Legal and Regulatory Challenges

Featured articles:

How Safe Is Your Private Information?

Using Standards to Create Effect in the Board Room

Governance, Risk and Compliance—Tying It All Together

And more...
HOW CAPABLE ARE YOUR IT PROCESSES?

The COBIT 5® Assessment Programme helps IT leaders provide a business view of IT’s ability to create value and support enterprise goals through effective IT processes.

THE COBIT® 5 ASSESSMENT PROGRAMME INCLUDES:

- COBIT Process Assessment Model (PAM): Using COBIT 5
- COBIT Assessor Guide: Using COBIT 5
- COBIT Self-Assessment Guide: Using COBIT 5

The COBIT Assessment Programme guides are now available at [www.isaca.org/cobit-assessment-programme](http://www.isaca.org/cobit-assessment-programme).

The COBIT 5® framework is available as a free download at [www.isaca.org/cobit](http://www.isaca.org/cobit).

TO LEARN MORE
Contact research@isaca.org or visit [www.isaca.org](http://www.isaca.org).
Regis University offers a graduate certificate as well as a master's degree in Information Assurance. With both programs, you have the option to take classes online or on campus. Our School of Computer and Information Sciences is also designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

**INFORMATION ASSURANCE PROGRAMS**

**GRADUATE CERTIFICATE**
- Can be completed in less than a year
- Four classes (12 credit hours) - choose the courses that most interest you

**MASTER'S DEGREE**
- Two year program
- Specialize in cyber security or policy management

The curriculum is modeled on the guidelines and recommendations provided by:
- The Committee on National Security Systems (CNSS) 4000 training standards
- The (ISC)² Ten Domains of Knowledge
- ISACA

Classes can be taken on campus or completely online.

**Regis University** is an accredited, 130-year-old Jesuit institution in Denver, CO. Regis has been recognized as a national leader in education for adults and is committed to programs that are accessible and affordable. *U.S. News & World Report* has ranked Regis University as a Top University in the West for 18 consecutive years.
Information Security Matters: Just Okay Practice
Steven J. Ross, CISA, CISSP, MBCP

Vicki Gatewood, CGEIT, CRISC

IT Audit Basics: How to Properly Audit a Client
Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA

Information Ethics: Trust in Information Systems
Vasant Raval, DBA, CISA, ACMA

How Safe Is Your Private Information?
Joanne Joseph, CISA

The ISACA Journal seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The Journal's noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.

Want more of the practical, peer-reviewed articles you have come to expect from the Journal? Additional online-only articles will be available on the first business day of each month in which no Journal is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA members during their first year of release. Use your unique member login credentials to access them at www.isaca.org/journalonline.

The Extent of Corporate Social Responsibility
Guy Hermann Ngambeket Nde., CISA, CISM, CGEIT, ITIL V3 (F), PMP

Improving Governance Models
Rajesh Bhatia, CISA, CGEIT, PMP, MDP

The Information Systems Auditor Unmasked
Brian Vazzana, CISA, CICA, CPA, CITP

ISO/IEC 27001:2005 Implementation and Certification—Doing It Again and Again
Nurudeen Odeshina, CISA, CISM, CRISC, ITIL V3, ITSM

Corporate Responsibility, Retaining Top Management Commitment
Nikesh Dubey, CISA, CISM, CRISC

Common Myths of Service Organization Controls (SOC) Reports
Deeja Seshadri, CISA, CISM

Securing Merchant Environments Is Good, Securing the Credit Card Itself Is Better
Ali Alaswad, ITIL, PMPG, PMP

Why Should Organizations Care About Professional Certifications?
Bob Smart, CISA, CISM, CRISC, MACS Snr, MBIS

Crossword Puzzle
Myles Mellor

Help Source Q&A
Ganapathi Subramaniam, CISA, CISM

CPE Quiz #147
Based on Volume 6, 2012
Prepared by Smita Totade, Ph.D., CISA, CISM, CGEIT, CRISC

Standards, Guidelines, Tools and Techniques
S1-S8
ISACA Bookstore Supplement

Discuss topics in the ISACA Knowledge Center: www.isaca.org/knowledgecenter

Follow ISACA on Twitter: http://twitter.com/isacanews; Hashtag: #ISACAJournal

Join ISACA LinkedIn: ISACA (Official), http://linked.in/ISACAOfficial

Like ISACA on Facebook: www.facebook.com/ISACAHQ
Smarter IT starts here…
ISACA® Training Week

Enhance your skills, learn proven strategies and techniques, and continue your professional development by joining the ISACA® community at our 2013 Training Week.

To register or to learn more visit isaca.org/training2013-journal2.

ISACA’s Second Quarter 2013 Training Weeks

An Introduction to Privacy and Data Protection
22-25 April • Chicago, IL

Cloud Computing: Seeing through the Clouds—What the IT Auditor Needs to Know
6-9 May • Washington DC

Network Security Auditing
17-20 June • New York City
I read that there is a new version of ISO 27001 in the works and that it is supposed to be released in 2013. It may be issued by the time this column goes to press. I have had a lot to say about ISO 27001 and other standards in this space and probably will again, but in this case, I would like to challenge the whole idea of information security standards.

Now, before anyone rounds up the posse to hang me from the nearest tree, I would like to restate what I have said before: “[ISO 27001] forms an effective framework for security. It has established the vocabulary with which we discuss the subject. Of course, it is only a starting point; management must be committed, and knowledgeable people need to act, for there to be real security.” Standards do not establish security, people do. For information systems, the population involved is so inclusive—management, business staff, technical staff, third parties and, in some cases, even customers—that universal, voluntary adherence to any standard is neither practical nor possible. Therefore, those responsible for security information resources within organizations build systems to protect information within the boundaries of management’s tolerance for risk and their willingness to pay to mitigate it, using standards as guides.

MAXIMIZED SECURITY

Clearly, the goal of security professionals is to implement controls that maximize security within organizational limitations. I recognize that for many professionals, a standard such as ISO 27001 is a tool to demonstrate to their managers what “maximized security” actually means. The presumption in using the standard in that way is that whatever ISO 27001 requires would provide the best possible security. (Please spare me the mail saying that ISO 27001 is a framework, not a standard. I have addressed that before, as well, and can only say that if it comes from a standards organization and has “standard” written on top, it is a standard.)

But if the 2005 version of ISO 27001 is about to be updated, it follows that the 2013 release will be better—however one would like to define better—than the existing one. Therefore, assuming that an organization could adhere 100 percent to the 2005 standard, it will find itself with less than “maximized security” in the coming year. Even if there were such a thing as total compliance, all that could be attained would be security as defined in 2005. My view is that both the technology and the risk have changed a great deal since 2005, so that obsolescence should be anticipated.

STANDARDS COMMITTEES

Standards are created by human beings working in committees (with all the attendant horse-trading and compromises that come with committees). These individuals bring to bear their experience in implementing and maintaining secure systems. Those who receive the new standards must assume that the changes, which are expected to be improvements, have been put in practice by individual organizations and that cumulatively there is enough of a base of experience to demonstrate that the changes are complementary, or at least not contradictory. That means that there are some organizations, whose representatives sit on the committee, that have implemented security using techniques that go beyond the currently issued standards.

Put bluntly, best practice will always outrun standard practice. The spread between the two will increase over time as technology, risk and culture change while standards remain the same. When the discrepancy becomes so great that the standard cannot be justifiably defended, the time comes to issue a new version of the standard.

I have always had difficulties with the term “best practice.” Who is to say which practice is best, which is almost as good, which is really not
good enough? The members of the standards committee have been appointed (who appoints them, anyway?) to define best practice at a point in time, but as I stated previously the best sinks to “just okay” practice with the passage of time. A standard is obsolete the day it is published.

Is a standards committee empowered to describe what they believe are generally the best methods, tools and techniques as evidenced by what most organizations are doing? If so, the committee is describing standard practice that has been overtaken by best practice, however defined. The process of standardization drives the thought process to the middle. Carried forward over time, standard practice is mediocrity.

**BRITISH STANDARDS**

Complicating the whole process is the tendency of the International Organization for Standardization (ISO) to use standards promulgated by the British Standards Institute (BSI) as trial runs for the globally applicable ones. This was true for BS 7799, which was the predecessor to ISO 27001. (Note that ISO 27001 is still categorized as a British Standard.) This has happened more recently as BS 25999 and its companion standard BS 25777 have given way to ISO 22301 and ISO 27001. Even though the British standards were applicable only to the UK, they were treated by many around the world as de facto global standards, especially because it was widely assumed that they would be subsequently adopted by ISO. In each case, including ISO 27001, the standards were modified somewhat from the British versions, much as new releases have been.

Those who strove to adhere to the British standards found themselves, after a few years, with the task of understanding the enhancements, often subtle, in the ISO adaptations. They obtained value by having a head start on compliance with the ISO versions. But what precisely is the value of an experimental standard? And, for that matter, why is Great Britain the laboratory in which to try one out? With all due deference to British security professionals, are the security requirements for systems in the UK representative of those around the world? Is security in Bristol defined identically in Boston, Berlin, Baghdad and Bora Bora?

From the perspective of someone outside the UK, is there any rationale at all to attempt compliance with a newly issued British standard when it is likely that it will be overridden in short order by an international one? It is my opinion that organizations should strive to implement what they consider to be the best affordable practice until a global consensus has been reached on what constitutes a standard…and then stay ahead of it.

Organizations should never aspire to being standard in any endeavor. In the security field particularly, standards should be viewed as floors, not ceilings. The goal should be to implement the strongest security that an organization can afford; it is not to be just okay, like everyone else.

**ENDNOTES**


3 See, for example, Ross, Steven J., “Standard Deviation,” *Information Systems Control Journal*, vol. 6, 2005.


5 BS 7799-2:2005

6 British Standards Institute, *Business Continuity Management, Parts 1 and 2*, 2006

7 British Standards Institute, *Information and communications technology continuity management—Code of practice*, 2008


Aspirations to Reality—Filling the Cloud Computing Performance Gap

A great deal about cloud computing and what it promises to enterprises that adopt this service model for delivering technology and access to information has appeared in technology and business publications. For all of the positive claims about the benefits of cloud computing, there have been as many articles warning of the dangers. This leaves trust professionals in security, risk and assurance roles wondering where the truth lies and what concerns they should realistically have concerning cloud. The two things that do not seem to be in doubt are that enterprise management and business unit leaders are interested in cloud and that the pressure to adopt cloud solutions cannot be avoided. The challenge then is for those responsible for implementing business and technology solutions using cloud to be able to identify the gap between the promise and reality of cloud computing so they can take the steps necessary to fill the potential performance gap.

The drive to cloud computing has been focused on achieving multiple benefits including increased agility and elasticity, improved quality of service, and enhanced reliability and availability. The ability to reduce costs, achieve higher return on investment and achieve quicker time to market has been described as among the many financial benefits to be gained from adopting a cloud strategy. Finally, the ability to increase data center performance through virtualization promises to reduce the environmental footprint of energy-consuming data centers. The drive to cloud computing can be justified simply by the business, financial and environmental benefits that are promised. While opportunity in the risk/opportunity equation seems to present the necessary business case to justify the adoption of cloud, many unknowns still surround cloud computing decisions. The unknowns lie in the gap between what cloud promises and what is delivered. The unknowns include the ability of users to overcome pressure points—areas of conflict between how cloud services are designed and delivered and how the enterprise integrates these services into business activities. Pressure points develop when the organizational structure, culture, processes or policies are challenged by new ways of operating or in integrating the culture, processes or organizational structure with those of the service provider.

CLOUD MATURITY AND PERFORMANCE

The ability of cloud providers to meet user requirements and deliver expected benefits is dependent on many factors. These factors can be expressed in terms of the maturity of the service. At each stage of maturity the ability of providers to deliver innovative services, facilitate interactions with user organizations, resolve problems associated with cloud services and distinguish cloud from other third-party service offerings increases. As the maturity of cloud advances from infancy, to growth and to full maturity, both user and service provider organizations develop new and innovative business models and product offerings. Roles are developed across organizations that, instead of duplicating skills and capabilities, provide an integrated staffing capability offering more effective functioning and increased access to specialized technical skill. Things that are problems in earlier stages are resolved, removing barriers for adoption and bringing greater value and return on investment.

The 2012 Cloud Market Maturity Study indicated that cloud was just approaching the growth level of maturity. Among the different service models—Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS)—SaaS was the most advanced, just entering the growth stage of maturity. The lack of maturity of offerings of both provider solutions and user capabilities creates a need for security, assurance and risk management trust professionals to identify performance gaps and
to ensure that risk factors are identified and organization structures, policies, processes and services are adjusted to accommodate cloud offerings.

**FILLING THE CLOUD PERFORMANCE GAP**

The Cloud Market Maturity Study indicated that there is a lack of clarity in the market about what cloud computing is, how roles between suppliers and users are coordinated, how risk factors are addressed, and how service-level expectations and requirements are defined and monitored. The lack of a clear understanding about cloud computing is characteristic of a market that is still in its infancy. The level of market maturity creates a need for those who want to adopt cloud and gain value from the service offerings to understand the extent of change that is required and to ensure that proper steps are taken in preparing the organization for the service.

**Distinguishing Cloud From Outsourcing**

When the concept of cloud was gaining market attention, it was difficult for some to distinguish cloud from other outsourced arrangements. A lack of clarity about what cloud is limits the ability of organizations to appreciate the value that cloud can provide or to structure innovative programs to leverage cloud to provide new or enhanced services.

The Cloud Market Maturity Study revealed that organizations are depending on service providers to take the lead in bringing innovative solutions to the market and that, within organizations, those in technology roles have a better appreciation of what cloud is and how it can be used. Viewing cloud as a technology solution and depending on service providers to set the limits of what is available restricts organizations from gaining value or exploring novel uses of cloud services. Not having a full appreciation of how cloud differs from traditional outsourcing restricts the ability of the board to govern and the ability of executives to define and manage cloud solutions.

To change perceptions, cloud computing should be on the board’s agenda to ensure that the board understands the benefits and risk factors associated with cloud service models. Business leaders should be encouraged to take the lead in visioning possible uses of cloud, leveraging the unique elements of cloud—agility, elasticity, quicker time to market, pay for use and the ability to control costs.

IT organizations should look for ways to leverage cloud to enhance their service capabilities and reduce costs. They should also help business units to define requirements and integrate cloud services into business operations. Practitioners in the security, assurance and risk management trust roles need to remain current concerning risk factors and vulnerabilities related to cloud computing. Practitioners should then ensure that users understand the risk as they embark upon the business solution provided in the cloud. Organizations may need to form a cloud task force, representing stakeholders from across the organization to clearly define what the business need is for cloud computing, defining goals and related risk, and ensuring that all stakeholders are aware and involved in cloud strategy decisions.

