define the process of system classification. At the highest level, there are three classes of system impact: low, moderate, and high. Many managers assume incorrectly that these level designations refer to secrecy levels, making the classification system unique to government environment. This is a fallacy, however, since a high-impact system can be dedicated to unclassified information. The operative word in the determination of level is *impact*. Classifications are directly related to the potential impact on the organization of losing a system or a significant portion of a system. Levels are therefore only indirectly related to the secrecy of the information processed by the system. NIST SP 800-60 defines a comprehensive list of information types with associated levels of impact on information confidentiality, integrity and availability:

---

[1] ISO/IEC TR 13335-3, "Guideline for Management of IT Security-Part3: Techniques for the Management of IT Security. 1998. Available for purchase at http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=21756

[2] Ross, Ron, et al. "Special Publication 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems." National Institute of Standards and Technology (NIST). May 2004. Aug 28, 2007. http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

[3] "Standards for Security Categorization of Federal Information and Federal Information Systems." National Institute of Standards and Technology (NIST). Feb 2004. Aug 28, 2007. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

[4] Barker, William C. "Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories." National Institute of Standards and Technology (NIST). Jun 2004. Aug 28, 2007. http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf

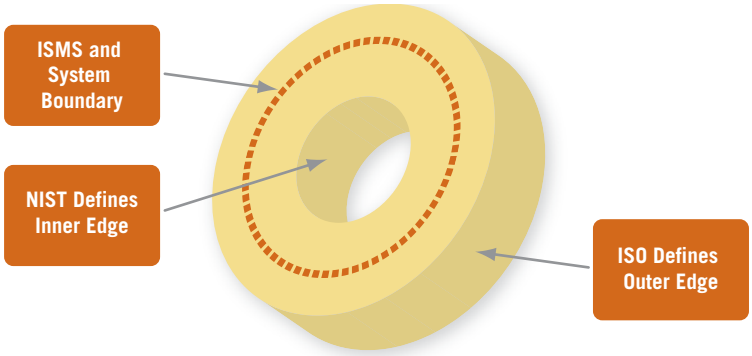


FIGURE 3 BOUNDARY DEFINITION ISO AND NIST

- If the potential impact is "limited with a minimal impact," the system may be classified as "low impact"

- If the potential impact is "serious," the system may be classified as "moderate impact"

- If the potential impact is "severe or catastrophic," the system may be classified as "high impact"

System classification can be a very complex process, since a defined system might process many different types of information, each with its own CIA impact levels. To simplify matters, NIST employs the "high water mark" concept, tying a system's total impact level to the highest-impact information-type classification. For example, if a system processes 10 information types, with 9 low-impact types and 1 high-impact type, the entire system must be considered "high" impact. Similarly, ISO 27002 accounts for information sensitivity in the assessment of controls that are needed to minimize risk—although, in comparison, ISO doesn't offer the level of guidance that NIST provides. The end-result for ISO is the same, however: a series of controls related to minimizing impact on CIA. Only the process of getting to the end result is much more logical and well supported in NIST documentation than in ISO 27002.

Redefining the Boundary Concept

As mentioned previously, boundary definition is one of the most critical steps in risk management. Traditionally, boundaries have been considered static and defined on the basis of physical demarcation points: mainframe, server, firewall, router, intranet, extranet, and so on. As applications have become more distributed, firewalls have become more transparent and the boundaries between intranet, extranet, and Internet have dissolved. The traditional concept of system boundaries are of little value in today's risk management discussion.

Today's boundaries must be defined in dynamic terms: fluid, flexible, resilient, intelligent, business driven, etc. Rather than thin lines dividing "in" and "out," "us" and "them," etc., boundaries can be conceptualized in more of a doughnut shape, as depicted in Figure 3. Outer edges are defined by management, policy and business mission; inner edges are defined by lower-level characteristics, such as information type, classification, access requirements, hosting requirements, and so on.

From a practical perspective, using NIST and ISO guidance is very helpful in defining this type of dynamic system/ISMS boundary. As shown in Figure 3, ISO guidance may be used to define the outer edge of the boundary, while NIST guidance defines the inner edge. Together, the combined guidance provides a boundary definition that is broad enough to meet high-level business requirements, yet sufficiently detailed to meet the more tactical, technical requirements of risk management.

Control Selection as a Key Aspect of Risk Treatment

Along with boundary definition, risk treatment is a make-or-break component of risk management covered in both ISO and NIST guidance. The choices for risk treatment as defined by both sets of guidance are the same:

- Implement security controls
- Modify systems to reduce risk
- Accept risk
- Transfer risk (buy insurance, outsource, etc.)

Typically, management spends the majority of its efforts on the definition and selection of security controls. After all, it's generally easier to implement a control than to redesign a system, so CISOs are reluctant to accept risk if they can instead reduce it with a control implementation. (The third option, offloading risk, is usually a last resort). Admittedly, the preference for control definition over system redesign might be stronger with government CISOs than for commercial CISOs, since the government CISO has fewer options for transferring or accepting risk. Nevertheless, NIST and ISO recommendations for security controls are almost identical.

The two standards do categorize controls a little differently; NIST defines 17 classes of controls, while ISO defines 9 classes. And there are a few areas of divergence in the standards, which are discussed in the next section of this paper. In general, however, the controls in NIST SP 800-53 and ISO 27002 are defined by three components: a control section, a supplemental guidance section and a control enhancements section (called "other information" in ISO 27002). The control sections define controls and provide a placeholder for user-specific control-related information. For example a control might be related to audit logs and the user-specific information would be the type of audit logs to be monitored. The supplemental guidance sections delve into more background information on the control, and NIST also cross-references its controls against other federal regulations and standards. Finally, the control enhancements sections provide recommendations for strengthening the control, if necessary. Both ISO and NIST disclaim their sets of controls as a "starting point," advocating implementation of additional controls to meet the unique characteristics of the systems being protected. ISO also contains a handy section that distills a small set of essential controls from the much larger group of common controls, creating a "legislative essentials" control group honed for regulatory compliance. These include:

- Data protection and privacy of personal information (§15.1.4)
- Protection of organizational records (§15.1.3)
- Intellectual property rights (§15.1.2)

Controls ISO defines as common practice for information security include:

- Information security policy document (§5.1.1)
- Allocation of information security responsibilities (§6.1.3)
- Information security awareness, education, and training (§8.2.2)
- Correct processing in applications (§12.2)
- Technical vulnerability management (§12.6)
- Business continuity management (§14)
- Management of information security incidents and improvements (§13.2)

NIST also offers control groupings and separation of universal controls from unique controls, but nowhere in the NIST documentation is selection of security controls for information protection defined as succinctly as it is in ISO 27002.

But, while ISO excels at defining high-level categories for controls, NIST shines at a tactical level by grouping controls into three categories: operational, technical and management. The allocation of controls into functional areas is helpful, particularly in light of NIST's recommendation that organizations select controls from all three categories. Typically, the type of person assessing and recommending controls is a technical person, and the guidance to implement operational and managerial controls (in addition to technical controls) can help overcome the tendency of technical staff to attempt to shoehorn management

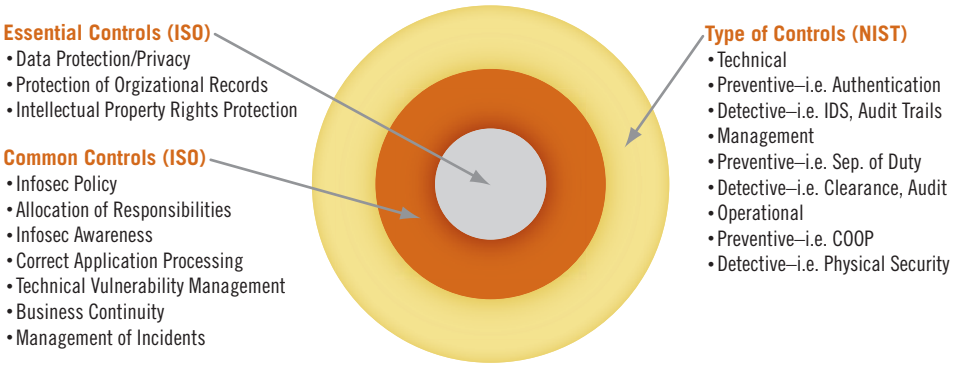


FIGURE 4 INTEGRATION OF ISO AND NIST SECURITY CONTROLS GUIDANCE

controls into technology solutions—a classic expression of the maxim, "when you only have a hammer in your toolbox, everything starts to look like a nail." NIST's control groupings force the auditor, CISO, or compliance officer to consider both technical and non-technical approaches to risk mitigation.