**Defining Roles and Responsibilities**

Approaching cloud as if it were an outsourced services arrangement creates incorrect assumptions about roles and responsibilities between providers and users. Outsourced services are more easily defined since they are typically limited to a specific technical or business function. The Cloud Market Maturity Study revealed that there is little confidence that IT staff roles are clearly defined, that supplier and user roles and responsibilities are understood and coordinated, and that there is a clear understanding between IT and business units concerning cloud roles and responsibilities.

Since cloud is predicted to be a technology that will disrupt how business units use information and serve customers, it is imperative that roles and responsibilities among business unit management and staff, technology personnel, and cloud providers are understood and agreed upon. Leveraging the technical capabilities of providers can add needed expertise not available to user organizations. When approaching cloud, the full technical and business needs should be assessed to identify opportunities to more extensively leverage cloud
provider capabilities and to supplement user organization capabilities. Understanding roles and responsibilities and interest in leveraging specialized provider staff resources needs to be incorporated into service level agreements (SLAs) or other accords developed between provider and user. Equally important is that the exit strategy clearly specifies the details on business data eradication to avoid potential risk exposure in the future.

Developing a Risk Management Approach
As a disruptive offering, cloud brings the opportunity for user organizations to significantly increase the value they receive from information and information systems. Cloud also has the potential for adding to existing business risk or for introducing risk that is outside of the organization’s current risk profile. The Cloud Market Maturity Study revealed that organizations overwhelmingly address cloud as a technical risk. Less attention is given to cloud within the context of business unit risk or as part of an enterprise risk management program. There was little agreement among those taking part in the study that board members and executive management make business decisions based on a realistic understanding of cloud risk factors. In a market where cloud maturity is in its infancy and cloud is addressed as a technical solution, it is understandable that risk is addressed from a technical rather than business or enterprise concern. This limited view, however, may be dangerous since those taking part in the study overwhelmingly identified cloud as a business enabler.

As a service offering, cloud computing will be integrated into how business sources technology solutions and how information is used and made available. Because of the operational importance of cloud computing, cloud risk needs to be considered from the perspective of operational risk management. A risk management committee, representing business and technology users, should be responsible for identifying and evaluating risk scenarios and communicating risk concerns to those responsible for their management or mitigation.

Risk-based assessments must be performed prior to the acquisition of services to understand what additional risk the organization may be exposed to with the selected cloud services, followed by regular risk-based assessments for the duration of the services. The audit committee of the board should make a special effort to monitor cloud-related risk and ensure that risk assumptions are satisfied.

Structuring Service Levels and Monitoring Performance
The level of confidence that cloud service levels are clearly defined and providers and users can monitor against service levels is very low. Of the six service components included in the confidence barometer reported in the Cloud Market Maturity Study, performance monitoring had the lowest confidence level. It appears that experience gained from traditional outsourcing has not increased the confidence that providers and users can capture the complexity of cloud service offerings in SLAs or that either party can effectively monitor performance against service agreements. The problem may be that cloud computing is more complex than traditional outsourcing, where performance requirements can be more easily identified and quantified and compliance can be more easily monitored.

Cloud may require, in addition to the legally binding SLA, a specification of other performance requirements. These requirements can include staff and technical support that will be made available to users, documentation that can be shared, common assumptions about how the relationship between provider and user will be managed, and what avenues will be used for ongoing communication.

If cloud services are to be considered a strategic enabler, and if the success of cloud computing extends into organizational enablers such as organization structure, culture, policy and practices, the cloud provider and user need to be linked at a more strategic level than defined in a traditional SLA. To enhance monitoring, users should identify the qualities of the cloud service and relationship that are most critical and ensure that the provider understands what information is required to support user assurance needs. A communication and notification plan that provides access to information and notification when things fall outside of acceptable bounds should be developed. Specific responsibility needs to be assigned in both the provider and user organization to support information and reporting needs. Users who receive information need to understand the importance of the information they receive from suppliers and ensure that it is effectively communicated and acted upon in their organization.
Cloud computing has been described as a disruptive technology. As such, how organizations use cloud and relate to service providers is different from what has been experienced in traditional outsourcing agreements. Because of this difference, board and executive management need to be informed about risk factors that cloud may introduce; they need to be sensitive to the extent of change that may be required to gain value from cloud, considering the impact of cloud on organizational structures, their culture, policies and practices, and how internal services are impacted by cloud.

Security, assurance and risk management personnel, in their role as trust professionals, need to consider their responsibility related to cloud implementation so that the enterprise can trust in and gain value from the information and information systems related to cloud computing services.

ENDNOTES

How to Properly Audit a Client

What Is the Benchmark for IT Audit Tests and Procedures?

One of the most fundamental questions for an entry-level IT auditor is: How does one measure something to determine whether it is good, bad or ugly in an IT audit? That is, what is the standard or the benchmark when conducting IT audit tests? While some may suggest that IT auditors do not use a concrete measure, the truth is they do use authoritative standards, and do so with some consistency across the IT audit profession.

This article addresses some of the existing technical literature and audit guidance that provides concrete measures and procedures in evaluating IT in the context of an IT audit. These standards, in general, are fairly widely known and used across the profession. Therefore, like all articles in this column, this one is aimed at the “basic” or entry-level audience of the profession. The specific standards provided are illustrative of those available and not intended to be an exhaustive list.

FRAMEWORK
A framework for performing an audit or review is a critical tool for IT audit tests and procedures. The most widely used framework is COBIT®. A version of what became COBIT® was first published in 1977 by the EDP Auditors Association (EDPAA), the former name of ISACA, which was organized in 1969. Over the years, COBIT has been updated to keep up to date with the ever-changing world of IT and business. COBIT became the de facto framework for performing IT audits, for evaluating IT risk and control, and for other similar purposes.

COBIT® 4.1 and earlier provided a multilayer approach to the audit that included four domains, processes for each domain (34), and control objectives for each process (318). It is from the latter that the IT auditor gets a benchmark of what to expect and a sense of how to measure effectiveness of those activities. In addition, COBIT includes quality, fiduciary and security requirements.

Recently, ISACA released COBIT® 5. The changes include the melding of certain globally accepted standards, principles, practices, and analytical tools and models for IT audits and other uses. COBIT 5 integrates ISACA’s COBIT, Val IT and Risk IT, and related standards from the International Organization for Standardization (ISO). COBIT 5 is restructured around five basic principles and seven categories of enablers.

The IT auditor can find much assistance in performing IT audits and reviews by studying and using COBIT, which serves as a framework for the approach.

PROFESSIONAL STANDARDS
The cornerstone of professional standards is the body of IT audit and assurance standards from ISACA. The most recent body of standards, exposed in late 2012 and awaiting release at the time of this writing, is outlined in figure 1. This body of standards is more about the process of performing the audit than the technical aspects of an IT audit.

SPECIALIZED STANDARDS
There are several standards that address certain types of organizations or certain aspects of IT. These provide special assistance and applicable benchmarks for those areas. They also are fairly technical in nature and provide a great deal of assistance and education in determining the issues, risk factors, controls and best practices by which IT can be measured and evaluated.

FFIEC
The Federal Financial Institutions Examination Council (FFIEC) provides guidance and oversight in the financial institution sector of the US. It has published several relevant booklets, each referred to as an “IT Examination Handbook,” that address certain aspects of IT for financial institutions, most of which are fairly common to all organizations. These booklets provide...
guidance and standards that can be useful as benchmarks for audits related to IT.

GLBA
With the advent of the US Gramm-Leach-Bliley Act (GLBA) of 1999, certain entities must provide adequate security for certain private information. Specifically, GLBA mandates that every applicable institution has policies and processes in place to protect nonpublic personally identifiable information (PII) from threats. Section 501(b) was implemented by the FFIEC, and its Security IT Examination Handbook discusses a process-based approach to auditing operations and data under GLBA and the 501(b) expectations. The SANS Institute provides a white paper, Conducting an Electronic Information Risk Assessment for GLBA Compliance, that offers good practices on GLBA compliance.\(^4\)

HIPAA
The US Health Information Portability and Accountability Act was passed in 1996. Title II (Administrative Simplification provisions) of the Act requires the establishment of national standards for electronic patient health information and reasonable security and privacy of patient data. Mandated elements of the Security Rule include administrative, physical and technical safeguards. HIPAA became effective in 2003 with enforcement effective beginning in 2006.

The American Recovery and Reinvestment Act of 2009 requires the US Department of Health and Human Services (HHS) to provide for periodic audits to ensure covered entities are in compliance with HIPAA standards. HHS has provided an Audit Program Protocol that serves as an authoritative standard for auditing HIPAA compliance, complete with items that can serve as benchmarks.\(^5\)

PCI DSS
If an organization stores, transmits or processes customer credit or debit card data, it is subject to the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS was created to meet the growing threat of credit card theft and fraud and to protect the cardholder’s personal information. Compliance is mandatory for the specified organizations. There is also a certification program for PCI DSS auditors, known as Qualified Security Assessor (QSA). The QSA produces a Report on Compliance (ROC) for larger institutions or uses a self-assessment questionnaire (SAQ) for smaller entities. The PCI DSS documents\(^6\) and QSA materials provide the benchmarking for this specialty area.

FISMA
The US Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to develop, document and implement information security for the information and systems that support the operations and assets of the agency, including those provided or managed by outsourced entities.
FISMA further requires chief information officers (CIOs) and inspector generals (IGs) to conduct annual reviews of the information security program and report results to the US Office of Management and Budget (OMB).

NIST
The US National Institute of Standards and Technology (NIST) is responsible for developing the standards, guidelines, and methods and techniques to provide for adequate information security for the agencies. NIST has developed the Security Content Automation Protocol (SCAP) that provides the specifications.7

There are a number of articles, white papers and independent materials that provide some general guidance and standards.8 The Office of Inspector General (OIG) provides releases of actual reports that can be reviewed.9

NIST provides the FISMA-related standards, and other IT-related standards, especially related to information security. Its Computer Security Division web site provides materials and research related to security standards, including an annual report on computer security.10 NIST also provides useful information on encryption standards.11

NAIC
The National Association of Insurance Commissioners developed the annual reporting model regulation known as the Model Audit Rule, in 2006.12 Although NAIC is insurance-specific, the Model Audit Rule can be applied to a variety of industries. For instance, the Model Audit Rule addresses internal control over financial reporting (ICFR). States individually adopt this rule as the standard for auditing insurers, and under this law, the first US Sarbanes-Oxley section 404 type reports were due in 2011 for states.

VENDOR-SPONSORED REPORTS
There are at least two major reports that security professionals often refer to in developing effective IT audits. One is the “Microsoft Security Intelligence Report” (volume 13, 2012, is the current version). This voluminous study provides insights into the current and developing risk factors in the IT space, in particular related to security and developing threats. A second is Verizon’s “Data Breach Investigations Report” (the most recent version was released in 2009). It is a study of threats and risk related to security.

CONCLUSION
When IT auditors evaluate IT and its risk factors, threats, controls and effectiveness, that process should always be performed with some benchmark in mind. The body of benchmarks could come from a range of sources. This article attempts to provide the basics of where to find authoritative, reliable standards and frameworks from which an IT audit can be developed and conducted. That research should begin with COBIT and, from there, appropriate standards can be added as applicable.

ENDNOTES
2 ISACA, IS Audit and Assurance Standards, USA, www.isaca.org/Knowledge-Center/Standards/Pages/default.aspx. ISACA released the exposure draft of these updated standards in late 2012; the exposure period ended 28 December 2012 and the new standards were being finalized at the time of this writing.
3 FFIEC, www.ffiec.gov
4 SANS Institute, Conducting an Electronic Information Risk Assessment for GLBA Compliance, 2003, www.sans.org/reading_room
5 Department of Health and Human Services, Audit Program Protocol, www.hhs.gov
7 National Institute of Standards and Technology (NIST), Security Content Automation Protocol (SCAP), USA, http://scap.nist.gov
9 See an example at www.gsaig.gov.
11 See the Publications section of the Computer Security Resource Center of the NIST web site (http://csrc.nist.gov) for an example of standards NIST publishes.
12 National Association of Insurance Commissioners, Model Audit Rule, www.naic.org
Graduate into a community that’s already winning the war on cyber warfare.

ONLINE MASTER OF SCIENCE IN INFORMATION SECURITY

MANAGEMENT TRACK | TECHNICAL TRACK

Do more than just advance your career with your MSIS from Lewis University. Put it to work right away defending and protecting freedom at the corporate, national and global cyber level.

The U.S. fights off millions of cyber attacks each year. Lewis alumnus and MSIS instructor Matt Kwiatkowski is a leader in that effort. His team at Argonne National Laboratory designed a shared network early warning system, an achievement that won the 2009 U.S. D.O.E. Cyber Security Innovation and Technology Award and has countered untold cyber threats.

Matt Kwiatkowski ’06
Since its modest beginning in 1969 as the EDP Auditors Association, ISACA has come a long way. In those days, relational data structures were still emerging. The proof of concept for the Internet was in progress, but not yet ready. Ronald Rivest and his colleagues were looking for an alternative model for authentication that would work in a network environment. Telecommunications infrastructure was doing reasonably well, but it was inextricably bound to land and the analog signals. Efficiency from computers was the key focus, and mainframes were the rule of the day. Power of data and scale of communication had yet to emerge.

So much has changed! The power of telecommunications has unleashed whole new industries, mobile devices and apps, data floods, and social networks. Business has gone global in a virtual sense and new companies with innovative technology backbones are surpassing older, established giants in market capitalization within years of their origin.

With this change, ISACA has embraced trust in information systems in a timely and visionary manner. Trust is a rather complex, age-old concept with political, social and moral dimensions. In recent decades, the rainbow of implications of trust and trustworthiness has grown in size and shades. At the same time, the risk of breakdowns in appropriate levels of trust has increased in scope and materiality. It is timely that the microscope is on trust, although control and security are also going to remain issues of the day.

In his book, Liars and Outliers, Bruce Schneier states: “Society runs on trust. We all need to trust that the random people we interact with will cooperate. Not trust completely, not trust blindly, but be reasonably sure that our trust is well founded and they will be trustworthy in return.” Trust involves “giving discretion to another to affect one’s interests.” Whereas an overwhelming majority of people obey the implicit societal contract on trust, there are always defectors. Because of them, the ecosystem of trust breaks down; as a consequence, people stop trusting each other. This is the beginning of a whole new set of actions: regulating, policing, monitoring, surveying, screening, checking and so forth. Because the defectors violated trust, everyone pays to maintain an infrastructure to check on the violators.