A Harmonized Approach to Control Selection

The successful selection of security controls is a critical component of IT risk management. Since ISO and NIST recommend essentially the same controls, control selection should be a relatively straightforward process. Unfortunately, with 133 controls listed in ISO 27002 and 172 controls listed in NIST 800-53 alone, the process can be quite complex and time consuming—especially when you consider the need to measure the performance of each control. Facing a mountain of control choices, it's easy to get bogged down in the details and lose sight of the overall goals of the project.

What's needed is a top-down approach to control selection. As shown in Figure 4, combining ISO and NIST guidance for control selection fits well into a top-down approach. ISO provides guidance for essential and common controls while NIST offers more detailed perspective on the division of the controls into operational, management, and technical categories. CISOs and compliance officers can use the cumulative guidance to create a tool-selection framework that meets the overall risk management goals, while providing a level of detail needed to make a balanced control selection.

STANDARD VARIATIONS

The discussion to this point has repeatedly stressed ISO's bent towards high-level risk management guidance, in contrast to NIST's more focused and tactical guidance. Put another way, ISO is far less prescriptive than NIST. This disparity raises several questions. How prescriptive should a standard be? How much guidance should a standards body provide? Is it better to lay out a menu of all options or segregate options into functionally targeted templates?

In general, NIST tends to parse controls into functional templates, while ISO tends to follow a "clean slate" approach that assumes each project starts from scratch. Possibly, this reflects the inherent differences between an international standard that must support all organizations, irrespective of local laws and customs, and a federal standard that need only support a relatively uniform group of governmental agencies. Even so, IT systems are IT systems, regardless of the owner. Types of risks are fairly universal, as are methods for risk mitigation. Therefore, this issue of approaching IT risk mitigation as a "clean slate" or via "templates" isn't a "governmental" or "commercial" issue, but rather an issue of managerial preference. Both approaches are designed to get a CISO or compliance officer to the same end-point: a successful risk-based approach to security.

This author's preference is for template over clean slate. The reasons for this are threefold:

1 **Process efficiency**–CISOs and compliance officers are busy with operational, managerial, and compliance responsibilities; anything that streamlines the planning and implementation processes without introducing additional risk is a benefit. If a preset baseline template streamlines management's ability to select appropriate controls, it might offer significant advantage.

2 **Time efficiency**–Despite what vendors and consultants say, choosing information security controls is not rocket science. If anything, security risk management is more of an art than a science. Threats and vulnerabilities tend to be universal, as are approaches to protecting against them. Managerial science and art should be applied to the adjustments required to meet the unique characteristics of the organization, as opposed to redefining commonly accepted best practices of information protection. Leveraging supplied templates and baselines reduces the need for the CISO or compliance officer to spend time on building the control baseline from scratch and allows them to move more quickly into tailoring general guidance to specific organizational needs.

3 **Knowledge and cost efficiencies**–The amount of knowledge required to build an ISMS from scratch, including definition of the information system, risk assessment, treatment of risk, and implementation of a risk management plan is great. ISO 27002 and NIST standards pre-codify much of this knowledge, providing a readily-accessible springboard of expertise and generally accepted best practices from which organizations can launch their own programs. Most CISOs and compliance officers rely upon outside consultants to guide them through the process. The more detailed the level of expertise provided (as in templates and explicit baselines), the less need for outside consultants. Another way of looking at this is that a template-based approach keeps expensive consulting resources focused on the hard work—fine tuning standards to meet the unique requirements of the organization.

Latitude for New Technologies

How is the management of risk associated with new technologies addressed in ISO and NIST standards? In theory, the standards are open ended and the disclaimer that "additional controls" may be required leaves the door open for incorporation of new technologies. This is another area in which the use of both standards can facilitate compliance with either standard.

Despite what vendors and consultants say, choosing information security controls is not rocket science. If anything, security risk management is more of an art than a science.

For example, nowhere in ISO 27002 is Voice over IP (VoIP) mentioned. By contrast, SP 800-53 has a specific security control for VoIP, as well as a reference to NIST SP 800-58 for additional security considerations for VoIP. Wireless network security is another area that NIST addresses more explicitly than ISO. Both standards reference wireless, but NIST cites specific controls for wireless access, and SP 800-48 discusses wireless access with a particular emphasis on the 802.11x and Bluetooth standards. Finally, the US government's emphasis on migration to IPv6 is driving NIST's development of a specific set of protocol security controls. These controls are also relevant to organizations attempting to comply with ISO 27002.

External Parties

Both ISO and NIST discuss the need to protect information systems that are either hosted by, managed by, located at, or belonging to third parties. Both ISO 27002 and NIST SP 800-53 offer specific security controls for third-party relationships. Of the two, ISO 27002 Section 6.2 provides far more guidance than NIST on risk management of third-party relationships, however. Federal CISOs can leverage this ISO guidance, particularly in light of the US

government's motivation and mandate to outsource competitive IT services.

CONCLUSION

The initial intent of this research was to better understand the standards by focusing on their differences. An early assumption was that the unique requirements of government agencies should mandate a different package of information security controls than a commercial organization would require.

What became clear during the research process, however, was that ISO and NIST information security standards are closely aligned. This either means that the security problems faced by government agencies are not much different from those faced by commercial organizations or that there is a serious disconnect between federal IT executives and the NIST standards makers.

Given the openness of the NIST standards development process and the professionalism and experience of the NIST team it's highly unlikely that the federal standards are misaligned with the federal requirements. It's much more likely that management requirements of public and commercial organizations are similar.

If you accept the validity of NIST's control recommendations for broader enterprise, application of the guidance in conjunction with ISO 27002 presents new opportunities and efficiencies. Referencing both ISO 27002 and NIST 800-Series standards as a cumulative reference point for a comprehensive information security practice provides more breadth and depth of guidance than either standard alone. Individually, each standard offers necessary information, but is not necessarily sufficient to achieve compliance. It's time organizations took off their regulatory blinders and reached outward to better protect within.

APPENDIX 1: BACKGROUND

FISMA and NIST

The Federal Information Security Management Act (FISMA) originated as Title III of the 2002 E-Government Act. FISMA mandates that government agencies develop, document, and implement information security to protect the assets of the agency including assets that are provided or managed by another agency, contractor or other party. FISMA is often referenced in conjunction with the Office of Management and Budget (OMB) Circular A-130, Appendix III: Security of Federal Automated Information Resources. FISMA and A-130 emphasize a risk-based approach to protection of assets. FISMA references a series of documents that are written and managed by the National Institute of Standards and Technology (NIST). Core documents include:

- NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems"
- NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems"
- NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems"
- NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems"
- NIST Special Publication 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems"
- NIST Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System"
- NIST Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories"
- FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"

- FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information. Systems"

The bulk of this paper is focused on SP 800-53 and SP 800-30.

ISO 27000 Series

ISO documents for information security are developed jointly with the International Electrotechnical Commission (IEC) and fall in the 27000 category of standards. Technically entitled "ISO/IEC", they are often (and in this document) referred to as simply "ISO." The series includes the seminal ISO 27001 and ISO 27002 standards, as well as others.

ISO 27001 was first published as BS 7799 in 1995 by the British Standards Institute (BSI). The original BS 7799 was divided into two sections: risk management process and security controls. In October, 2005 the risk management component (revised BS 7799 Part2:2005) was adopted as ISO/IEC 27001, "ISMS–Requirements." Essentially, ISO 27001 defines the Information Security Management System (ISMS) requirements and references ISO 17799:2005 for suitable information security controls. After review and discussion, the security component of BS 7799 was adopted in 2000 as an ISO standard numbered 17799:2000. With revision of the standard in June 2005, the publication number was changed to 17799:2005, also called the "Code of Practice for Information Security Management." As of 2007, ISO 17799:2005 has been renamed ISO 27002:2005, in order to bring the document number in line with ISO's 27000-series of security standards. ISO 27002 content is identical to ISO 17799 content.

Although ISO 27001 and 27002 are the most widely recognized information security standards published by ISO, they are actually part of a larger series of security related documents. The series includes:

- ISO 27000: Information systems, information technology, and ISMS overview and vocabulary
- ISO 27001: Information systems, information technology, and ISMS requirements
- ISO 27002: Information technology and security techniques code of practice for information security management
- ISO 27003 (under development): ISMS implementation guidance
- ISO 27004 (under development): Information security management measurement
- ISO 27005 (under development): Information security risk management (based on and incorporating the ISO/IEC 13335 standard for management of information and communications technology security)
- ISO 27006: Information technology security techniques and requirements for bodies providing audit and certification of information security management systems

AUTHOR BIO

Ted Ritter has more than 20 years of experience in information assurance, telecom technology management, business development, marketing, and sales. He is currently an analyst with Nemertes Research, an IT advisory firm. Prior to joining Nemertes, Ritter was principal of iTRitter, an information security consulting firm. He also built a cybersecurity practice at Intelligent Decisions, a federal systems integrator, growing the company's security business from less than $200K to more than $8M in two years. A published author and international speaker, Ritter has performed extensive research on regulatory compliance tools and their value (or cost) in corporate governance, risk, and compliance (GRC) processes. Ritter's education includes a BA in Neuroscience from Oberlin College and an MA in Telecommunications Management from The George Washington University.

Relying on conventional key-encryption technologies, IT staff might be forced to manage several distinct symmetric key-management infrastructures, each with its own technology, training, documentation, procedures and audits. Clearly, key-management capability needs to be abstracted from the applications that use it.

Symmetric Key Management Systems

Arshad Noor

The time has come for the information security (infosec) community to address Symmetric Key Management Systems as an application-independent, enterprise-level defense mechanism.

RELATED GUIDANCE

PCI DSS

CA SB 1386

Most security professionals are familiar with symmetric key-based cryptography when presented with terms such as Data Encryption Standard (DES), Triple DES (3DES) and the Advanced Encryption Standard (AES). Some are also familiar with Public Key Infrastructure (PKI) as an enterprise-level solution for managing the life-cycle of digital certificates used with asymmetric-key cryptography. However, the term Symmetric Key Management System (SKMS)—which refers to the discipline of securely generating, escrowing, managing, providing access to, and destroying symmetric encryption keys—will almost always draw blank stares. This is not surprising, because symmetric encryption key management has traditionally been buried in applications performing encryption. These applications primarily focused on business functions, but managed encryption keys as an ancillary function. Consequently, there was no reason to emphasize key management. This article advances the notion that the time has come for the infosec community to address SKMS as an application-independent, enterprise-level defense mechanism that is more effective when addressed separately.

While encryption has been in use for centuries,[1] computer-based cryptography entered the general computing field with the advent of the DES algorithm. The primary business uses for this technology was within the military, and later banking. Given the nature of what encryption technology was protecting, implementers were willing to live with custom key-management solutions, however contrived they may have been. With the explosion of the World Wide Web, businesses have been racing to implement business processes on the Internet, bringing sensitive information significantly closer to attacks.

Although businesses have invested billions in firewalls, intrusion detectors, intrusion prevention systems and other defense mechanisms, the US has witnessed more than 300 breach disclosures[2] since the passage of California's Breach Disclosure law.[3] One recent disclosure was from the University of California in Los Angeles (UCLA).[4] This is the seventh[5] breach disclosure by the University of California across all schools in the UC system, and it reflects a situation completely out of control. Breaches at retailers such as Ralph Lauren, BJ's, DSW and credit card processing companies such as CardSystems Solutions have prompted credit card giants Visa,

1 History of cryptography. http://en.wikipedia.org/wiki/History_of_cryptography

2 A Chronology of Data Breaches. http://www.privacyrights.org/ar/ChronDataBreaches.htm

3 California Senate Bill 1386. http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

4 Breach at UCLA exposes data on 800,000. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005925

5 California Senate Bill 1386 Disclosures of Breaches to PII. http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Mastercard, American Express and Discover to standardize on security requirements for merchants and card-acquirers through the Payment Card Industry's Data Security Standard (PCI-DSS).[6] One critical element required within PCI-DSS is the encryption of credit card numbers and a robust key management system to accompany encryption.

RATIONALE

Why is symmetric key management a problem? After all, applications seem to have addressed the problem within the applications for decades, and appear to be continuing to do so. The problem becomes obvious if you are in IT Operations. As an illustration, if you are responsible for managing a point-of-sale (POS) application that accepts credit cards for payment, an e-commerce application that requires credit cards for payment, a payment processing application that communicates with the credit card network for settling transactions, a back-office database that consolidates transactions, and a business analytics application for determining retail fraud, you have five applications that require encryption.

In addition, with the proliferation of laptop and PDA losses and thefts, companies are now mandating encryption on these devices, adding one or two more key-management schemes to the infrastructure. Add database and operating system-specific encryption to the mix, and you round out the picture with at least 8 to 10 key-management infrastructures.

Since applications are typically purchased from multiple vendors, each vendor, focusing primarily on its own business application, implements encryption and performs key-management functions using its own design. As a result, the IT Operations staff are forced to manage at least 8 to 0 distinct symmetric key-management infrastructures, each with its own technology, training, documentation, procedures and audits. (PCI-DSS regulated entities are required to perform annual audits of any system that stores credit cards.) Not only does this border on the ridiculous, more importantly, it raises total cost of ownership (TCO). One might even argue the potential danger of a vulnerability in the security strategy, because, with so many pots cooking on the stove, something could get burned.

SOLUTION

Presented with the problem in this perspective, the logical solution springs to clarity: the key-management capability needs to be abstracted from the applications that use it. Such a solution is not unlike the Domain Name System (DNS) for hostname-IP address resolution, or a Relational Database Management System (RDBMS) for data management.

In 2006 an open-source software product was released on the Internet that struck at the heart of this problem.[7] Architected along the lines of DNS, the completely free software abstracts symmetric key management functions from applications and consolidates them on one or more centralized Symmetric Key Services (SKS) servers on the network. Using a client-side API, applications on most platforms can make requests for symmetric key services without knowing the semantics of symmetric key management. Designed to be extremely secure, the SKMS architecture also allows for business continuity in the face of network failures, massive scalability and the use of many well-understood technical standards.

ARCHITECTURE

An SKMS, as defined within the context of this architecture, consists of at least two centralized SKS servers—a primary and a disaster recovery server—and any number of clients using the Symmetric Key Client Library (SKCL) to request services from the SKS servers. (While they are referred to as clients, the client software may themselves be database servers, web servers, application servers and/ or any business application.) The XML-based protocol between the SKCL and the SKS servers, known as the Symmetric Key Services Markup Language (SKSML), has a technical committee (open to anyone) that formed recently at OASIS to consider standardizing this protocol on a royalty-free basis.[8]

6 PCI Security Standards Council. https://www.pcisecuritystandards.org/index.htm

7 StrongKey. http://www.strongkey.org

8 OASIS Enterprise Key Management Infrastructure Technical Committee. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi

Each SKS server consists of:

- A server-class computer running an operating system—typically Linux, UNIX or Windows—that has a compliant Java Virtual Machine (JVM) available for it
- A relational database that serves as the storehouse for the symmetric encryption keys
- A J2EE-compliant application server to respond to requests over the network, serving as the workhorse of the SKMS
- A JCE-compliant cryptographic provider to perform the cryptographic operations of key generation, key protection, digital signing, verification, etc.
- An optional, but strongly recommended, Hardware Security Module (HSM) or Trusted Platform Module (TPM) for securely storing the cryptographic keys that protect the database's contents
- The SKS server software itself, consisting of an Enterprise Archive (EAR) and a Web archive (WAR) file for the administration console, along with ancillary utilities

Each SKCL client platform consists of:

- A client machine running an operating system—once again, typically Linux, UNIX or Windows, but includes the OS/400—that has a compliant Java Virtual Machine (JVM) available for it
- A JCE-compliant cryptographic provider to perform the cryptographic operations of encryption, decryption, digital signing, verification, etc.
- An optional, but highly recommended, Trusted Platform Module (TPM), smartcard or other USB-based cryptographic token for securely storing the cryptographic keys that protect the clients' authentication credentials
- The SKCL software itself, consisting of an API callable by Java applications for communicating with the SKS server and performing cryptographic functions (non-Java applications have the option of either using a Java Native Interface (JNI) library to call the SKCL, or communicating with the SKS server directly using the SKSML protocol)
- The SKSML protocol itself is extremely simple, and consists of:
- A call from the client to request a symmetric key—new or existing—from the SKS server
- A call from the client to request key-caching policy information from the SKS server
- A response from the SKS server containing the symmetric key and the key's use policy
- A response from the SKS server containing the key-caching policy
- A fault message from the SKS server, if either of the two calls does not succeed

SECURITY FEATURES

Given the sensitivity of the information managed within the SKMS, the architecture is predicated on an extraordinary level of security. (As with any security architecture, the controls and procedures in place at any specific implementation determine the degree of vulnerability the SKMS will have against attacks, so please don't assume these controls are bulletproof and you can skimp on other aspects of security.)