Among all the developments affecting the role of trust in modern times, the Internet stands out both in terms of scale of impact and enormity of challenge of maintaining trust. This system of loosely connected networks includes 40,000 privately managed networks among 425,000 global routes that cut across national boundaries and cultures. Arguably, this system is functioning remarkably well. Perhaps this is due in large part to the fact that the technology in place nurtures trust; the online retailer can expect payment for what it sells and buyers can expect delivery of what they bought online. People can use mobile devices to donate to a worthy cause; the donee gets the funds and the donor gets the proof of his contribution. So far, the level of trust has seemed to grow along with the impressive growth in Internet-based organizations.

But cracks in this trustworthy system have begun to surface. At its recently held conference in Dubai, the International Telecommunications Union (ITU), a United Nations agency, approved by a majority vote a treaty giving governments new powers to close off access to the Internet in their countries, effective 2015. Authoritarian governments will be able to place control over access to the Internet. Although selective censorship of content has been practiced currently at individual, organizational and national levels, this change could result in a massive authoritarian control. Nations can censor content, monitor traffic and go after those who violate their “law.” Their citizens will not be able to access unfiltered content such as that which caused the Arab Spring, for example. Call it a digital Cold War, or just plain resistance to rights.
of information access—it will change the logically seamless, free-flowing and always accessible network of networks. A digital Iron Curtain would mean a less-resilient network and the loss of truly global web sites. Undoubtedly, the nations that are standing by the concept of a free Internet and have not signed the treaty will also lose—all because of the conviction of the supporters of the treaty that cooperation, or keeping the trust, is simply not to their advantage. And the recourse to compensating controls to offset the treaty’s impact seems almost unrealizable in this case.

The following is another example with relatively much less concern, but which, nevertheless, brings home the point: Consider a neighborhood community or a large apartment complex that permits pets on its premises. People walk their dogs and are trusted to pick up after their dog. A few residents violate this trust. Of course, the hunt for these violators, if feasible, will promptly appear on the neighborhood’s board of directors’ agenda. Technology is now available to nab the violators. How? Businesses like PooPrints offer to create a database of resident dogs’ DNA, which is then used to identify violations by looking for matches between the unattended waste and the database entries. In sum, violation of trust by some pet owners results in the deployment of a technology to free the neighborhood from those who stray from the implicit social contract. And this, in turn, restores the trust mechanism so that those who stray can expect few, if any, instances of the undesired behavior.

A key difference between the Internet access issue and policing wayward dog owners is that in the latter case, the problem is local and can be addressed locally. Although the cost of governance will also hit the pockets of otherwise cooperating dog owners, the undesired behavior can be controlled and trust of the community can be reestablished. The Internet issue is different, however, in that the scale is global, where it is hard for communities of nations to agree on and commit to their common interests.

There is another major difference between the two cases. One can say that the action of violators does not make the Internet untrustworthy. Put differently, you can still trust the system to provide trust in the Internet. It is the user community that brings on the restrictions of rights to access, not the system as such. The question is: Do we consider the user nations in this case an integral part of the system, or outside of those who build, maintain and provide the Internet? In contrast, the neighborhood community in the second case can be asked to accept monitoring as a part of the contract to belong to the community. Interestingly, the technology comes to help maintain the trust among the community residents, rather than being the lever that prompts the breakdown of trust.

So the scope and reach of individuals, communities, organizations and nations in nurturing trust and trustworthiness is a complex issue. Technology may only be one of the forces in the mix.

Distrust rules out the beneficial effects of trust. Failure to be trustworthy is not the norm, but it can happen anytime, anywhere. Take, for example, the December 2012 Newtown, Connecticut, USA, tragedy, where a young man shot to death innocent school children and staff at the school. Regardless of the reasons why this happened and whether it can be prevented in the future, deep down at the root level, the issue is whether parents can trust the ecosystem of the school where their child is spending a lot of time. How do you make society work when a major crisis like this one says to a parent, “Don’t trust the school’s ecosystem to protect your child.”?

ENDNOTES

1 I remember having to sleep by the telephone while waiting for the requested international connection. The call operator would wait until the person called showed up on the other end of the line at a local post office in India.
2 The complete vision/tagline states: Trust in, and value from, information systems.
3 Horsburgh, H.J.N.; “The Ethics of Trust,” The Philosophical Quarterly, 10(41), October 1960, p. 343-354
4 Schneier, Bruce; Liars and Outliers, Wiley, 2012
5 Ibid. This definition from Russell Hardin was quoted by Schneier.
7 Op cit, Crovitz
9 Op cit, Horsburgh, p. 350
In light of current and evolving technologies, electronic data privacy is a global issue and there is a growing public concern surrounding the infringement of personal privacy rights and information security in the way data are transmitted, stored and used across borders on the Internet and with wireless devices (e.g., mobile phones, interactive TV, global positioning systems [GPSs]). The concern is that the electronic data that are captured from these sources can be used for unintended purposes to the detriment of the individuals using the services. Based on research performed by the Ponemon Institute, it appears that mobile devices, coupled with ubiquitous access to sensitive personal data, present a significant risk to the invasion of privacy in the digital landscape.¹ This article explores the threats as well as the policy measures that are universally applied to protect users’ data from privacy infringement.

WHAT TYPES OF PERSONAL DATA ARE AT RISK?
Examples of personal data at risk include, but are not limited to, name, date of birth, home address, telephone number, ethnic group, sexual orientation, political affiliations, religion, social security number, driver’s permit number, identification numbers for various systems, customer credit information, medical information on applicants for jobs, qualifications and experience, employee performance appraisals, Internet browsing history, and emails.

Privacy Rights Clearinghouse describes incidents of personal data security breaches in organizations between 2005 and 2012 as a result of:²

- **Unintended disclosure**—Information inadvertently sent to the wrong parties
- **Insider information**—Data deliberately leaked from persons with legitimate access
- **Physical documents**—Lost, discarded or stolen printed documents
- **Portable devices**—Lost, discarded or stolen laptops, hard drives, flash drives, CDs and smartphones

WHAT IS PRIVACY?
Privacy is “freedom from unauthorized intrusion.”³ In the conduct of business, organizations must acquire personal information about individuals, companies and other institutions.

Privacy protection is to be managed on three fronts: users, consumers and employees. On the users front, it is expected that their records will be protected from unauthorized persons/entities. From the consumers’ perspective, trust and confidence must be maintained wherever business is conducted. And, from the employees’ perspective, they should be assured that their information is not disclosed without their consent.

Where sensitive data are processed, additional protection measures should be in place, in particular strong encryption of data transmission and recording of access to sensitive data. The best defense, however, is not the application of technical security controls, but information security training and awareness. Encouraging users to be security-savvy could be a primary concern for service providers and organizations. Users can be considered to be a weak link in information security as it relates to keeping information confidential. Between 2005 and the writing of this article in 2012, there were 364 instances recorded in the chronology of data breaches that resulted from insider information.⁴

DATA PRIVACY LEGISLATION: PROTECTIVE MEASURES
In recent years, new legislation has been introduced following publicly announced privacy violations in order to provide security to users, consumers and employees whose data could be manipulated and their privacy invaded in data security incidents.

The Code of Fair Information Practices established in 1972 by the US Department of Health, Education and Welfare provided the basis for subsequent legislation, such as the US Data Privacy Act (1974) and UK Data Protection Act (1998). The Code of Fair Information Practices is based on five principles:⁵

---

Joanne Joseph, CISA, is an IT auditor in Atlantic LNG Company of Trinidad & Tobago. In 2005, while at BP Trinidad & Tobago, Joseph was the IT representative on a cross-functional team that was formed to develop the local data privacy policy and promote information security awareness among the user community.

---

Do you have something to say about this article? Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:
1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent abuses of the data.

The US and UK legal frameworks supporting good privacy practices were extended to include industry-specific legislation to address the inherent risk associated with particular types of data. Examples of those practices include:

- The Gramm-Leach-Bliley Act (GLBA)\(^6\) of 1999 for US financial institutions
- The Sarbanes-Oxley Act\(^7\) of 2002 enacted in the US, also known as the Public Company Accounting Reform and Investor Protection Act and Corporate and Auditing Accountability and Responsibility Act
- The Health Insurance Portability and Accountability Act (HIPAA)\(^8\) of 2006 for US health insurance companies and medical providers
- UK Privacy and Electronic Communications Regulations (EC Directive)\(^9\) of 2003 to prohibit direct marketing via telephone, email or text messages without prior consent of the user

Regulatory demands of US and UK legislation coupled with growing concern about privacy and information security have stimulated companies and government institutions toward compliance with national laws or, alternatively, intergroup agreements in countries where there is no legislation on the matter. Legal requirements and compliance standards\(^10\) are examples of externally driven mandates\(^11\), which serve as a framework for implementations of privacy policies across international borders,\(^12\) and are designed to defend individuals' rights to privacy by prohibiting unauthorized disclosure of personal information.

An additional concern in the legal framework is the duty of organizations to notify persons whose personal data have been compromised. This requirement varies from state to state in the US and is generally enforced if the data are unencrypted (i.e., it can be read in clear text). The National Conference of State Legislatures maintains a list of enacted and proposed security breach notification laws in the US.\(^13\)

The European Network and Information Security Agency (ENISA) published a report in January 2011 on the status of the data breach notification laws in European countries. The report states that data breach notifications are not yet mandatory in most European Union (EU) countries, as the member states are still preparing to transpose the directives of the EU telecommunications regulation reform package, which was passed in November 2009.\(^14\) The reform package requires EU member states to introduce mandatory data breach notifications into local legislation.

To effectively implement the policies of the legislative framework in addressing the technology risk, industry-specific standards have emerged. These standards are updated based on the industry risk profile and published for use as a baseline in conducting digital operations. Examples of these standards include:

- Payment Card Industry Data Security Standard (PCI DSS)\(^15\)
- National Institute of Standards and Technology (NIST)\(^16\)
- ISO/IEC 27001 Information technology—Security techniques—Information security management systems—Requirements

\(^6\) The Gramm-Leach-Bliley Act (GLBA) of 1999 for US financial institutions
\(^7\) The Sarbanes-Oxley Act of 2002 enacted in the US, also known as the Public Company Accounting Reform and Investor Protection Act and Corporate and Auditing Accountability and Responsibility Act
\(^8\) The Health Insurance Portability and Accountability Act (HIPAA) of 2006 for US health insurance companies and medical providers
\(^9\) UK Privacy and Electronic Communications Regulations (EC Directive) of 2003 to prohibit direct marketing via telephone, email or text messages without prior consent of the user
\(^10\) Legal requirements and compliance standards are examples of externally driven mandates, which serve as a framework for implementations of privacy policies across international borders, and are designed to defend individuals' rights to privacy by prohibiting unauthorized disclosure of personal information.
\(^11\) An additional concern in the legal framework is the duty of organizations to notify persons whose personal data have been compromised. This requirement varies from state to state in the US and is generally enforced if the data are unencrypted (i.e., it can be read in clear text).
\(^12\) The National Conference of State Legislatures maintains a list of enacted and proposed security breach notification laws in the US.
\(^13\) The European Network and Information Security Agency (ENISA) published a report in January 2011 on the status of the data breach notification laws in European countries.
\(^14\) The report states that data breach notifications are not yet mandatory in most European Union (EU) countries, as the member states are still preparing to transpose the directives of the EU telecommunications regulation reform package, which was passed in November 2009.
\(^15\) The Payment Card Industry Data Security Standard (PCI DSS) is a widely recognized standard for credit card data security.
\(^16\) The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the U.S. Department of Commerce that develops and promotes information technology standards to enhance the nation's economic security and the reliability and security of the U.S. infrastructure. ISO/IEC 27001 is an international standard for information security management systems.
HOW DO DATA PRIVACY BREACHES OCCUR?
Unauthorized access or inadvertent disclosure of sensitive personal data occurs universally in digital communications. Examples of these points of ingress for information security exploitation are noted in figure 1.

DATA PRIVACY BREACHES
At times, stories appear in key media highlighting instances of data security breaches and identity fraud, placing enterprises, celebrities and public officials in a hall of shame or leaking information that is considered confidential or secret.

“Solitude and privacy have become more essential to the individual, but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”17

Recent examples of media reports of data security incidents occurring across a range of sectors include the following:
- Google “in breach” of UK data privacy agreement (July 2012)18
- Wyndham Hotels sued by the US Federal Trade Commission over alleged data breach (June 2012)19
- Elections Ontario’s discovery of privacy breach of voter data (July 2012)20

An ISACA white paper emphasizes the risk that perpetrators can use geolocation systems to track an individual’s whereabouts for the purposes of committing crime. This type of information is highly personal and should be classified as sensitive with the appropriate restricted access.21

<table>
<thead>
<tr>
<th>Figure 1—Examples of Information Security Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat</strong></td>
</tr>
<tr>
<td>1. Lax users</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2. Social engineering</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3. Inappropriate handling of data</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4. Communications sent to the wrong recipients</td>
</tr>
<tr>
<td>5. Weak logical access controls</td>
</tr>
<tr>
<td>6. Breach in physical security</td>
</tr>
<tr>
<td>7. Exploitation of information collected from monitoring devices</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>8. Insecure network connections</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>9. Malware</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>10. Decommissioning of systems</td>
</tr>
</tbody>
</table>
Every time persons sign up for a discount card at a store or complete a form to obtain some preferential service, the potential for personal information being proliferated in unknown places increases. Protection of personal data to some extent largely depends on each individual.

**PREPARING FOR BREACHES**
User education on key information security concepts, such as social engineering, e-privacy and cybersecurity, is critical. With respect to company monitoring, access to digital communications and electronic files should be carried out only for legitimate business reasons, such as technical maintenance; monitoring system security; complying with company policy and/or legal requirements; and investigating allegations of misconduct, fraud or other wrongdoing. Users should be aware that their electronic communications may be accessed for such purposes.

Where data are being used for marketing purposes, the individual should be given the opportunity to opt out from this arrangement at any time.

It is important that data custodians be provided with training that is specific to their role and function in order to ensure that the appropriate safeguards are maintained over the data under their responsibility. Custodians hold accountability for appropriate data classification and approval of access to sensitive data.

Performing regular information security reviews, auditing data privacy policies and procedures, and actively monitoring for new security vulnerabilities helps to ensure that the appropriate data protection standards are being maintained. Upper-level management support is a key strategy in the successful implementation of information security initiatives.

**CONCLUSION**
Given the type and extent of the damage that can result from personal data security breaches, continuous risk assessments need to be performed by privacy professionals as communication technologies evolve. Alongside this effort is the need for stricter policies and regulations to mitigate growing threats.

“The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual,” according to Earl Warren (former US Chief of Justice). Thus, the protection and security of personal private information must be a priority for privacy professionals who can influence the development of policies and laws against privacy invasion.