The SKMS incorporates the following security features:

- All symmetric keys are generated using any number of compliant cryptographic providers, thus allowing sites to use whatever level of sophistication is desired for their implementation
- All symmetric encryption keys are themselves encrypted using multiple RSA asymmetric keys
- All database records on the SKS server are digitally signed before storage, and verified upon retrieval to ensure their integrity hasn't been compromised
- All administrative operations through the console are digitally signed and maintained in a history log for audit purposes, and verified upon retrieval

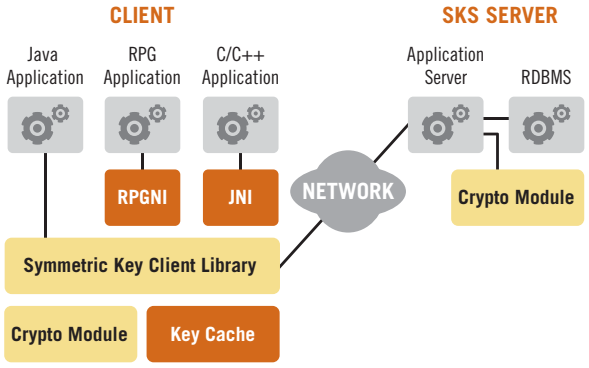


FIGURE 1 SYMMETRIC KEY REQUEST

- All administrative operations through the console require SSL/TLS-based client authentication
- Only digitally signed client requests are accepted by the SKS server from SKCL clients
- Only digitally signed responses from the SKS server are accepted by SKCL clients
- All symmetric keys are transported, encrypted for the specific client making the request
- All cached keys on the client are digitally signed and encrypted on storage, decrypted and verified upon retrieval to ensure their integrity
- All private keys of the digital certificates can be stored on FIPS-certified cryptographic tokens ranging from software to smartcards, TPMs to HSMs, to ensure their security

OPERATIONS

Refer to Figure 1 for the following discussion.
When a client—be it a laptop, a DB application or an e-commerce Web server—needs a symmetric key to encrypt some information, it makes a request for a new symmetric key to the linked-in SKCL (or directly to the SKS server if it has implemented the protocol itself).

The SKCL checks its key-cache to determine if it has any cached symmetric keys that are valid for use. If so, it retrieves the key, decrypts it, verifies its integrity, checks its KeyUsePolicy (every symmetric key object has an encryption policy embedded in it, previously defined by the site Security Officer) and then hands the requesting application the symmetric key for use. If the application chooses not to use the SKCL for the actual encryption/decryption operations, it is expected to use the key in conformance with the embedded Key-UsePolicy.

If any of the local checks result in no valid symmetric key being available for use, the SKCL creates a new symmetric-key request, digitally signs it with its authentication credentials, and sends the request to one of its pre-configured SKS servers as an OASIS Web Services Security (WSS)-compliant SOAP request. It is noteworthy to mention here, that since all requests and responses between the SKCL and the SKS servers are secured (digitally signed and encrypted) at the message level, transport-level security (SSL/TLS or IPSec) is not required for the operations of the SKMS; plain old HTTP is sufficient. Administration console communications, however, do rely on mutually authenticated SSL/TLS sessions.

The SKS server, upon receiving such a request, verifies the authenticity and integrity of the request, determines the authorization and the symmetric-key policy in force for the requester (or the default policy), generates a new symmetric key based on this policy, assigns it a Global Key-ID (GKID), escrows the key (which includes encrypting it with multiple RSA keys), encrypts the key with the requester's transport digital certificate, logs the transaction details (which includes digitally signing the transaction) and responds to the client with a WSS-compliant SOAP response.

The SKCL client, upon receiving the response, verifies the authenticity and integrity of the request, caches the secured object if so configured, decrypts the symmetric key and the embedded key-use policy, and returns it to the calling application. The calling application at this time may choose to have the SKCL perform the actual encryption, or perform it itself.

A similar process is repeated when a client application needs to decrypt a previously encrypted object such as a file, directory of files, database record, etc. The application determines the GKID of the symmetric key it needs (which would have been previously stored with the encrypted ciphertext) and makes a request for this key to the SKCL. The SKCL checks

to see if the requested key is in the key-cache. If it is, it goes through the standard security checks and returns the symmetric key to the application; if not, it makes a request to the SKS server for this symmetric key. Upon receiving the request and after the standard security checks, the SKS server responds with the symmetric key to the client. If the key does not exist for any reason, or the client is not authorized to receive the key, or for other error conditions, the SKS server returns a SOAP Fault to the requesting client.

It is noteworthy that, given this operational infrastructure, use of a unique symmetric key to encrypt every record in a database is feasible. With such an encryption policy, the breach of any key reduces the exposure of the database down to just a single record. This is in stark contrast to existing designs, where a single key typically encrypts an entire database or dataset, thus magnifying the loss associated with the loss of that single key.

IMPLEMENTATION

The construction of an SKMS will typically begin with the creation of a PKI—or procurement of PKI services—to manage the issuance of digital certificates to every client. The architecture deliberately eschewed the use of User ID/Password for authentication because of their inability to prevent attacks against single-factor credentials. The clients and servers in an SKMS use digital certificates for authentication, and secure storage and transport of symmetric keys within the infrastructure. (Notwithstanding the use of digital certificates, the administration console allows an Operations or Security officer to "deactivate" any client or server on the SKMS network without revoking the digital certificate of the affected entity.)

Simultaneously, the application that will use the SKCL is modified to integrate the API and accommodate the encrypted data (ciphertext) and the GKID in its database. This raises a valid question of commercial off-the-shelf (COTS) software: How does one use the SKMS if a specific COTS at a site does not support it? Currently we are at a stage of the SKMS' evolution, just as DNS and RDBMS were at their inception. Before the creation of these "abstraction" technologies, applications had to resolve hostname-IP addresses and perform data management on their own. As DNS and RDBMS protocols and APIs became standards, application developers abandoned their proprietary implementations to adopt industry standards—the monetary benefits were too good to ignore. It is anticipated that SKSML will be adopted faster than DNS and the RDBMS, because of the same benefits that would accrue to independent software vendors, and also due to the regulatory and TCO pressures on IT organizations.

Multiple SKS servers are deployed (installation instructions are available at www.strongkey.org), and encryption policies configured on the servers, while digital certificates are issued to clients that will communicate with the servers. The applications are now ready to start requesting key-management services from the SKS servers. The SKMS transitions to Production status at this point, and traditional operational activities take over (backup, configuration management, DR, etc.).

CONCLUSION

While symmetric encryption has been in use for decades within general computing, we have reached a confluence of inflection points in technology, the Internet and in regulatory affairs, that require IT organizations to implement Symmetric Key Management Systems (SKMS) as independent infrastructures. Using the newly released open-source software, and the soon-to-come Symmetric Key Services Markup Language (SKSML) standard from OASIS, IT organizations have another—and perhaps, one of the most effective—defense weapon in their arsenal against an increasingly hostile Internet.

AUTHOR BIO

Arshad Noor is the architect and primary developer of the open-source StrongKey Symmetric Key Management software. He is also the Chair of the OASIS Technical Committee on Enterprise Key Management Infrastructures that hopes to standardize the SKSML protocol. He can be reached at arshad.noor@strongauth.com.

This paper was originally printed in the ISSA Journal, February 2007. It is reprinted here with permission of the author.

Corporations are free to design responsive e-discovery measures that are reasonable and practical for their size, stature, and IT environment. Against this degree of latitude is counterbalanced the corporate responsibility of addressing, preparing for, and responding to legal e-discovery requests with a strong process and a good-faith program.

Addressing IT Preparedness for E-Discovery: A Control Framework

MARY ANN REICHARD, ESQ., CISA

RELATED GUIDANCE

US Federal Rules of Civil Procedure 16(b), 26(b), 26(f), 34(b), 37, 45

Recent FRCP Amendments. The United States' Federal Rules of Civil Procedure (FRCP) govern the procedural processes for civil litigation in federal court. One important area of particular emphasis within the FRCP is the discovery of evidence, which now includes electronic evidence. Recent amendments to the discovery rules explicitly cover electronically stored evidence, giving rise to the term "e-discovery." E-discovery is the identification, preservation, collection, processing, review, and production of electronically stored information (ESI) for use in litigation.

As of December 1, 2006, the FRCP has been amended to specifically include the discovery of ESI as part of the formal discovery process mandated for federal civil litigation. This change is significant for businesses because it dictates that courts, for the first time, formally require litigants to examine, discuss, and produce ESI that relates to civil court cases.

Prior to the amendments, discovery and production of ESI was at the discretion of the parties and their attorneys. Often, both sides would agree to limit e-discovery to a subset of e-mail or the hard drives of only a few corporate employees. Sometimes discovery was limited to paper-based information, altogether eliminating the need to address the IT aspects of corporate information storage. This approach worked well in some instances. In others, it led to the omission of relevant information, with the result that critical evidence was not brought to the court—either because the parties' were unwilling to dedicate the time and effort required to determine what relevant electronic information they possessed or because the attorneys were uncomfortable with technology and therefore reluctant to pursue any technology-driven discovery efforts.

Under today's e-discovery mandate, however, investigation of a corporation's electronically stored information is a part of standard litigation procedure. To facilitate this paradigm shift in the legal community, corporations must increase their focus on how they manage and track their many sources of ESI.

Both the federal and state bars and the courts are increasing their technical knowledge. The formal guidance in the FRCP notes that it is important for counsel to become familiar with their clients'

information systems, placing the onus of technical competence on the attorney.[1] This, in turn, puts attorneys in a position of engaging in IT operations that impact e-discovery and engages IT and compliance directors at the forefront of the e-discovery response.

INFORMATION RISK MANAGEMENT AND E-DISCOVERY

New e-discovery pressures pose challenges for IT risk management. In addition to managing the security and privacy aspects of corporate information, IT management must now consider information accessibility and identification, as well as content management. Organizations must implement IT-based business processes that utilize technology and incorporate control points to ensure the consistency, repeatability, integrity, and overall defensibility of their e-discovery efforts.

The FRCP updates have dramatically changed the face of legal discovery—and, consequently, corporate information management practices.

One of the greatest challenges to creating a corporate preparedness plan is that most organizations lack a well-defined set of procedure-like rules, such as those they often have in place for many other compliance and regulatory matters. But the new FRCP requirements are not immediately instructive on what form these procedures should take: they are generally broad in nature, outlining the desired end result without voluminous extrapolation on method. The comments to the Federal Rules, along with case law decisions interpreting the Rules, are two of the few additional sources of official guidance. Without an itemized regulatory scheme, a detailed checklist, or defined methodology, corporations are free to design responsive measures that are reasonable and practical for their size, stature, and IT environment. With this level of latitude is counterbalanced corporate responsibility of addressing, preparing for, and responding to legal e-discovery requests with a strong process and a good-faith program.

THE CALL FOR CORPORATE PREPAREDNESS

The FRCP updates have dramatically changed the face of legal discovery—and, consequently, corporate information management practices. Discovery of ESI is now a part of every case in the federal civil court system. By obligating litigants to provide, at a minimum, a list of all locations where ESI relating to a claim or defense might reside, even before a formal discovery request is received, the FRCP effectively requires companies to have an organized, classified system for the management and tracking of all forms of ESI, not just the information within the "records management" files. The complexity and tracking of each ESI source varies greatly depending on its form and structure, as well as the likelihood that the information would fall under a discovery request. These complexity factors notwithstanding, a well-established monitoring baseline should be in place for all sources of ESI.

Moreover, just as preparedness helps a company meet its e-discovery demands, it can also protect a company that inadvertently fails to be able to supply requested information. The FRCP endorse controlled, well-structured information management practices by carving out a sanction-free zone for organizations that can demonstrate they are implementing effective information retention and litigation hold policies and procedures. This so-called "safe harbor" provides legal relief for parties that, due to an inadvertent error, cannot produce requested ESI, despite good-faith efforts, sound policies, and effective operation of their information systems.[2] Although this provision of the FRCP has not yet been interpreted by the courts in any significant fashion, it is clear that in order to be granted protection under the provision,

[1] Comment to FRCP 26(f): "It may be important for the parties to discuss those systems, and accordingly important for counsel to become familiar with those systems before the conference."

[2] FRCP 37(f): "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."

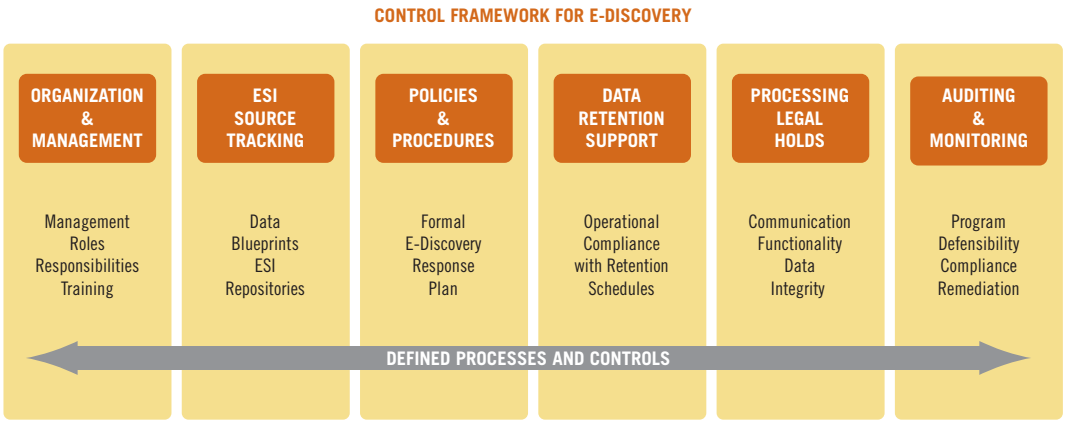


FIGURE 1 COMPONENTS OF E-DISCOVERY, THE IT PERSPECTIVE

organizations must first ensure that they operate a routine, good-faith information system. Ad hoc processes, informal processes, chaotic production, ineffective information hold procedures, and inadequate policy auditing and enforcement cannot support an argument for corporate protection under the safe harbor provision. That argument must begin with a demonstration that the company has effective controls in place to prevent non-production of information needed for legal discovery.

Taken as a whole, these changes require companies to take steps to better manage their information assets, adding another dimension to information risk management and compliance efforts. Companies must learn to manage their information sources by content, rather than size or format alone. And IT must be able to quickly and accurately inform counsel as to where relevant ESI resides and how it can be retrieved, at the same time ensuring that all the information is identified and preserved in a legally defensible manner.

A CONTROL FRAMEWORK FOR E-DISCOVERY

Using a framework of preventative and detective IT controls over e-discovery operations is a way to channel an organization's response to e-discovery requests into a methodological, organized, and compliant business process that is both repeatable and defensible. Successful e-discovery efforts center on strong business processes that surround the information environment in which the discovery game-plan exists.

Six areas outline the components of a corporate e-discovery response from an IT perspective. (See Figure 1.) Implementation of control points within each area leads to the development of a detailed action plan to improve preparedness and efficiently create a baseline level of protection against court sanctions and costly, inefficient discovery.

Control Area 1: Management & Organization

The overarching management and organization of corporate e-discovery is the foundation of a successful response effort. A highly organized team that provides centralized project management enables clear communication and, ultimately, production of responsive information. The corporate e-discovery team should include representation from legal, IT, records management, and representative line-of-business personnel who are familiar with the information generated by their respective departments. The e-discovery team serves as the centralized point of contact for support vendors, legal counsel, and outside experts, as well as a centralized operations point for internal employees.

Establishing the controls supporting "soft" management processes can be difficult, due to the often-undefined and dynamic nature of interpersonal relationships. During the initial team structuring, management should seek to institute clear processes with inherent controls that require a collaborative working environment. This provides a foundation for effective communication and management of e-discovery tasks.

- **Action Item:** Designate a dedicated resource to collaborate with legal and records management staff on e-discovery issues; ideally, within a formal e-discovery response team.

  ➤ **Key Control Points:** Define roles and responsibilities within the e-discovery response team and verify the presence of open communication channels, in order to ensure effective collaboration and information exchange.

- **Action Item:** Training and educate the user community on compliance with information management policies.

  ➤ **Key Control Points:** Create a formal training program with a responsive point of contact for questions and follow-up for legal and records management issues, as well as technical issues. Incorporate the use of trainee feedback and ongoing compliance updates to continually improve the training program.

Organizations must know where they store electronic information and understand, at a high level, the type of content contained within all data stores.