Privacy law is still in its infancy in many territories and every major entity should be engaged in sustainable initiatives aimed at preventing and detecting abuses of personal data. Continuous information security campaigns must be in place to educate users about the risk of having their personal data stolen as well as the controls for protecting it. A key success factor in user awareness initiatives is C-level support—demonstrating leadership by example and accountability. This mission can be extended through stakeholder partnership with nonprofit privacy organizations to disseminate public information media releases geared toward the education of users universally. To put it simply, data privacy is everyone’s responsibility.

**ENDNOTES**
4. Op cit, Privacy Rights Clearinghouse
9. “UK Privacy and Electronic Communications Regulations: E-mail, Faxes, Phone Calls, and Cookies,” http://www.the-dma.org/international/articles/UKElectronicprivacyreg.PDF
The expression “externally driven mandates” refers to changes that are driven or mandated by an external source (e.g., regulatory requirements, industry standards).


Nonprofit privacy organizations as well as enterprise representatives from human resources, security, IT, internal audit, records management, legal and other functions with aspects of their roles dedicated to data privacy

Warren, Earl; www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16502cc&wit_id=e655f9e2809e5476862f735da16502cc-0-0


Nonprofit privacy organizations as well as enterprise representatives from human resources, security, IT, internal audit, records management, legal and other functions with aspects of their roles dedicated to data privacy

Warren, Earl; www.judiciary.senate.gov/hearings/testimony.cfm?id=e655f9e2809e5476862f735da16502cc&wit_id=e655f9e2809e5476862f735da16502cc-0-0
Many companies today have some form of risk assessment, but the idea of a larger risk management program often gets laid aside for new technology or reduction of budgets. Companies spend millions on new and changing technology before they spend a fraction of that on developing, implementing and maintaining a proper risk management program. These programs help management evaluate risk and determine what controls are necessary to reduce or manage that risk. Not performing a full risk assessment before determining what security controls should be implemented is equivalent to not “looking before you leap.” Some professionals today would prefer the gadgetry of new technology to the “drudgery” of risk assessment. That mentality may end up proving foolhardy and costly because it would mean constantly changing technology to bring on the new and improved version of system safety and protection.

**TJ HOOPER CASE AND TODAY’S RISK MANAGEMENT**

The TJ Hooper¹ was a tugboat that had three barges in its charge when it started up the coastline from Maryland to New York, USA, in March of 1928. The tugboat met with a strong storm that eventually made it run to shore and all three of the barges sank with their cargo aboard. The tugboat and barge companies were sued for a large customer loss. There was testimony during the lower district court trial in New York that claimed if the tugboat captain had a working radio on board (not a requirement in those days), he would have avoided the storm and saved the cargo. The premise was that there was a technology out there that was readily available and would have greatly reduced the risk of disaster had it been utilized. The defense argued that no one in the industry used the receiver set radio technology and there was no legal requirement to do so. The decision made and published by Justice Learned Hand said that there are some precautions that are so essential to an industry that “even their universal disregard will not excuse their omission.”²

This premise can be broadened to cover information security measures of today—how they would or should meet that same level of scrutiny. Those in the information security field have generally moved through technological minefields for years, decades really, a step behind the technology that may thwart security measures. The TJ Hooper case and the opinion of Justice Hand, if applied to information security literally, says that even if companies and industry universally ignore critical information security measures, that universal disregard does not excuse omission if a data breach occurs.

While Justice Hand’s decision still holds true today, because of the difference of current technology and the speed at which it changes, morphs and is used to break the very measures it was developed to enhance, the decision’s relevance may need to be adjusted.

In 1928 technology growth moved at a much slower pace. Even in the 1970s and 1980s, the pace was much slower, with technology changing about every five years. So, in 1928 radios were simply cool gadgets that few understood, but many bought just for the thrill of the sound that emanated from them. Radios that gave weather reports twice a day along the coastlines of the US were so new that boat owners and cargo companies refused to pay for them or install them on their vessels. More often than not, the ship’s captain purchased one with his own money and brought it along for news and weather reports. The boat captain of the TJ Hooper had two radios on board; neither one was functional. Radios were not considered by the industry to be important (or reliable) enough to be considered standard ship’s gear.

Fast-forwarding to the 21st century, some technology is still seen as cool gadgetry that companies will not pay for because the technology is not needed or proven. Tokenization comes to mind, for example. It is a technology

---

¹The TJ Hooper
²Justice Learned Hand, TJ Hooper vs. Atlantic Fleet Co., 237 F 1st 457 (1928)

**Darlene Tester** is a senior compliance analyst with US Bank. She has more than 30 years of experience in the information security field in the financial services, healthcare and retail industries. She is a Minnesota, USA, attorney and has published articles for local and national law journals and technology magazines. She is also the author of Building a Sound Information Security Program.
that can reduce the payment card industry (PCI) footprint and establish a secure environment for all sensitive data. If properly installed, implemented and configured, a company can store personally identifiable information such as social security numbers, national identification numbers, credit card numbers and bank account numbers. Even if the network is hacked, all that is revealed is a tokenized number. Yet, many large organizations believe that the tokenization technology is not cost-effective and creates more headaches than it resolves security issues. They acknowledge the technology but refuse to admit its value.

These companies need only ask Heartland if US $120 million to $150 million in damages, fines and repairs was more cost-effective than better technology. If Justice Hand were still around, he might warn today’s executives: “There are precautions so imperative that even their universal disregard will not excuse their omission.”

In TJ Hooper’s time there was no legal requirement (or industry standard) for “receiving sets”; rather, only “transmitting sets” were required to send out distress signals for help under federal maritime law. Current security does not require an organization to have “receiving sets” of security, only “transmitting sets.” That is, an organization must have a means of notifying customers, shareholders and lawmakers when an incident has occurred and recovery is needed. There are federal laws that require organizations to have reasonable security in place, but the statutes do not define what “reasonable” is from a security perspective. The recent Patco case says, when it comes to wire transfer security, “reasonable” is not: (1) user IDs and passwords, (2) invisible device authentication, (3) risk profiling, (4) challenge questions, (5) monetary amount rule and (6) a subscription to the eFraud Network. For Heartland, Payment Card Industry Data Security Standard (PCI DSS) certification did not protect it from a lawsuit and costly implementation of better security systems when their systems were hacked.

When TJ Hooper is brought up in today’s security discussions, it is usually to declare that organizations should heed the warning of 80 years ago, but 80 years have brought technology that was not even dreamed of 20 years ago. Can organizations and security professionals be required to jump on every new technology to provide security to their systems when they know a new technology will come along in another month or so?

Perhaps the TJ Hooper case can be an example, not so much for technology adoption as for process adoption. Rather than chasing new technology, security professionals should be establishing a sound risk assessment process and risk management strategy. If the captain and owner of the TJ Hooper had actually done a thorough risk analysis of whether radios would be cost-effective and would reduce the risk of cargo loss during those cold March trips prior to the ship setting sail, they might have determined a working receiver set radio would help them. By the same token, if companies establish sound risk management strategy and a good risk assessment process triggered by specific events (customized for their industry and company complexity), they may determine technology that was considered cutting-edge at one time has now become required to help reduce the risk of data exposure—both from a cost and impact perspective.

Consistent use of a risk management strategy and assessment process will show outside assessors (and courts of law) that due diligence was completed and justification for any specific direction in technology implementation was documented. Will it resolve all liability and risk? No, of course not. Will it show due diligence and risk analysis? Absolutely.

CONCLUSION

“There are precautions so imperative that even their universal disregard will not excuse their omission,” said Justice Learned Hand. He was right for his time and the technology of the era. In this age of ever-changing technology, however, establishing such an edict for business is foolhardy and costly because it would mean constantly changing technology to bring on the new and improved version of system safety and protection. While the courts and plaintiff attorneys would love it, it does nothing for the security profession or professionals attempting to assist the corporate decision makers in finding the right solution for their particular data protection environment.
Several years ago the author gave a presentation at a Computer Security Institute conference in Washington DC, USA, based on the old 1932 Circuit Court of Appeals case about the TJ Hooper. Without more context, it may sound like a strange presentation for a computer technology conference, but there was a reason for the tale. The idea at the time was that information security measures are so critical to infrastructure that failure to have those measures in place equates to a violation of industry standard—even if the industry doesn’t have a common information security standard for specific measures. Over the last few years, this case and the opinion of Justice Hand have been used as a means of defining what information security professionals should know.

The TJ Hooper, 60 F.2d 737 (2d Cir. 1932), sups note 4, at 740

ENDNOTES

1 Several years ago the author gave a presentation at a Computer Security Institute conference in Washington DC, USA, based on the old 1932 Circuit Court of Appeals case about the TJ Hooper. Without more context, it may sound like a strange presentation for a computer technology conference, but there was a reason for the tale. The idea at the time was that information security measures are so critical to infrastructure that failure to have those measures in place equates to a violation of industry standard—even if the industry doesn’t have a common information security standard for specific measures. Over the last few years, this case and the opinion of Justice Hand have been used as a means of defining what information security professionals should know.

2 The TJ Hooper, 60 F.2d 737 (2d Cir. 1932), sups note 4, at 740

4 Op cit, The TJ Hooper
5 §484, title 46, U. S. Code [46 USCA _ 484]
6 Patco Constr. Co., Inc. v. People’s United Bank, 684 F.3d 197 (1st Cir. 2012)
7 Ragen, Steve; “Does the Heartland Breach Prove PCI Useless?,” The Tech Herald, 26 January 2009
Using Standards to Create Effect in the Boardroom

To be effective from an audit or supervisory perspective, it is essential to align to risk perception and priority setting in the boardroom. Ensuring board members are attentive and committed to continuous improvements is essential to improve the effectiveness of both corporate governance and the internal control environment. To this end, the Dutch Central Bank (DNB)’s IT Supervision Department (ITSD) has revised its approach, which is now increasingly based on the use of frameworks and standards.

**BEST PRACTICES AS TOOLS**

The ITSD started using best practices in 1988 with the publication of the ‘Memorandum on the reliability and continuity of electronic data processing’. This was developed by the ITSD and described the then-prevailing controls pertaining to risk analysis, security and continuity. The memorandum filled a need, as generally accepted market standards were not available yet.

This situation changed at the turn of the century, as the familiarity with and the use of standards and frameworks such as ITIL, International Organization for Standardization standards and COBIT® increased. This and DNB’s preference for principle-based supervision induced the ITSD to subscribe to these standards/frameworks. The ITSD learned from experience that it is important to translate legislation and regulations into practical measures to create effective supervision of compliance with legal and regulatory requirements. In this context, the use of assessment frameworks based on open, international standards and frameworks is an important tool. However, the ITSD does not prescribe the use of any specific standards.

From a supervision perspective, the use of standards and frameworks has advantages and drawbacks as shown in figure 1. The advantages usually outweigh the drawbacks, which the ITSD has tried to limit.

The following case example illustrates the implementation of standards in daily supervision practice.

**CASE EXAMPLE**

At the end of 2009, the ITSD started a multiyear IT security examination with the purpose of enhancing the level of information security within the financial sector in The Netherlands. The IT security examination consisted of four steps.

**Step 1: Drafting the Assessment Framework**
To ensure an effective supervisory approach, five design criteria were used while building the assessment framework:

1. The assessment framework should be based on an international standard.
2. Institutions should be able to fill in the assessment framework by themselves.
3. In addition to points for improvement, strong points should also be made clear.
4. It should be possible to prioritise results.
5. The assessment framework should provide a suitable basis for benchmarking.

Based on the above design criteria, the COBIT framework was chosen as the basis for the assessment framework. COBIT offers a great deal of advantages, one of which being that it fits within DNB’s principle-based supervision. In addition, COBIT offers a broad base of control measures and provides connections with other frameworks and standards, such as ITIL, the ISO 27000 series and COSO Enterprise Risk Management—Integrated Framework (COSO ERM). Another advantage is that COBIT is widely used among financial institutions in The Netherlands and internationally.

Based on COBIT® 4.1, 54 control measures were selected and linked with control targets clustered into six domains. These domains are further detailed in figure 2, and they have been linked to DNB’s risk methodology. The assessment framework is available on DNB’s web site.1

<table>
<thead>
<tr>
<th>Figure 3—Description of Maturity Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
</tbody>
</table>

Step 2: Process Design and Pilot
For efficiency’s sake, several process steps in the examination were standardised and templates were made. Subsequently, a tool was built to easily process and analyse the completed assessment frameworks.

A pilot test was performed to test the assessment framework and the support process in practice. To this end, the ITSD approached some institutions that had shown interest in the examination, which resulted in improved applicability. The biggest challenge was the determination of the correct scores. Insufficient knowledge of specific circumstances, misinterpretations and window dressing may lead to incorrect assessment of the maturity levels by the institutions. These causes for incorrect assessment were all the more relevant since the institutions were supposed to

In addition, a maturity model was applied, which is strongly related to COBIT 4.1 and consists of five levels. Figure 3 further details these levels, whereby the ITSD expects institutions to be able to prove that the control measures work structurally throughout the organisation. Within the maturity levels, this equals level three.

Before putting the assessment framework into practice, the ITSD talked to (amongst others) the Dutch Banking Association to create sufficient support for further steps amongst the institutions involved.
complete the assessment framework by themselves. Based on the outcome of the pilot test, two checkpoints were incorporated in the control examination process:

1. Using statistical sampling, the relevant IT supervisors discuss the conclusions of the completed assessment frameworks with the institutions concerned and, if necessary, perform additional evidence testing.
2. The board member responsible for IT signs the final version of the completed assessment framework.

The pilot test also revealed that the involvement of audit or IT audit officers often improved the quality of the results. Hence, the ITSD recommends explicitly involving the (IT) auditor during the self-assessment process. Owing to their independence, knowledge of the organisation, experience with COBIT and the subject of information security, (IT) auditors are equipped to assess the results correctly.

Step 5: Field Work and Reporting
Following this preparatory work, the examination was sent out to a number of institutions in pension funding, banking and insurance. During the fieldwork, the results were discussed with the institution by sampling, and, if necessary, additional evidence was requested. Based on the results, the ITSD drew up formal reports. Each of the institutions involved subsequently created and submitted plans for improvement in order to elevate the relevant control measures to the minimum maturity level of three. As a supplement to the individual feedback reports, benchmark reports were sent to all institutions.

Step 4: Monitoring and Communication
In the end, ‘effective supervision’ means that day-to-day operations and control are actually improved. To ensure this is happening, the ITSD actively monitors the progress of the plans for improvement by receiving and reviewing progress reports and conducting periodic interviews with the institutions concerned. If the implementation of the improvement actions does not progress according to plan, DNB may decide to resort to formal enforcement. So far, experiences are positive; the institutions are seriously working on improving their level of information security.