Control Area 2: ESI Source Tracking

Organizations must know where they store electronic information and understand, at a high level, the type of content contained within all data stores. ESI source tracking, as a practice, extends records management concepts to storage repositories outside of traditional records management system. With source tracking, the organization can identify and track content sources in order to quickly report on where relevant ESI might reside. The expansion of content-based management beyond the domain of traditional records management requires strong leadership and support by IT. The goal of ESI source tracking is to apply an information lifecycle management approach to all of the organization's ESI.

- **Action Item:** Create a data blueprint.

  ➤ **Key Control Points:** The blueprint should represent the IT environment's information stores, described for a non-technical audience.

- **Action Item:** Identify and quantify "not reasonably accessible" information.

  ➤ **Key Control Points:** Classifications should be supported by case law (prior decisions) and contain an estimate of the cost and resource burdens that the organization would face if it were required to produce specific ESI.

Control Area 3: Policies and Procedures for Information Management

An organization's plan for responding to e-discovery requests should be formally documented, both for reference and defensibility. Overarching objectives, principles, and guidance should take the form of policy statements. These statements should underscore a disciplined, comprehensive effort and attest to the importance of compliance to upper management. Detailed step-by-step instructions make up the procedural portion of documentation. Written instructions support compliance (increasing the likelihood that the procedures will be carried out as required), help ensure consistency of action, and support the repeatability of all e-discovery processes, from preparedness to production.

- **Action Item:** Update and expand retention schedules to include all reasonable sources of ESI.

  ➤ **Key Control Points:** Records management and legal staff should collaborate to define retention timeframes. IT must identify sources of ESI that are reasonably subject to discovery within the defined timeframes. Some forms of ESI, such as information embedded in RAM memory, do not lend themselves to structured information management. Formal retention schedules cannot

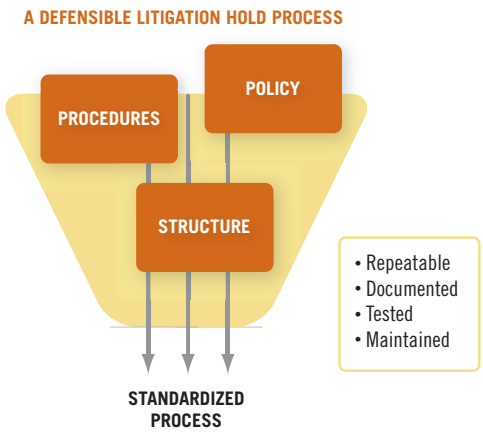


FIGURE 2 COMPONENTS OF A DEFENSIBLE LITIGATION HOLD PROCESS

be reasonably defined for these sources, which should simply be identified as potential ESI sources.

- **Action Item:** Formalize e-discovery response measures.

  - **Key Control Points:** Organizations should use procedural checklists for routine preparedness efforts and document process steps for preserving and securing relevant ESI. The organization may use different procedures, depending on format and type of ESI.

Control Area 4: Support for Data Retention Schedules

Once data retention schedules have been created for the expanded retention schedule, IT is responsible for implementing e-discovery policies; for example, destruction of information that is expired under the retention schedule. ESI in legacy systems, backup tapes, unclassified network shares, and other "orphaned" information sources can present "high-risk" exposure due to the volume of unmanaged information they represent, and the fact that much of the information is expired.

Software and search appliances can aid in the housekeeping effort required for e-discovery by quickly identifying expired information, creating a log of the activity surrounding its disposition, and providing some inherent application-level controls for the e-discovery process. Integrating software solutions into the compliance program can increase the efficiency of e-discovery efforts by reducing the volume of unmanaged information and ensuring that information is retained for the proper period.

- **Action Item:** Apply updated retention schedules to data stores.

  - **Key Control Points:** Organizations should use staged or tiered information deletion to control the final disposition process. A plan for evaluating data stores ensures that the organization takes appropriate action in line with legal requirements and current data retention policies. If practicable, software can help create a disposition audit trail.

- **Action Item:** Document disposition activity.

  - **Key Control Points:** Organizations should cross-reference information deletion sets with legal hold orders to ensure that legally "frozen" data is not modified or destroyed. IT managers should attain legal sign-off prior to deleting information sets.

Control Area 5: Processing Legal Holds

A "legal hold" is a process that suspends the normal deletion or modification of corporate records and information (see Figure 2), thereby preserving the current state for investigative or legal purposes. A hold is required whenever the organization has notice or a reasonable expectation that a matter will go into

litigation, which is often prior to the initiation of formal legal proceedings or the receipt of a formal discovery request. The ability to ensure legal holds is arguably the most important component of the e-discovery response, one that is ultimately carried out by IT. As such, IT must ensure it has the proper policies, operational procedures, and resources in place to preserve and protect information once a hold is required.

An e-discovery control framework provides a systemic foundation for standardization, which helps reduce the risk of e-discovery failures.

Proper implementation of legal holds is central to successful e-discovery. Structured processes and defined control points help ensure that the organization fulfills its obligations to identify, preserve, and produce relevant ESI. Organizations should strive for procedural standardization, which results in routine, repeatable efforts that support efficient, defensible e-discovery. An e-discovery control framework provides a systemic foundation for standardization, which helps reduce the risk of e-discovery failures.

- **Action Item:** Establish automated and manual controls over IT operations supporting the legal hold process.

  - **Key Control Points:** Because the risk of noncompliance in this area is significant, the organization needs a more detailed control framework. Control points can be divided into three types: 1) initiation and communication, 2) system functionality, and 3) data integrity.

    Initiation and communication

    The organization should define a "trigger point" for the execution of a legal hold: standardized hold policies and procedures should be created with the advice of legal counsel and should take into account 1) the organization's past experience with similar matters moving to litigation; and 2) the reasonableness of holding all potentially relevant information, considering the impact on regular business operations and factors such as storage costs, infrastructure demands, and general impact on the IT environment. If there is a question about whether a hold should be instituted, management should err on the side of caution, initiating a hold if the potential for legal action can be argued to exist.

    The organization should identify relevant information for preservation: IT should be a central party in determining where relevant ESI might reside and which ESI should be subject to the legal hold. Legal counsel is likely to look to IT to provide a comprehensive list of all information sources and then work with IT to determine which sources contain relevant information and how IT can suspend the normal deletion or alteration of the information. Decisions about whether information is within the scope of an e-discovery request should include documented rationale and sign-off by involved decision-makers.

    The organization should provide documentation of e-mail correspondence about hold requirements: Use of automated e-mail tracking features, such as delivery receipts, and manual message confirmations and replies can document the communication of e-mail notices relevant to the hold. IT should confirm that e-mail is operating properly and that no interference or routing failures are impeding message delivery. In addition, IT staff should preserve both outgoing e-mails and replies. Routine follow-up reminders about the hold should be sent to ensure continuing compliance with the scope of the hold. IT should also create a central e-discovery mailbox, ensuring that any questions sent to the mailbox are answered in a timely fashion and preserved as a record.

System functionality

The organization should implement a preservation process: IT actions to copy and preserve ESI should be manually documented and supported by general change management controls that provide proof of authorization, proper execution of the hold, and evidence of successful preservation. Included in this requirement are system-based controls within search and migration applications.

Data Integrity

The organization should implement access controls for held data: preserved information must be secured against unauthorized access. Limited, read-only access; role-based permissions; access audit trails; and review of rights associated with user IDs and access logs should be used to ensure information is used only by authorized individuals.

The organization should preserve metadata: information must be preserved in a manner that does not compromise the integrity of the information and preserves accompanying metadata to the extent that is possible. Sampling source and destination files, use of file hashes, and other control measures to document data integrity should be in place, and all methods of preservation should be tested to ensure metadata is not lost or corrupted in the process.

The organization should document the ESI's chain of custody. For use as electronic evidence, ESI must have demonstrated authenticity; that is, the organization must be able to provide evidence that the information is what it is purported to be. The handling of ESI from its original source to its final production should be documented, noting custodians and actions taken. Additionally, access, update and change logs for any preserved ESI should be recorded, to support the information's ultimate authenticity.

Control Area 6: Auditing & Monitoring

The continuous review of e-discovery preparedness and preservation activities is necessary for this evolving area of corporate compliance. Routine audits indicate management's commitment to sound information management practices that ensure the reliable production of corporate information, should a request be made for production of ESI. Continuous review of corporate information management practices provides an incentive for compliance and improves the likelihood of an efficient, cost effective e-discovery response. Audit evidence can also be used as a defensive tool, demonstrating that the organization has taken and continues to take responsible steps to address e-discovery and follows a methodical business process to support e-discovery requests.