In addition to monitoring, internal and external communications are becoming an increasingly important activity in the information security examination. Communications can be used to reach a larger and more diverse audience and this way the examination can be brought to the attention of an increasing number of people. This gives us the opportunity to approach more institutions with the available supervisory capacity in order to realise a level playing field. The transparent exchange of information with stakeholders, such as financial institutions, supervisory authorities, umbrella organisations, IT service providers and external auditors, further aids to create the desired level playing field.

In addition to individual and benchmark reports, the ITSD uses various other forms of communication such as a seminar for institutions and external auditors. The ITSD also published an article in a newsletter for insurers and pension funds, and sent out a circular on information security.2 To achieve the desired effects, continuous attention for this subject over a period of time is very important.

In accordance with the Financial Supervision Act (Wet op het financieel toezicht or WFT), the ITSD’s goal is to achieve controlled and ethical operations at institutions. Essentially, this is about influencing behaviour. From this perspective, the use of standards alone does not create the desired effect. Benchmarking, identifying good points and points for improvement, active monitoring of improvement actions, and regular feedback of results have proven to be equally essential.

Subsequent steps
Independent of the continuous information security examinations, the use of international frameworks and standards, including maturity models, will increase in the ITSD’s daily work. In due course, the existing assessment frameworks will also be adjusted in line with the underlying frameworks and standards. The assessment framework for
information security will, for instance, be based on COBIT® 5 in the years ahead.

The on-going need for benchmark data will stimulate the use of standards, not only within the ITSD, but also at other supervisory authorities around the world. As a result, both European and non-European supervisory authorities have shown great interest in the ITSD’s new approach. To create a sectorwide effect, the ITSD will also further investigate cooperation with relevant parties such as external auditors, IT service providers and the public sector.

The ITSD is also devoting attention to the integration of various examination results and the translation of IT risk with regard to its relevance for the institution’s operational management or strategy. This is expected to improve the understanding of the effects of IT risk amongst strategists at financial institutions—in short, more effective supervision.

**CONCLUSION**

Merely drawing the conclusion that control measures do not have sufficient effect is not the essence of supervision or audit activities. The key factor is to ensure that both management and board members devote sufficient attention to improvement and commit themselves to pursuing it. Simply applying frameworks and standards is not enough. The case example revealed that the following six recommendations are important to achieve and maintain the necessary involvement at the management board level:

- **Ensuring a transparent assessment framework**—A transparent assessment framework promotes transparent communications and creates clear expectations.
- **Understanding good points and points for improvement**—Strong points as well as shortcomings must be explained.
- **Ensuring direct involvement**—Signing off on a completed assessment framework by a board member responsible for IT increases involvement and prevents a lack of engagement.
- **Benchmarking**—Benchmark information shows the organisation’s performance relative to its peers.
- **Translating IT risk factors**—IT risk factors must be linked to the institution’s risk appetite or operational strategy.
- **Monitoring improvement actions**—Active and regular monitoring ensures permanent attention for points for improvement and follow-up thereof.

**ENDNOTES**


A version of this article was previously published in Dutch in The IT Auditor, a Dutch magazine from NOREA. Reprinted with permission.

---

**Get noticed...**

Advertise in the ISACA® Journal

For more information, contact media@isaca.org.
Governance, Risk and Compliance—Tying It All Together

How does an organization that is faced with numerous federal and state compliance requirements meet the challenge? This article summarizes the efforts, the experience, and the challenges in setting up a governance, risk and compliance (GRC) program not only to satisfy the various requirements but, more important, to safeguard the organization’s confidential information resources.

MD Anderson Cancer Center is a Texas (USA) State Institution within the University of Texas System. The mission of MD Anderson is “to eliminate cancer in Texas, the nation and the world through outstanding programs that integrate patient care, research and prevention, and through education for undergraduate and graduate students, trainees, professionals, employees and the public.”

IT plays an important role in supporting the mission of MD Anderson. In addition to providing quality patient care, MD Anderson also conducts cutting-edge research programs in the form of clinical research, basic science research and translational research. IT provides the information architecture for the research community to house, process, integrate and analyze the large volume of data generated daily. The challenge of information security is to protect the confidentiality, integrity and availability of these data.

COMPLEXITIES OF INFORMATION SECURITY REGULATIONS
As a health care provider, MD Anderson is subject to the US Health Insurance Portability and Accountability Act (HIPAA) to protect Protected Health Information (PHI). As an institution within the state of Texas, MD Anderson is governed by the Texas Administrative Code 202 (TAC 202). As a member of the University of Texas System, MD Anderson is subject to the policies of the system to protect the information resources of its institutions. These policies include the University Identity Management Federation and the University of Texas Policy #UTS165 Information Resources Use and Security Policy. MD Anderson is a large research institution, and is subject to the US Food and Drug Administration’s Code of Federal Regulations (CFR). As a merchant in the payment card industry, MD Anderson is subject to the Payment Card Industry Data Security Standard (PCI DSS) to protect payment card data.

TECHNICAL COMPLEXITIES
MD Anderson has hundreds of applications, thousands of servers, platform disparities and several data centers. There is ongoing development of new applications with continual infrastructure build-out. Its Electronic Medical Record has been developed in-house. There are over 700 employees in centralized IT and about 300 employees in distributed IT.

COMPLIANCE AUDITS
MD Anderson is subject to multiple audits: federal, state, University of Texas, internal controls, Joint Commission, payment card industry (PCI), as well as other key audits.

MANAGING THE COMPLEXITIES
One method of managing these technical complexities would be to perform individual risk assessments per regulation on a periodic basis, for example, individual assessments for HIPAA, PCI DSS, TAC 202 and 21CFR Part 11. However, there are many disadvantages to this practice, some of which include resource constraints, duplication of efforts leading one to focus on a few regulations and neglect others, inefficiency, and customer frustration by asking the same questions repeatedly. MD Anderson has chosen to take another approach: a GRC general approach.

Security Regulations Compliance and Best Practices Mapping
As the first step in meeting the challenges, MD Anderson’s information security department (ISD) completed the Unified Controls Matrix.
The principal goal of this matrix is to illustrate and combine the commonalities as well as to indicate the differences among the regulations that MD Anderson has to observe. It enables one assessment to satisfy applicable regulations vs. conducting a special assessment for each regulation. It reduces the hundreds upon hundreds of regulatory control points to a smaller set. The matrix has been used to develop the following:

- High-level information security policies for end users
- An information security operations manual for system administrators
- Information security guidelines to be inserted to requests for proposals (RFPs) and requests for information (RFI) to set expectations for information security with potential vendors
- A system security checklist to support application owners and custodians in their design and development of new systems or making significant upgrade to existing systems
- Risk assessment questionnaires used for conducting security risk assessments

**MD Anderson GRC Program Execution**

Information security works closely with the institutional governance process at MD Anderson to initiate security risk assessments (figure 2). Security risk assessments are conducted based on the following:

- New projects
- Existing applications going through significant changes
- Reassessment of critical systems annually
- Reassessment of other systems every other year

**RISK MANAGEMENT PROGRAM**

The first step in setting up the risk management program was to define the methodology with the risk assessment workflow. The risk assessment program includes:

- An inventory of all applications and assets and the infrastructure on which the application is riding
- Information security guidelines, which provide information security guidance that is in compliance with applicable regulations and security best practices. These provide a high-level overview of various security topics and concepts in order to educate the reader about potential information security issues during the early stages of solution discovery. These guidelines can be used as an insert to the RFI and RFP documents to set expectations for information security with potential vendors.
- A system security checklist with the purpose to support application owners and custodians in their design and development of new systems or making significant upgrade to existing systems
- Risk assessment questionnaires used for conducting security risk assessments
development of a new or significantly upgraded application. The checklist is to be used as a tool to help assess coverage of all appropriate policy, regulatory mandates and best practices and to help identify issues and areas that are in need of remediation. Any deficiencies identified must be addressed before the application is moved into a production environment.

- A risk assessment questionnaire aligned with the Unified Controls Matrix
- Collaboration and cooperation among information security and project team stakeholders

**Risk Management Methodology**

Information security sets expectations by holding a kickoff meeting with the application owner or designee as well as the information systems (IS) administrator. During these meetings, data type and data classification are determined with input from the application owner. Through the same inquiry, infrastructure information, which supports a respective application, is collected.

The application owner or designee as well as the IS administrator complete self-assessments. Host, web and database scans, using custom scripts and manual checks, are undertaken in parallel with the risk assessment process. The criticality assessment (see the Security Risk Self-assessment section) is built into the application owner self-assessment.

The information security risk analyst validates the application owner self-assessment for accuracy. An action plan for low-risk, noncompliant controls is developed, as is an exception process based on technology or business needs for high-risk noncompliant controls with applied compensating controls for risk mitigation and risk reduction. Risk is quantified based on impact and probability (figure 3). These are exceptions to policies and regulatory issues. These issues are then processed through executive review and tracked over time.

Security is everyone’s business and is included in all information security awareness training for the user community.

**Security Risk Self-assessment**

Application owners and IS administrators are provided in-person training as well as training guides and training manuals on completing the security risk self-assessments (figure 4). The self-assessment consists of the following:

- Application profile and data content
- Regulatory requirements
- Gating based on data classification, which means that only the appropriate questions based on data classification are presented

<table>
<thead>
<tr>
<th>Figure 3—Risk Quantification Diagram</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Category</strong></td>
</tr>
<tr>
<td>Probability of occurrence</td>
</tr>
<tr>
<td>Factor 1</td>
</tr>
<tr>
<td>Factor 2</td>
</tr>
<tr>
<td>Factor 3</td>
</tr>
<tr>
<td>Impact</td>
</tr>
<tr>
<td>Factor 1</td>
</tr>
<tr>
<td>Factor 2</td>
</tr>
<tr>
<td>Factor 3</td>
</tr>
<tr>
<td>Factor 4</td>
</tr>
<tr>
<td>Risk detection controls</td>
</tr>
</tbody>
</table>

Learn more and collaborate on risk management, governance of enterprise IT (GEIT) and information security in the Knowledge Center.

[www.isaca.org/knowledgecenter](http://www.isaca.org/knowledgecenter)
• A criticality assessment with an applied scoring system to objectively rank the criticality of applications based on information provided by application owners. The key impact factors considered are patient care and patient health in the event that the applications are unavailable. The criticality assessment is used to feed information to the risk assessment to rank the applications and prioritize use of information resources during a disaster.
• A vulnerability self-scan, in which IS administrators and custodians scan the systems they manage by using the vulnerability scanning tool provided by information security. Critical and high-risk issues have to be remediated before the system goes into production.
• Overall scheduled remediation action plans, which have to be documented and accepted by the application owners

PROCESS AND TECHNOLOGY IMPROVEMENTS

In 2009, information security acquired a basic online tool to implement the process. The tool was highly customized in-house to fit the MD Anderson process. After obtaining feedback from pilot users, improvements were made before mass rollout.

After almost three years, the following benefits have been realized:
• Increased efficiency in conducting security risk assessment by decreasing the time required to perform risk assessment by 30 percent
• Implementation of gating by asking pertinent questions of the appropriate individuals
• Improvement of question set for clarity by including explanatory text and hyperlinks to information resources
• Carving out the risk assessment process into definable steps/tasks for information security or customers (application owners and IS administrators)

Figure 4—Risk Assessment Process Diagram
• Building in aging and time frame for task completion with reminder emails sent by the risk assessment tool
• Remediation action plan tracking by the risk assessment tool
• Improving the escalation process to upper management for compliance failure
• Improving the core competency of information security staff with training on all aspects of the process, including risk assessment validation and vulnerability assessment

Metrics Reporting
The risk assessment program has collected considerable data that provide management with valuable metrics that show tangible results of the program. These include:
• Compliance reports that show the degree of compliance of each application to specific regulations, internal policies and procedures
• Service delivery reports that show risk assessment cycle time metrics for each step of the process
• Operations improvement reports that include the change management readiness level for each application going through change management, server assignment for application, and the programs alignment report between disaster recovery plan management and risk assessment program management
• Wall-of-shame reports that show noncompliance with the risk assessment program. This usually brings belated actions from customers who do not want to be compared unfavorably with their peers.

MOVING FORWARD
Information security is in the process of building an information security dashboard. This provides consolidated views of every aspect of the information security program with the capability to roll information up the organization. Executives and customers can view reports on demand on integrated views of security posture within their areas of responsibilities.

The Unified Controls Matrix is an evergreen process with the following characteristics:
• Updates to regulations are entered in the matrix.
• New regulations are added to the matrix.
• Policies are updated based on the matrix.
• Risk assessment questionnaires are updated based on the matrix.
• Security guidelines and checklist are updated based on the matrix.

The future plan is to incorporate the following information into the dashboard where management information is accessible at one’s fingertips (figure 5):
• Application risk assessment
• Disaster recovery
• Self-service scanning of host, database and web application
• Enterprise security metrics of virus and spam
• Server and desktop compliance

CONCLUSION
The GRC program at MD Anderson incorporates application risk assessment, disaster recovery, self-service scanning and enterprise security metrics with near-future plans to add server and desktop compliance. A byproduct of the GRC program is the improved relationships between information security and other departments within the institution. The prior contentious relationship has been replaced by a collaborative one. There has been a definite cultural change within the organization in which security risk assessment had a negative connotation six years ago. There are many champions of this process inside as well as outside of information security.

This program is now included in the change management process and is mandatory for new projects before go-live. The information security director cochairs the change management committee with the IT program manager from the chief
information officer (CIO)’s office. Every new IT project as well as every application going through significant change has to go through security risk assessment, to include host and web scanning, before receiving approval to move into production.

ACKNOWLEDGEMENTS
The authors thank Barry Shatswell, CISSP, for his contribution to the design as well as structure of the GRC program, and the following individuals for their contributions to the structure of the GRC program: An Nguyen, CISSP, Janty Tang, CISM, CISA, CCEIT, Bin Xie, CISSP, CISA, Kim Woodruff, CISA, CISM, CISSP, Joseph Ponnoly, CISA, CISM, CISSP, Joannie Ashland, CISA, CIS/MS, CISSP, Yvette Mitchell and Paul Hensarling, CISSP.