Audit evidence can also be used as a defensive tool, demonstrating that the organization has taken and continues to take responsible steps to address e-discovery

- **Action Item:** Establish a defined audit schedule for program compliance.
  - **Key Control Points:** The organization should create a formal audit plan and charter. It should define the scope of each audit review with the input of legal and compliance management, based on projected IT risks.
- **Action Item:** Periodically review program defensibility.
  - **Key Control Points:** The organization should undertake continuous monitoring of controlling case law, available technology, and legal standards that might impact IT's e-discovery processes (for example, standards of accessible vs. not reasonably accessible information, good-faith operation of information systems, and undue burden or costs related to production of ESI).

RISKS OF NONCOMPLIANCE

The risks of corporate noncompliance with e-discovery requests can be significant. Sanctions range from monetary fines and cost-shifting arrangements[3] to jury instructions permitting jurors to make adverse inferences as to why a party has not produced requested ESI. The effects of noncompliance can also have more direct implications for the IT professionals who are tasked with ensuring that e-discovery efforts are complete.

In the infamous Morgan Stanley case [Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc. (2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005)], for example, an IT director bore the brunt of the responsibility for the organization's failed e-discovery response.[4] The director has now filed a wrongful termination suit against Morgan Stanley, claiming he was fired in bad faith and made a scapegoat in the company's e-discovery fiasco.[5] The director was asked by the corporation's in-house attorneys to sign a certification that Morgan Stanley had produced a complete set of requested ESI. Although the IT director was not fully versed in the legal duties and ramifications represented in the document (as he was not an attorney), he signed in arguable good faith, believing that he had understood the requests and performed the tasks in accordance with the request of the corporate legal department. At some point, a miscommunication between legal and IT resulted in a failure to produce requested ESI. In the end, Morgan Stanley was subject to a $1.5 billion judgment and the director was fired.[6] The incident demonstrates the critical need for IT to be a primary player in e-discovery requests, involved from the beginning of the process.

IT directors must educate themselves on the basics of e-discovery[7] and work with legal and records management staff to proactively develop a response plan and maintain an ongoing dialogue regarding e-discovery requirements. In many cases, the legal staff is not sufficiently knowledgeable about IT systems to request correct procedures; meanwhile, IT does not know enough about the legal commitments the company is making, in terms of its ability to search and produce ESI. IT should work to bridge this gap, seeking to acquire its own knowledge and relying on subject-matter experts to help develop sound compliance programs. Most corporate legal departments are currently working on or evaluating their e-discovery efforts; therefore, IT should seek to integrate itself into these formative processes.

SUMMARY

E-discovery and the new FRCP amendments are spurring a real shift in corporate information management. However, organizations should take a measured response to e-discovery goals, attempting to reduce the risk of noncompliance without relying on a software solution or product to solve all problems. Effective corporate e-discovery response planning involves an evolution of policies, procedures, processes, and controls built around—and used in conjunction with—IT solutions. The development of a full program that includes both technology and IT-based business processes creates a defensible IT response that ultimately reduces the risk of noncompliance.

Corporate e-discovery planning does not lie exclusively in IT's domain. However, IT management must have a strong voice in e-discovery responses, in order to effect a true understanding, within in any organization, of the cross-disciplinary aspects of e-discovery. Moreover, IT management should work with legal, risk management, and compliance personnel to define the extent to which IT can deliver on and support

---

[3] Cost-shifting arrangements are court-ordered divisions of fees and costs whereby producing parties are required to pay for additional costs of producing information, not typically born by parties in their position.

[4] "Morgan Stanley's Legal Fumble Over Emails," *Wall Street Journal*, May 16, 2005

[5] Reil v. Morgan Stanley, 2007 U.S. Dist. LEXIS 11153 (S.D.N.Y. Feb. 16, 2007)

[6] The judgment was recently reversed on unrelated procedural grounds and is currently pending a re-hearing.

[7] Additional education-based reference sources include: Sedona Conference (Working Groups 1 and 6; www.thesedonaconference.org); The E-Discovery Reference Model (www.edrm.net); ARMA International (www.arma.org/legal/ediscovery/index.cfm); The Federal Judicial Center (http://www.fjc.gov/public/home.nsf → education programs → materials on e-discovery)

e-discovery requests. Basic policy and procedure development, monitoring of operational compliance, and overarching process controls are the foundation of a defensible IT response and should be a first priority for IT professionals.

AUTHOR BIO

Mary Ann Reichard, Esq., CISA, is a Senior Consultant with AdamsGrayson Consulting, a corporate risk management and e-discovery consulting firm. Prior to joining AdamsGrayson, Mary Ann began her career as an IT auditor with a large public accounting firm, reviewing corporate IT environments to ensure the accuracy, integrity and sound management of data for financial reporting purposes. She later went on to work in corporate law and compliance, and now helps organizations undertake information risk management and compliance issues, especially those that relate to law and technology such as data retention and e-discovery response planning. She holds a B.S. in Management Science and Information Technology from Virginia Tech and a J.D. from the University of Pittsburgh. She is a licensed attorney in Maryland and the District of Columbia.

Managers should have the right to require the proper, legal assurance from auditors, as well as the right to assess an auditing team's policies and procedures before they interact with corporate data.

Holding Auditors Accountable for Data Security

PETER GALLINARI

RELATED GUIDANCE

Sarbanes-Oxley

Third-Party Relationships, Risk Management Principles, OCC Bulletin 2001–47

Do Auditors Have Rights to Your Data? As the Sarbanes-Oxley Act (SOX) and other laws increase the oversight of information processes, they can actually increase the risk of unintended data exposure. Even corporations that once kept all data processing internal can be subject to internal and external auditor requests for documentation and data that supports the assurance of internal controls. And while it's true that few managers consider external auditors to represent a data risk, it is equally true that even fewer have deep insight to what happens to the proprietary corporate data they share with auditors.

A fundamental question managers should ask is whether auditors have the right to review sensitive data. This is a thorny issue. Auditors can request access to review data for either legal or regulatory reasons, but they don't own the data. But just as corporations are under the control of the regulators, when it comes to data privacy and security, data is under the control of its owner. This means it is the responsibility of the company to ensure that all controls are in place to protect data from external and internal compromises and threats.

Certainly, an auditor may request data during its review process. Since the goal of the audit process is to support managerial processes, it generally benefits the company to supply the requested data, insofar as it facilitates an effective audit. But if you are the data owner, you must know what happens to your data when it is accessed—whether by an external auditing firm, a regulator, or a client.

QUESTIONING THE DEFAULT OF DATA SURRENDER

IT management is expected to take reasonable and adequate measures to protect both business data and clients' sensitive data. Thus, businesses are reviewed on a regular basis by external auditing firms representing both client and regulators in support of compliance with Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB), HIPAA, the Payment Card Industry Data Security Standard (PCI), and potentially other rules. The goal of these reviews is to ensure that the business is meeting its obligations to maintain controls and processing standards for security and data privacy.

As a part of the audit process, businesses might submit for review all types of procedural and transactional documentation, along with charts of their networks and production workflows. At times they are even asked to let auditors run their own proprietary data extraction software to do discovery of the environment. These processes might speed up the review process. But often they also result in data being sent

back to the auditor's home location (or a third party) for review and analysis. Auditors might also transport data on CDs, USB drives, and other portable media, as well as via e-mail attachments. Are these media secure? Is the data encrypted? Where does it go? How do you know?

Most businesses permit these types of data transfer because the auditor has signed a non-disclosure agreement (NDA), confidentiality agreement, business associate agreement, or statement of work (SOW). The signatures give management some confidence that the data, which management owns and for which it is ultimately responsible, is perfectly secure.

This is not necessarily the case.
If you, as a manager, accept responsibility and accountability for your data integrity and security, why should you just give your information away? Perhaps because you think it is the right thing to do, because you assume the auditor will handle the data responsibly, or because you think you need to appear cooperative in order to obtain a clean audit report. But if you job depends on your ability to protect your data, you should apply the same control standards to auditors as you would to any third party.

You should apply the same control standards to auditors as you would to any third party.

TAKING CONTROL OF YOUR DATA

Management must ensure that the institution's data is secure. This means attaining a level of confidence in the auditor's controls over the information it handles. Particularly if the auditor is employing a third party to process your audit documentation, you must also ensure that vendor is secure.

Managers should have the right to require the proper, legal assurance from auditors, as well as the right to assess an auditing team's policies and procedures before they interact with your data.