REFERENCES
British Standards Institution (BSI), BS 7799, www.bsi-global.com/Global/bs7799.xalter
ISACA, COBIT, www.isaca.org/cobit

ENDNOTES
1 Clinical research is patient-oriented research. Research may be conducted in human volunteers or on samples from humans. Well-conducted clinical trials are the fastest and safest way to find improved treatments and preventions for diseases. Clinical trials or interventional trials determine whether experimental preventions, treatments or new ways of using known therapies are safe and effective under controlled conditions. National Institutes of Health, glossary, http://grants.nih.gov/grants/policy/hs/glossary.htm
2 Basic science research is the investigation of a subject to increase knowledge and understanding about it. In medicine, basic science research aims to better understand certain diseases. Understanding the changes in cells and molecules associated with illness provides the knowledge that helps eventually find new ways to diagnose, treat and prevent a variety of ailments. American Medical Association, JAMA, 3 April 2002
3 Translational research is applying new discoveries from basic science research to patient care. Translational Research Work Group, www.cancer.gov/researchandfunding/trwg/TRWG-definition-and-TR-continuum
4 Confidentiality refers to the need to keep information private or secret, and to prevent disclosure of information to those who do not need to see it. Confidentiality can be achieved through the use of encryption, by selective use of access controls or by keeping sensitive information apart from publicly available systems and networks. Integrity is the notion that information should be complete and unaltered as it is used and that only authorized people can make changes, which then must be recorded properly. Availability refers to the need to have information ready for use in a usable form when it is needed. Federal Register, 45CFR Parts 160, 162 and 164, Health Insurance Reform: Security Standards; Final Rule, vol. 68, no. 34, 20 February 2003
Common Myths of Service Organization Controls (SOC) Reports

In today’s dynamic environment, organizations face multiple challenges in terms of various standards and compliance requirements. They are required to provide certificates, opinions and reports to their customers for various purposes. While organizations need to provide assurance to their customers, often there is ambiguity on the certificate/opinion that will be relevant to an organization.

This article provides an overview of the Service Organization Controls (SOC) reports available. The article also aims to highlight the key mistakes or misnomers of usage of SOC reports and key pointers that organizations need to keep in mind to ensure their investments in such activities are fruitful and provide a real benefit to their customers.

SOC 1 REPORTING PROCESS

In December 2009, the International Auditing and Assurance Standards Board (IAASB) issued a new International Standard on Assurance Engagements: ISAE 3402 Assurance Reports on Controls at a Service Organization. Shortly thereafter, the American Institute of Certified Public Accountants (AICPA) revised the Statement on Auditing Standards (SAS) No. 70 guidance around the execution of third-party service organization reports, releasing Statement on Standards for Attestation Engagements (SSAE) 16 Reporting on Controls in a Service Organization.

The following fictional example explains how the ISAE 3402/SSAE 16 process works. ABC Insurance Company outsources certain claims processing functions to service provider ITBPO Ltd. In ISAE 3402/SSAE 16 terminology, ABC Insurance Company is the user organization and ITBPO Ltd. is the service organization. To ensure that the claims are processed properly and adequate internal controls are in place at the service organization, the user organization appoints an independent Certified Public Accountant (CPA) or service auditor (XYZ Auditor) to examine and report on the service organization’s controls. The service organization must respond to meet the needs of the user organization and obtain an objective evaluation of the effectiveness of controls that address operations, compliance and financial reporting at ABC Insurance Company. The CPA uses the ISAE 3402 or SSAE 16 SOC reporting options—SOC 1, SOC 2 and SOC 3—as the framework to examine controls and to help management understand the related risk factors. The service auditor, based on the IAASB/AICPA guidelines, performs the engagement and provides the report to ITBPO Ltd., which, in turn, shares the report with ABC Insurance Company.

The overall approach is depicted in figure 1.

The service organizations can provide these reports to various user organizations to provide reassurance on the functioning of internal controls. A service organization can obtain this report by appointing an independent service auditor to perform the audit and provide a SOC 1 report. A SOC 1 report provides assurance on the controls that support internal controls over financial reporting. This report can then be shared with user organizations and their auditors on request or as deemed necessary.
AICPA also provides for two other reports: SOC 2 and SOC 3. The SOC 2 and SOC 3 reports are used for reporting on controls other than the internal controls over financial reporting. One of the key differences between SOC 2 and SOC 3 reports is that a SOC 3 is a general-use report that can be provided to anyone while SOC 2 reports are for users as specified in the report.

SOC 1 MYTHS VS. FACTS
Service organizations frequently adopt the SOC 1 (ISAE 3402/SSAE 16 Type I and Type II) reports (SSAE 16 reports were formerly known as SAS 70 reports) for the wrong purposes. Some of the common errors surrounding adoption are:

1. These reports are certifications. After completion of the work, organizations publish externally (to customers and stakeholders) that they are SOC 1- or SSAE 16-certified organizations.

**Fact:** IAASB/AICPA guidelines clarify that ISAE 3402/SSAE 16 reports are not certifications. The guideline specifies that the reports are limited distribution reports and can be used by the service organization, user organization and user auditors only.

2. These reports can be generally distributed to potential customers and used as a marketing tool. Organizations distribute or plan to distribute Type I and Type II reports to potential customers, not considering the restriction in use of the report as part of the opinion.

**Fact:** The SOC reports are issued by the service organization for a specific purpose. The audiences for the reports are clearly defined. The reports are generally limited-distribution reports and have specific restrictions on use.

3. All operational areas can be included in SOC 1 reports. Organizations blindly scope in operational, marketing and regulatory areas that do not have a direct/indirect impact on financial reporting.

**Fact:** IAASB/AICPA guidelines specify that the SOC 1 report is applicable only to internal controls over financial reporting. In cases where organizations want to include other areas such as privacy or confidentiality, for example, they should adopt SOC 2/SOC 3 reports. The key difference is that SOC 1 reports are used for internal controls over financial reporting exclusively, while SOC 2/SOC 3 reports cover areas with respect to security, confidentiality, availability and privacy.

4. Once the report is obtained, no controls need to be verified by the user organization. Very often, stakeholders rely on SOC reports, see the controls defined in report on a stand-alone basis and do not consider the controls at the user-entity level while reading the report.

**Fact:** While evaluating controls at the service organization, the controls at the user organization should also be considered.

5. Application software can be made to comply with SSAE 16 requirements. When software vendors develop particular application software that is used for financial reporting, they generally would like the software to be compliant to SSAE 16 requirements.

**Fact:** Usually SOC 1 reports are assurance provided on the internal controls over financial reporting and not product evaluations.

6. Work done by an internal auditor cannot be used for the purposes of SSAE 16 engagements. The work of the internal auditor is not being used for purposes related to SSAE 16.

**Fact:** The work of the internal auditor can be used for work related to SSAE 16, and whether to do so is the judgment of the service auditor.

7. The service auditor needs to verify accuracy of the section related to “other information provided by service organization.” Service organizations provide considerable information (e.g., the business continuity plan) in this section. Organizations are under the assumption that accuracy of such information may not be verified by the service auditor.

**Enjoying this article?**

- Read the SOC 2 User Guide.
  *www.isaca.org/soc2*

- Learn more about, collaborate on and discuss service management in the Knowledge Center.
  *www.isaca.org/knowledgecenter*
Fact: The service organization has an obligation to verify accuracy of the other information provided by them; however, the service auditor will not opine on this section.

8. The service auditor does not test the effectiveness of the entity-level controls. The entity-level controls described by the service organization are used by the service auditor and no testing is performed on them.

Fact: Service auditors do opine on entity-level controls, such as the control environment, risk assessment, information and communication, and monitoring.

9. The period for testing of controls should be six months. Organizations avoid performing SOC 1 reports if controls are newly designed, thinking SOC 1 reports are not applicable.

Fact: There are specific circumstances when reports can be issued for a period of less than six months and the service auditor puts in the necessary restrictions in section 1 of the report.

CONCLUSION

AICPA’s SSAE 16 and IAASB’s ISAE 3402 standards define the purpose of SOC 1 reports as reports that provide assurance on the processes that support internal controls over financial reporting. Organizations should, therefore, take due care to understand the purpose of a SOC 1 report and also accurately define the scope of the processes to be covered. This report can be extremely useful to user organizations to understand the controls that impact financial operations and related IT controls at the service organization, especially in multiple-service-provider scenarios.
ISO/IEC 27001:2005 Implementation and Certification—Doing It Again and Again

While organizations may apply the same methodology and/or process approach specified in the ISO/IEC 27001:2005 standard, Information technology—Security techniques—Information security management systems—Requirements, in their information security management system (ISMS) implementations, the challenges and opportunities in establishing and operating the management system are never the same, even in the case of apparently similar organizations. No two organizations are ever alike.

For every organization, the crux of establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS is a scope that is dependent on the nature and characteristics of the business in which the organization is engaged, its location, assets and the technology in use within the organization. Thus, since the nature and characteristics of any two entities/businesses, their assets and technologies are not the same in their entirety, their ISO/IEC 27001:2005 implementation and certification process cannot be the same.

The journey often starts with the scope definition and a gap analysis/assessment. Often called a diagnostics assessment, the organization’s policies, procedures and practices (PPPs) are compared with the requirements of the ISO/IEC 27001:2005 standard to determine the gaps in the existent or nonexistent ISMS within the organization. The aim is not only to determine the gaps, but to close them and comply with the requirements of ISO/IEC 27001:2005. Without this phase, implementation would be an onerous project. This phase also involves policy definition (ISMS policy and other supporting policies) and carrying out a comprehensive risk assessment on the overall information assets of the organization (i.e., those within the scope of the ISMS). The results of this phase include policies, the outcome of the risk assessment (the risk treatment plan) and the assignment of controls to mitigate the risk based on the organization’s risk tolerance and risk acceptance threshold. Also, a statement of applicability (SoA) is determined, with applicable and nonapplicable controls from the 135 controls available in annex A of ISO/IEC 27001:2005. The SoA must include the justification for the nonexclusion of the nonapplicable controls as well as a reason for the selection of the applicable controls.

The diagnostics assessment provides a guide to the design phase wherein an implementation road map and/or blueprint are developed to guide the organization in its implementation efforts for the selected controls and the risk treatment plan. It is extremely important to have this high-level overview to understand what the implementation effort would cost the organization in terms of resources (i.e., budget, time, people, technology).

The implementation phase involves closing the gaps observed during the diagnostics phase in accordance with the road map developed in the design phase. This basically involves implementing, then operating and managing the ISMS. The treatment of identified risk through the implementation of policies and selected controls is carried out at this stage. Quick-wins requiring minimal implementation efforts should be addressed straight on as this may provide leverage for achieving the “big wins” and overcoming the obstacles in the implementation. Controls are implemented to meet the requirements of the control objectives specified in annex A of ISO/IEC 27001:2005. Guidance for the implementation of these controls can be taken from ISO 27002 Code of Practice for Information Security Management and/or a number of other frameworks or standards. It is also important to specify criteria for measuring the effectiveness of the controls that are being implemented. Controls can be said to be the PPPs required to mitigate identified risk.

It is imperative that the organization’s ISMS has gone through at least one Plan-Do-Check-Act (PDCA) cycle (figure 1) prior to requesting certification. The Check-Act phase helps ensure that the controls being implemented are assessed, their performance measured and, if need be,
improved. Basically, this phase, mainly a precertification phase, involves assessing the implemented controls by an internal or external (in the absence of an internal) auditor. A report from this audit is to be submitted not only to management for review but also to the implementation team to take any corrective action and preventive action (CAPA) as a result of the ineffectiveness of any of the controls that have been implemented. As with every other management system, it is important to achieve continual improvement of the organization’s ISMS. Incidents, events and security breaches should also be monitored in real time and documented to ensure that they are promptly detected and corrected and preventive actions taken to forestall a recurrence. Once these are being done consistently, certification beckons.

The certification assessment is carried out by a certification body in two phases. Stage I audit is the mandatory audit between the organization’s application for certification to a certifying body and the stage II audit. Stage I basically involves checks to ensure that the organization is ready for the assessment and the assessment is planned effectively. In most cases, it is called a documentation review audit because

<table>
<thead>
<tr>
<th>Figure 1—ISO 27001 Implementation PDCA Process Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plan (establish the ISMS)</strong></td>
</tr>
<tr>
<td>Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives.</td>
</tr>
</tbody>
</table>

| **Do (implement and operate the ISMS)**   |
| Implement and operate the ISMS policy, controls, processes and procedures. |

| **Check (monitor and review the ISMS)** |
| Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience, and report the result to management for review. |

| **Act (maintain and improve the ISMS)** |
| Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS. |

manditory documents such as scope statement, process documents, internal audits and management review reports/documents are assessed. This stage sets precedence for the stage II audit. It determines if the organization should proceed to the stage II audit. Having scaled through the stage I audit, the stage II audit is meant to provide reasonable assurance that all elements of the organization’s ISMS covered within the scope conform to the applicable control requirements of ISO/IEC 27001:2005 (mandatory clauses 4 to 8 and the control objectives of annex A). At a minimum, the audit assesses (in no specific order of importance): operation control of processes; contractual, obligatory and legal compliance; performance monitoring, measurement, reporting and reviewing; management responsibilities; and information and evidence in respect to conformity to the standard.

Hopefully, the organization passes the audit and becomes certified to the internationally recognized standard in information security management. The certificate has been signed, sealed and delivered. But, it does not end there; the surveillance audit is just around the corner. As is often said, “information security is not a destination, it is a journey,” and for the organization it means continuous improvement.

**REFERENCES**

Corporate Responsibility, Retaining Top Management Commitment

As we know, there is an increasing amount of legislation and regulation today that drives top management to ensure that adequate security controls are in place to protect their information assets and avoid, counteract or minimize security risk for an organization. Among other financial, operational and delivery commitments, top management must effectively balance its time, resources and strategic portfolios to meet today’s demanding, intrinsically woven business and security needs.

To fulfill these obligations from a security perspective, top management needs to understand the business risk, current state of existing security controls, gaps within them, and how the changing threats over time may require alignment of existing security initiatives and demand new ones. Once this understanding is clear, the necessary effort can be made to leverage today’s security technologies to better manage the overall business risk effectively. However, that alone is a daunting task.

THE ISSUE

Today, the most important and globally accepted cognizant connection between top management and the success of the information security portfolio is “top management or senior management commitment.” Almost all information security and assurance programs speak about management’s commitment as the most important driver for the success of any information security program in an organization. This is reflected in certification exam materials and management frameworks.

Organizations, however, tend to take top management’s ability to remain continuously committed to information security programs for granted, without having any means of measuring the degree of commitment. Today’s information security products and tools come with an ocean of white papers and supporting documents that highlight business and security benefits. Often these present a flowery and ideal representation to top management. However, the kind of issues that should be anticipated and practically experienced at the time of implementation or use of a tool in an organization’s specific technical landscape are never really documented in product white papers and manuals. Generally, these papers do not discuss in understandable terms the negative impact a security product or tool may have on a particular environment. This creates false expectations for management, failing which impacts management’s ability to remain committed.

Frameworks on security metrics seem to come close, but do not address the core issue. The ability to attain top management’s commitment toward information security programs should be based on the degree of quantitative understanding management has on how an information security product/tool or activity performs in the specific environment without negatively impacting the business.

The lack of such knowledge makes management susceptible to two types of trends: 1. Squeezing ad hoc tasks or subactivities or postponing them to justify information security initiatives to the internal community. Management does this to get insight about current, critical business applications. Management does this primarily to address a political in-house standoff, caused by the impact of a previously implemented security product/tool. 2. Squeezing ad hoc tasks or subactivities or postponing them due to the uncertainty of the impact a product/tool may have on current, critical business applications. Management does this to get insight about the negative impacts of using such products/tools. This often happens after purchasing and implementing security tools and products, i.e., after the fact.

In both cases, short-term information security goals and, hence, the overall information security program are negatively impacted. Thus, it is ironic that senior management often contradicts strategic security projects and decisions of which they had been an active proponent.
Both of these trends are the result of three prime underlying causes:

1. Lack of senior management understanding of the quantitative risk exposure and impact to business for any deviations from the information security initiatives. This is due to the lack of an intrinsic view available to help them make accurate and informed decisions impacting information security goals and programs. This may also be because the information security portfolio is still treated as a good-to-have program in some organizations instead of a necessity.

2. Lack of reasonable technical understanding by top management of how information security tools and products technically work. This lack of technical knowledge eventually results in decisions that delay the progress of the overall information security initiative.

3. Lack of midlevel management ability to justify and communicate the true technical nature and performance of the information security products/tools in the organization-specific, technical environment.

**CHANGE IN THOUGHT—WHAT REALLY DRIVES COMMITMENT**

With reference to top management commitment, it is time to look beyond the traditional commitment-factor statement as the biggest driver for success of information security programs. The question is: If it is the key driver, how do you measure the degree of commitment?

There is a need to provide top management with a better understanding of how different security products/tools and activities perform in the specific environment, including the negative impacts they may have on existing systems. The drivers for this are:

1. Measuring top management’s technical understanding of the nature of an information security product/tool in the specific environment. This could be represented by factors such as management’s technical understanding of how the security product works.

2. Measuring the negative impacts a security product/tool or activity has on the existing or planned technical environment. This could be represented by factors such as breaking of reports or malfunctioning of certain functionality of critical business applications.

3. Measuring the tangible business benefits the security product/tool or activity has in the existing technical environment. Tangible benefits could be represented by factors such as reduction in risk exposure and reduction in successful penetration acts.

4. Measuring the degree of architectural changes required to fully leverage the security product/tool or activity in the existing and/or planned technical environment. This degree could be represented by factors such as scope of change and cost of associated change.

**THE CONNECTION WITH SUCCESS**

These measures or degrees of knowledge directly impact the degree of real-world, top-management commitment toward information security programs and, hence, are directly proportional to the eventual success of information security programs. This is represented in [figure 1](#).

To gather such metric information, it may become necessary to have a trial-run period with the products before they are implemented. This prerequisite gives an opportunity to gather information specific to the organization’s environment.
Figure 2—Example Measurement Parameters

<table>
<thead>
<tr>
<th>No.</th>
<th>(Col. A) Seven Parameters Impacting Management Commitment and Success of Information Security Programs</th>
<th>Current Environment Score (Scale of 10)</th>
<th>Future Environment Score (Scale of 10)</th>
<th>Weightage (Scale of 10)</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Degree of <strong>technical understanding</strong> of the security product/tool/activity amongst top/senior management</td>
<td>5</td>
<td>6</td>
<td>High weightage (75%)</td>
<td>4.125</td>
</tr>
<tr>
<td>2</td>
<td>Degree of <strong>negative impact</strong> a security product/tool/activity has on technical landscape (e.g., breaking of reports or malfunctioning of certain functionality)</td>
<td>4</td>
<td>4</td>
<td>High weightage (75%)</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>Degree of <strong>business benefits</strong> the security product/tool/activity offers</td>
<td>4</td>
<td>6</td>
<td>High weightage (75%)</td>
<td>3.75</td>
</tr>
<tr>
<td>4</td>
<td>Degree of <strong>negative impact on the normal functioning</strong> of the end users of applications with the use of security product/tool/activity</td>
<td>5</td>
<td>7</td>
<td>Medium weightage (50%)</td>
<td>4.5</td>
</tr>
<tr>
<td>5</td>
<td>Degree of <strong>customization/change required in the technical landscape to implement</strong> the security product/tool/activity</td>
<td>4</td>
<td>4</td>
<td>Medium weightage (50%)</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Degree of <strong>customization/change required to leverage</strong> the expected features and benefits of the security product/tool/activity</td>
<td>7</td>
<td>5</td>
<td>Low weightage (25%)</td>
<td>4.5</td>
</tr>
<tr>
<td>7</td>
<td>Degree of <strong>transparency and communication of the technical performance</strong> of the security product/tool/activity within the organization</td>
<td>3</td>
<td>6</td>
<td>Low weightage (25%)</td>
<td>3.375</td>
</tr>
<tr>
<td></td>
<td><strong>Total Score</strong></td>
<td>32</td>
<td>38</td>
<td></td>
<td>3.75</td>
</tr>
</tbody>
</table>

**Figure 3—Ratio Scoring Table**

<table>
<thead>
<tr>
<th>Increase</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 10%</td>
<td>10</td>
</tr>
<tr>
<td>11 to 30%</td>
<td>7</td>
</tr>
<tr>
<td>31 to 70%</td>
<td>4</td>
</tr>
<tr>
<td>71 to 100%</td>
<td>1</td>
</tr>
</tbody>
</table>

**MEASUREMENT PARAMETERS**

Figure 2 lists different parameters that could provide measurement of top management commitment. For a more accurate organization-specific view, these parameters could be scored based on other key drivers specific to the organization’s environment. As an example, consider the second parameter in Figure 2: degree of negative impact a security product/tool/activity has on the technical landscape.

One of the key drivers of this parameter in an organization could be the ratio of the number of breaks in reports or existing activity (negative incidents) before and after implementing the security product/tool/activity. The referring table is represented in Figure 3.

Thus, based on where the calculated ratio falls (Figure 3), a score can be generated for the parameter (Figure 2, column A). The score for the parameter in the example is three. Similarly, other key drivers that would support and provide measurement of the parameter can be identified and scored respectively.

**CONCLUSION**

To sustain top management commitment, it becomes a corporate responsibility to provide them with a granular and accurate view of how the use of a security product/tool or activity may perform across different spectrums of business and security requirements in the organization’s specific environment. This quantitative information must filter down to numbers that eventually guide top management and everyone involved in information security to clearly understand the benefits, risk and negative impacts of employing different security products/tools and activities. Figure 2 can be used to provide top management with this view. It guides top management to get an intrinsic view...
of the various challenges that can be expected, helping top management take the necessary steps to address these challenges. This, in turn, helps top management remain committed to and achieve information security goals. This germinal understanding is the pillar that drives top management commitment to information security programs, which, in turn, drives the true success of information security programs in an organization.

ENDNOTES

Enjoying this article?

- Learn more about information security management in the Knowledge Center.
  www.isaca.org/topic-information-security-management

I AM BUILDING
for my future

UPCOMING EXAM DATE
8 JUNE 2013

FINAL REGISTRATION DEADLINE: 12 April 2013
For more information and to register for an ISACA exam, visit isaca.org/myfuture-journal2.
The advent of the Payment Card Industry Data Security Standard (PCI DSS) resulted in many organizations mandating its use. However, in many initiatives, the regulatory compliance projects face difficulties in funds allocation because it is easier to justify and calculate the projected cash benefits for projects that deliver products or services than for projects of regulatory compliance deliverables such as those related to PCI DSS.

One of the important factors that impact the cost and time in PCI DSS compliance projects is the lack of a realistic definition of scope of work. A major challenge to the project sponsors and managers is defining the gap between where the organization stands on PCI DSS requirements and the amount of work required for it to become compliant. Spending more effort on the planning phase can help to control the cost and time spent in the later phases of the project.

There is no doubt that the reliance on credit cards as a method of payment has increased, and the necessity of providing security, integrity and availability around the credit card environment is continuously pressing as the number of merchants and service providers, processes, stores, and transmissions of credit card data is projected to increase in the future. In 2011, IT research firm Gartner’s survey of 77 US retailers revealed that PCI compliance continues to be aggressively enforced by the card brands and spending with credit cards has continued to increase since 2008.¹

A survey conducted by Federal Reserve Bank of Boston in 2010 found that 72.2 percent of consumers had used a credit card in 2009.² On the other side, the number of credit card holders has increased in the US from 159 million in 2000, to 164 million in 2003 and 176 million in 2008,³ and in 2012 the estimated number of credit card holders in the US is 181 million.⁴ Visa made US $6.3 trillion worth of transactions (payments and cash transactions) over the four quarters ending 30 September 2012.⁵

The challenges of bringing a PCI environment into a new compliance system include, but are not limited to, the following:
• Sensitivity of the credit card information
• Strictness of the compliance requirements
• Zero tolerance of breach
• Different organizational structures, culture and management styles among credit card clients
• Implementation of the right technology
• Embracing changes in the established business processes, policies and procedures
• Maintaining compliance (sustainability)

THE SMART CREDIT CARD SOLUTION

The current approach to securing credit card holder information focuses on securing the credit card client’s (merchant’s) environment in compliance with industry standards to protect card information from theft and fraud.⁶ The proposed Smart Credit Card (SCC) approach looks to secure the credit card holder information from a different perspective.

SCC intends to eliminate the risk at its source: the credit card. This entails replacing the current credit card with one with more features and intelligence. This proposed credit card will resemble a small, ultrathin calculator with a smart chip that contains all the credit card holder information. It also contains a minimal processing capability to generate a random and temporary credit card number (TCCN) at each transaction. The random numbers are derived from the unique and individual credit card for each cardholder based on a strong algorithm. Each cardholder will have a unique set of temporary numbers, generated randomly on usage. To use the SCC, the user needs to enter a password on the credit card itself, preventing misuse of the credit card in the case of loss.

The SCC, which weighs no more than and is similar in size to a current card, has the following technical features (figure 1):
• A seven-segment display capable of displaying 16 or 32 digits
• A smart chip containing the cardholder’s information
• Two touch buttons: request for confirmation (RC) and correction (CORR)
• Touch buttons from numbers zero to nine
• A unique number not necessarily printed on the card

Money transactions will have two processes based on business requirements: standard (STD) and request for confirmation (RC). The STD process is for a regular money transaction through a merchant point-of-sale (POS) device. This transaction is only for one-time use and for a specific amount of money. The steps for an STD transaction are:
1. Merchant calculates the amount of purchase and requests payment from buyer.
2. Buyer presents the SCC and enters the password on the card for activation.
3. By default, the SCC is activated to the STD process unless the buyer selects the RC option.
4. The SCC automatically generates a temporary credit card number (TCCN); this number is derived from the holder’s unique credit card number using a strong algorithm.
5. Once the credit card is inserted in the merchant’s POS device, the TCCN number is tagged for the dedicated buyer, merchant and acquiring bank. This number cannot be used for another transaction in case of theft as it expires after one use. The possibility that the SCC generates a used number for a particular cardholder must be no more than three in one million transactions; this ratio is based on the Six Sigma best practice objective of quality that strives for near-perfection.
6. The amount of the sale is either manually entered or the product bar code scanned and automatically transmitted by the cash register.

7. The merchant transmits the buyer credit card data and sale amount with a request for authorization to the acquiring bank.
8. The transaction process concludes with the regular activities of verification and authorization of the credit card payment process, which is not limited to, but includes the following main steps:
   • The acquiring bank sends the authorization request to the card-issuing bank.
   • The issuing-bank sends approval to the acquiring bank and forwards it to the merchant’s POS.
   • Buyer signature is obtained on a sale slip print-out from the merchant POS.
   • The sales draft is interchanged between the acquiring bank and the card-issuing bank.
   • The amount of sale is deposited to the merchant’s bank account by the acquiring bank.

The RC process is designed to satisfy the business requirement of confirmation of money transactions. It is appropriate to use with credit card number provisions for purchases made over the phone, when filling out an electronic application or filling out a paper application. It can also be used with a merchant’s POS device. The steps for an RC transaction are:
1. The amount is either known, entered by the buyer in the online or paper application, or it is communicated over the phone by the merchant. In case of using a POS device, it is manually entered or automatically transmitted by the cash register.
2. The buyer enters the password on the SCC for activation.
3. The buyer presses the RC button. This automatically generates a temporary credit card number (TCCN) that is derived from the unique credit card number of the cardholder using a strong algorithm. The number is tagged with the request for confirmation, which will put the transaction on hold for 72 hours for the buyer’s confirmation. The 72 hours start from the date and time of purchase.
4. If the buyer requires multiple transactions, the buyer should enter the required number of transactions immediately after pressing the RC button. For example, if the buyer presses RC followed by the number 12, this means the buyer authorizes the merchant to draw money 12 times using the same TCCN. Confirmation from the buyer is necessary for each request whenever it is due.

5. Based on the purchase method, the buyer communicates the TCCN that shows up on the SCC display screen to the merchant either verbally over the phone, by writing it down in the online or paper application, or by sliding the SCC into the merchant’s POS device. The money transaction will not be completed until the buyer confirms the purchase or the 72-hour period has elapsed.

6. To complete a transaction, the confirmation request is sent to the buyer as:
   - A text message sent to the buyer’s registered mobile phone. The buyer needs to reply to the message with “yes” to confirm or “no” to decline.
   - A message sent to the buyer’s online bank account. The request will be listed in a queue waiting for the buyer’s confirmation for each request.
   - A phone call to the buyer’s bank using the bank’s interactive voice response (IVR) system to confirm the transaction

The buyer can also go to the bank and personally ask the teller to confirm the pending requests. The buyer must provide confirmation within 72 hours from the purchase date and time; otherwise, the transaction will automatically proceed and the buyer will have all responsibility in the case of false representation.

The buyer’s confirmation for each purchase is important for two reasons:
1. Helps to prevent illegitimate transactions
2. Declines unauthorized purchase of any commodity or service

The SCC solution benefits include:
- Significantly reduces fraud-related activities due to the utilization of the TCCN concept and the RC feature
- Is easy and quick to use
- Allows merchants to focus on implementing their overall security strategy for the whole environment without the need to address the security of the cardholder data environment, as the latter is being handled by the SCC
- Helps businesses avoid penalties and the risk of not being PCI-compliant
- Saves merchants and service providers from the cost of PCI compliance projects and the cost of PCI sustainability—thus allowing them to focus on their core business
- Enhances business reputation and increases client trust, leading to the increased use of credit cards as the mode of payment

THE SCC SOLUTION AND THE PCI CONTROL OBJECTIVES

The SCC solution has two payment processes. In the STD process, the TCCN is valid for one usage only, and if the TCCN is stored, processed or transmitted, it will require no implementation of PCI compliance security measures.