Initially, this means the business should have a contract, SOW, and NDA signed by auditors and reviewed not only by management, but also by the corporate attorney. The contract should explicitly reserve your right to assess the auditing firm's information security controls. The review might consist of both documentary review of the auditor's programs and your inspection of their procedures, as they relate to security and privacy.

You can also request a contractual provision that absolutely prohibits data from leaving your premises. This reduces the risk of data compromise and can also eliminate the need for you to assess the auditing firm's internal security controls. If the auditor does need to transfer data outside of your control, however, management should take additional steps to ensure that the transfer of data and the auditing firm's internal environment meet your internal security standards.

The traditional goals of information protection are confidentiality, integrity, and availability (CIA). But the increasing focus on information security assurance—and managerial pressure on the IT staff to provide it—has made accountability (A) a de facto fourth goal. Ironically, many managers who diligently uphold an accountability standard for their data processing vendors fail to apply the same standards to auditors. This is a control gap. To ensure the CIA*A* of information security, management must consider how auditors interact with business information and respond appropriately.

1 Auditors perform all work on the premises and do not transport data

Not all auditors will agree to perform all work on the premises, nor is it always the best option for the business. It is, however, the easiest way to ensure the information you give to auditors is consistently protected. Even if all work is performed onsite, however, you should still institute some operational controls to ensure the security of auditors' work; specifically:

- Assign auditors a secure location where they can do their work
- Log all documents being reviewed by the auditing team
- Sign documents in and out each day for control purposes

2 Auditors transfer some data off premises—either to the audit firm's internal environment or to a third-party vendor

If your company agrees to allow auditors to transfer data offsite, management should implement more robust control steps to ensure the security of data at all points of transfer and storage; specifically:

- Assign auditors a secure location where they can do their work onsite
- Log all documents reviewed by the auditors
- Assess the audit firm's security controls
- Ask the auditor to supply security documentation, such as an ISO 27001 certification, SSL certificates, or a SAS 70 audit report[1]
- Log all information transported by auditors, including:
  - Hardcopy documents and print-outs
  - Softcopy documents and data
  - Method of transfer
  - Types of storage media used (CDs, USB drives, handheld devices, and so on)
  - Location of data and storage media
- Require the use of a secure FTP, use of a virtual private networks (VPN), employment of encryption, and other standard security procedures to protect data in transit and at rest in offsite repositories

COMMUNICATING SECURITY NEEDS TO AUDITORS

Implementing controls over audit data is not a question of trust between auditors and management, but an issue of maintaining a consistent level of control over data security, irrespective of the parties involved. Accordingly, management should insist on control assurance from auditors, but remain courteous and gracious in all communications. Auditors, like business managers, are performing a function that is greatly needed to ensure that companies are staying accountable for their actions.

[1] SAS 70s are generally not validation of a strong security program; however, they can provide a measure of assurance that the auditor is making an effort to secure its environment. The benefit of an ISO 27001 certification over a SAS 70 report is that the latter is based on controls that are defined by the company being certified; whereas an ISO 27001 certification reflects predetermined controls based on industry standards.

AUTHOR BIO:
Peter Gallinari holds CSO, CISO, CHS-III, Six Sigma and other certifications. He has worked extensively in the financial and healthcare industries.

Compliance Bibliography

Key research in compliance, risk management, and governance from 2006 to 2007

- **Security study maps global hotspots for malware** *McAfee, Inc.*
  Just like the real world, the Web has risky neighborhoods and dark alleys
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3252
  Full report: http://tinyurl.com/23hhmr

- **Most major e-commerce web sites have serious security flaws**
  Many are at risk for phishing attacks and information leakage
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3421
  Full report: http://tinyurl.com/2br2fl

- **Corporate lawyers are spending more time on regulation**
  Lawyers in the healthcare and retail industry are tackling more investigative requests from regulators
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3258
  Full report: http://tinyurl.com/yrdgps

- **US slips to seventh place in global network readiness rankings**
  Study measured business, regulatory, and infrastructure environments for IT
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3296
  Full report: http://tinyurl.com/2et3kw

- **American businesses losing $71Bn each year due to spam**
  Identifying and deleting the spam costs $712 per year per employee
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3327
  Full report: http://tinyurl.com/yuqcer

- **Data breaches can cost $305 per record, survey shows**
  Notification, legal fees, and lost productivity can amount to a hefty total
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3376
  Full report: http://tinyurl.com/2ufef2

- **Americans favor electronic healthcare records, survey finds**
  Nearly three fourths believe that the efficiency of electronic records outweighs any privacy concerns
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3488
  Full report: http://tinyurl.com/yov6c4

- **Off-network security dangers remain largely unaddressed**
  Seventy percent of data breaches result from mobile hardware
  Abstract: http://www.itcinstitute.com/display.aspx?id=4076
  Full report: http://tinyurl.com/2bs94o

- **Thumb drives are now a bigger headache than malware for IT managers**
  Majority of IT managers have no effective answer to the risk posed by portable storage devices
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3510
  Full report: http://tinyurl.com/yvzucz

- **Vast majority of corporations have suffered data breaches**
  Almost 60 percent experience the collateral damage of lawsuits and 32 percent hit by a drop in stock value
  Abstract: http://www.itcinstitute.com/display.aspx?ID=3555
  Full report: http://tinyurl.com/2heuc3

- **IT management and compliance rarely mix**
  Risk managers participated in only 23 percent of the cases involving compliance
  Abstract: http://www.itcinstitute.com/display.aspx?id=4035
  Full report: http://tinyurl.com/2fz3ua

- **Study shows that auditing fees are up 345 percent, thanks to SOX**
  Median auditing costs rose from $1.4MM in 2001 to $2.7MM in 2006
  Abstract: http://www.itcinstitute.com/display.aspx?id=4074
  Full report: http://tinyurl.com/23r7jk

- **Sarbanes-Oxley compliance drives up audit fees and legal costs in 2006**
  Expenses reported to drive companies towards privatization and mergers
  Abstract: http://www.itcinstitute.com/display.aspx?id=3965
  Full report: http://tinyurl.com/2ennzu

- **Feds claim 1,236 corporate fraud convictions over the past five years**
  One third of those prosecuted were CEOs or other senior level executives
  Abstract: http://www.itcinstitute.com/display.aspx?id=3956
  Full report: http://tinyurl.com/37hudk

Sources for COMSTAT statistics

From page 7

1. McAfee, Inc., "Mapping the Mal Web report": http://tinyurl.com/23hhmr
2. WhiteHat Security, "Web Application Security Risk Report – April 2007 Edition": http://tinyurl.com/2br2fl
3. ibid
4. Fulbright & Jaworski LLP, "Third Annual Litigation Trends Survey Findings": http://tinyurl.com/yr2mdn
5. ibid
6. ibid
7. World Economic Forum, "The Global Information Technology Report 2006-2007": http://tinyurl.com/2et3kw
8. ibid
9. Nucleus Research and KnowledgeStorm, "Spam: The Repeat Offender": http://tinyurl.com/yuqcer
10. ibid
11. Forrester Research, Inc.,"Calculating the Cost of a Security Breach": http://tinyurl.com/2ufef2
12. ibid
13. ibid
14. Kaiser Permanente, "Health Care Information Technology Summit Survey": http://tinyurl.com/yov6c4
15. ibid
16. ibid
17. Redemtech Inc., "National Survey: The Insecurity of Off-Network Security": http://tinyurl.com/2bs94o
18. Centennial Software, "Security Attitudes Survey": http://tinyurl.com/yvzucz
19. ibid
20. Scott & Scott, "The Business Impact of Data Breach": http://tinyurl.com/2heuc3
21. ibid
22. ibid
23. ibid
24. SailPoint Technologies Inc., "Audit & Compliance Professionals: Survey on Identity Compliance": http://tinyurl.com/2fz3ua
25. ibid
26. IT Policy Compliance Group, "Why Compliance Pays: Reputations and Revenues at Risk": http://tinyurl.com/ys6o9a
27. ibid
28. ibid
29. The Corporate Library, "The Audit Landscape: 2001–2007": http://tinyurl.com/23r7jk
30. ibid
31. ibid
32. ibid
33. Foley & Lardner LLP , "The Cost of Being Public in the Era of Sarbanes-Oxley": http://tinyurl.com/2ennzu
34. ibid
35. ibid
36. ibid
37. United States Department of Justice, "Fact Sheet: President's Corporate Fraud Task Force Marks Five Years of Ensuring Corporate Integrity": http://tinyurl.com/37hudk
38. ibid

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 or visit http://www.itcinstitute.com/display.aspx?id=202.