In the RC process, the TCCN can be used multiple times, and gets stored at the merchant environment, but in the SCC solution, the liability shifts from the merchant to the cardholder by providing the cardholder the ability to confirm each transaction. For a transaction to complete, the cardholder must provide approval within 72 hours of the transaction initiation. The cardholder is legally responsible for any breach. Merchants, service providers and credit card issuers must make sure cardholders are aware of this responsibility.

In the SCC solution, the real work of PCI DSS compliance requirements implementation is mainly focused at the card-issuing bank where the primary account number (PAN) of the cardholder is stored, processed and transmitted. Furthermore, the environment where the encryption keys are stored and the keys used to decrypt the TCCN to identify the actual account number, cardholder name and other required information to complete the transaction must be secured in accordance with PCI DSS requirements.

ALTERNATIVE APPROACH: CREDIT CARD WITH WIRELESS INTERFACE

The proposed SCC solution provides the technical capabilities to enable the credit card to generate the TCCN by itself. An alternative solution would be adding a wireless feature to the credit card. In this approach, the same steps of the SCC process are followed with the single exception of generating the TCCN remotely and, in case of the RC process of payment, having the confirmation request received on the card itself.

The alternative wireless approach works with the credit card sending a remote request for a TCCN to the card-issuing
bank through a wireless connection; the card-issuing bank processes the request, identifies the card holder account, generates a temporary and unique TCCN based on a strong algorithm, and sends a TCCN to the credit card. If the transaction requires confirmation from the cardholder, a request for confirmation is received on the card itself, and the cardholder is given the capability to approve or decline through the credit card. Serious considerations would need to be taken into account when adopting this approach, specifically:

- Wireless coverage
- Security
- Responsiveness

CONCLUSION
The SCC solution is proposed to provide a different security framework that provides peace of mind to all parties—the merchants, the credit card issuers and the customers (credit card holders). The current PCI compliance implementations focus on securing all merchants’ environments by adding controls to business processes, modifying applications, removing data with credit card information and changing network configurations as needed. The proposed solution adds control at the credit card level. The solution features and components can be summarized as follows:

- The credit card is changed to include features with more intelligence and processing capabilities.
- The credit card is protected by password, which can be used by the legitimate holder only.
- The credit card numbers are dynamic; different transactions use different credit card numbers.
- The generated TCCN is created randomly by a strong algorithm that uses the unique number given to the cardholder account by the card issuer.
- In the case of the one-time payment option (STD procedure), once the TCCN is used, it is no longer valid for additional payments.
- The cardholder always has the option to request confirmation (RC procedure) if there are multiple payments on the same TCCN or if it is required by the cardholder for one reason or another. The cardholder can set the number of payments in advance on the credit card itself.
- Cardholders have the option to control their own transactions by approving or declining money transactions through different methods.
- The cardholder confirms the money transactions through one of the following methods: text message, online bank account, using a bank IVR system or in person at the bank.

REFERENCES

ENDNOTES
1 Gartner Survey, “PCI Compliance Activity Shifts Downstream as Aggressive Enforcement Continues,” June 2011
3 US Census Bureau, 2010
Bob Smart, CISA, CISM, CRISC, MACS Snr, MBIS, is the IT security advisor within the South Australian Department of the Premier and Cabinet. He previously managed IT audit and advisory teams within PwC. Smart shares his experience in cybersecurity management, IT audit and risk management through facilitation of Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) study sessions and as a guest lecturer at the University of South Australia (Adelaide, South Australia).

Why Should Organizations Care About Professional Certifications?

Conventional wisdom says that professional certifications provide individuals with improved career and income prospects, greater networking opportunities, professional respect, and increased self-confidence through independent validation of competencies. But what is in it for organizations hiring certified professionals?

Engaging certified professionals can be considered a risk management tool. Professional certifications can be defined as a promise made by the certifying body that the recipient has demonstrated a minimum level of capabilities. Therefore, hiring professionals with reputable credentials reduces the likelihood of poor judgments or missed opportunities. This can also boost a company’s image and success rate in winning contracts and new customers.

Consequently, organizations are willing to pay 27 percent more for a certified professional than an uncertified comparable specialist. This pay premium differs among credentials, reflecting business benefits delivered. This value comes from increased credibility, standardization with industry frameworks, and having skilled and motivated people.

CREDIBILITY

A professional designation is an independent confirmation of credibility. This is invaluable for job roles without other opportunities to effectively demonstrate capabilities to management, boards, business partners, regulators, customers and third parties. Certification provides assurance that the individual possesses the required competencies and, therefore, a source of credibility. Examples are roles where high-impact discretionary decisions are made—such governance, risk management and assurance functions or any positions that are likely to be required to demonstrate credibility to a judge or jury, such as a security investigator, digital forensic professional or incident response specialist.

Because credibility is inherited from the professional credential, it is directly related to the credibility of the certifying body and the certification process. For this purpose, even certifications can be certified against the ANSI/ISO/IEC 17024 standard for personnel certification programs. Knowing that a certification has been independently assessed for conformity against requirements of ANSI/ISO/IEC 17024 gives it a certain level of credibility. According to ANSI/ISO/IEC 17024, a credential should clearly state competencies being examined. The examination must be independent and include a suitable test of demonstrated ability to apply knowledge, skills and appropriate personal attributes, which constitute required competencies. The certifying body should ensure a consistent examination approach over time and for all regions where the certification is offered. Some credentials are also accompanied by a code of ethics that shapes personal attributes and supports credibility and ethical conduct of the certified individuals. Finally, reputation, history and governance of the issuing body are inseparable from the certifications themselves.

STANDARDIZATION

Alignment of certified competencies with skills and industry frameworks simplifies skills management and helps organizations better utilize industry frameworks intended for “matching the skills of the IT workforce to the needs of the business.” For instance, if position descriptions are aligned to the Skills Framework for the Information Age (SFIA), professional designations, such as the Certified Information Systems Auditor® (CISA®) and the Certified Information Security Manager® (CISM®), that are aligned to the same framework would be easier to incorporate in hiring, learning and development plans. Additionally, if a certification is mapped to SFIA, it makes it apparent if it is intended for coordinator, management or executive levels, which may not be clearly disclosed in certification materials.

Furthermore, if an organization has embraced an industry framework, such as
COBIT®, Sherwood Applied Business Security Architecture (SABSA) or IT Infrastructure Library (ITIL), focusing on the corresponding certification issued by the framework-originating body would deliver greater business benefits.

Finally, although national certification schemas may address local requirements, global certifications improve collaboration and communication among specialists from business partners in a globalized business environment.

SKILLED AND MOTIVATED PEOPLE
The final and, arguably, most important benefit for employers is related to having skilled and motivated people in the organization. This is a key organizational objective as identified in COBIT® 5,9 and certifications both identify and prove the existence of skills and motivation in a positive loopback system.10

The dynamic nature of the current IT environment demands that certifications have a shelf life and must be kept up to date through monitored continuous learning and development. While centrally managed organizations in less-dynamic business sectors may have professional development programs that are inadequate for IT specialists, continuing professional education requirements of leading professional organizations prevent obsolescence of skills. Furthermore, most issuing bodies provide cost-effective education services to members. Certifications without expiry and supporting professional development programs may be preferred by some individuals, but they will certainly be less valued by employers.

Continuous education provisions of leading certifications provide organizations with assurance that the credential holders have kept their skills current and covered the required breadth of knowledge.

Professional certifications also assist with developing staff for emerging skills gaps. Certifying bodies are usually faster than traditional educational institutions to respond to changing market demands as they often have strong industry and research alliances that contribute to keeping their body of knowledge current.11 For example, as a consequence of the increased focus on risk management within the information security management profession, the domain of risk in ISACA’s CISM job practice and, therefore, in the exam recently increased from 22 to 33 percent.12 Furthermore, the new converging and rapidly digitized world has created a demand for cross-disciplinary skills in areas such as digital forensic science, IT audit, health care information management, information security management and IT governance. Professional certifications commonly deliver required outcomes faster in addressing these skill gaps.13

Even for supposedly single-disciplinary fields, such as IT security management, very few universities offer the required breadth of knowledge to equip students with the skills necessary to develop and implement an information security management program—not to mention that academic credentials do not cover practical situational experience and competence, which are crucial for any decision-making role. Fortunately, professional certifications have sufficient geographical reach and agility to help individuals develop the necessary IT capabilities to serve changing business needs.

CHOOSING THE MOST VALUABLE CERTIFICATIONS
Many organizations have taken a focused effort to best utilize the value of professional certifications. This is particularly evident within government and regulatory bodies. In India, Indian CERT-IN, the Reserve Bank of India, Securities and Exchange Board of India (SEBI) and the Controller of Certifying Authorities have prescribed mandatory certification for specific assurance roles.14 In the US, the Department of Defense,15 the Drug Enforcement Administration (DEA) and the Federal Reserve Bank also specify certifications for IT audit and cybersecurity management roles. Similar requirements are placed on the staff of Colombian Superintendencia General de Entidades Financieras and the Banking Regulation and Supervision Agency of Turkey and government IT auditors in Mauritius and Poland.16

The governments of Japan and South Australia have gone one step further by specifying professional designations as part of IT procurement requirements. The South Australian Government’s Office of the Chief Information Officer (OCIO) reviews IT audit and advisory reports from professional
services firms. While the lack of a certification does not equate to a lack of capabilities, it is far less likely that the work of a certified professional would contain serious error of judgment or incorrect advice. As a result of these and other assessments, South Australia’s OCIO has identified valuable certifications and recommended common credentials for cybersecurity services (figure 1).17

While creating such comprehensive certification criteria may not be feasible for smaller organizations, they can leverage the work of other organizations, such as local and foreign governments and specialized media that publish annual lists of top professional certifications18 or certifications commanding the highest salaries.19

Monitoring relevant job listings could also be an indication of preferred credentials20 for certain roles, including how much the market values them.

<table>
<thead>
<tr>
<th>Services</th>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation services</td>
<td>• Encase Certified Examiner (EnCE)</td>
</tr>
<tr>
<td></td>
<td>• AccessData Certified Examiner (ACE)</td>
</tr>
<tr>
<td></td>
<td>• Certified Computer Examiner (CCE)</td>
</tr>
<tr>
<td></td>
<td>• GIAC Certified Forensic Analyst (GCFA)</td>
</tr>
<tr>
<td></td>
<td>• Certified Computer Forensic Examiner (CFCE)</td>
</tr>
<tr>
<td></td>
<td>• ASIS Professional Certified Investigator</td>
</tr>
<tr>
<td></td>
<td>• Licensed Security/Investigation Agency under Act 1995</td>
</tr>
<tr>
<td></td>
<td>• SANS Global Information Assurance Certification (GIAC)</td>
</tr>
<tr>
<td>Security assessment</td>
<td>• Certified Information Security Manager (CISM)</td>
</tr>
<tr>
<td></td>
<td>• Certified in Risk and Information System Control (CRISC)</td>
</tr>
<tr>
<td></td>
<td>• Certified Information Systems Auditor (CISA)</td>
</tr>
<tr>
<td></td>
<td>• Payment Card Industry Qualified Security Assessor (PCI QSA)</td>
</tr>
<tr>
<td></td>
<td>• Infosec Registered Assessor Program (I-RAP)</td>
</tr>
<tr>
<td></td>
<td>• ISO 27000 Lead Auditor</td>
</tr>
<tr>
<td>Cybersecurity auditing</td>
<td>• Certified Information Systems Auditor (CISA)</td>
</tr>
<tr>
<td></td>
<td>• Infosec Registered Assessor Program (I-RAP)</td>
</tr>
<tr>
<td></td>
<td>• Payment Card Industry Qualified Security Assessor (PCI QSA)</td>
</tr>
<tr>
<td></td>
<td>• Certified Business Continuity Auditor (BCBA)</td>
</tr>
<tr>
<td></td>
<td>• Certified Functional Continuity Professional (CFCP)</td>
</tr>
<tr>
<td></td>
<td>• SANS Global Information Assurance Certification (GIAC)</td>
</tr>
<tr>
<td>Consulting: security policy/strategy</td>
<td>• Certified in Risk and Information Systems Control (CRISC)</td>
</tr>
<tr>
<td></td>
<td>• Certified Information Security Manager (CISM)</td>
</tr>
<tr>
<td></td>
<td>• Certified in the Governance of Enterprise IT (CGEIT)</td>
</tr>
<tr>
<td></td>
<td>• SANS Global Information Assurance Certification (GIAC)</td>
</tr>
<tr>
<td>Security architecture and design</td>
<td>• Certified Secure Software Lifecycle Professional (CSSLP)</td>
</tr>
<tr>
<td></td>
<td>• Certified Business Continuity Professional (CBCP)</td>
</tr>
<tr>
<td></td>
<td>• Certified Business Continuity Auditor (BCBA)</td>
</tr>
<tr>
<td></td>
<td>• Certified Functional Continuity Professional (CFCP)</td>
</tr>
<tr>
<td></td>
<td>• Master Business Continuity Planner (MBCP)</td>
</tr>
<tr>
<td></td>
<td>• Certified Enterprise Architect (CEA)</td>
</tr>
<tr>
<td></td>
<td>• Certified Information Systems Security Professional (CISSP)</td>
</tr>
<tr>
<td>Security systems development and analysis</td>
<td>• Certified Information Systems Security Professional (CISSP)</td>
</tr>
<tr>
<td></td>
<td>• GIAC Secure Software Programmer (GSSP)</td>
</tr>
<tr>
<td>Government security implementation services</td>
<td>• Certified in Risk and Information Systems Control (CRISC)</td>
</tr>
<tr>
<td></td>
<td>• Certified Information Security Manager (CISM)</td>
</tr>
<tr>
<td></td>
<td>• Holistic Information Security Practitioner (HISP)</td>
</tr>
<tr>
<td></td>
<td>• South Australia Police Supplier Relationship Management (SAPOL SRM)</td>
</tr>
<tr>
<td></td>
<td>• South Australia Police Advanced Supplier Relationship Management (SAPOL Advanced SRM)</td>
</tr>
</tbody>
</table>
Another reason is that IT has very few regulations and attribute the impact of certified professionals to business outcomes. Another surprising that some organizations still do not actively support waiting on a regulation, embracing professional certifications is a simple solution in the hands of organizations that will also pay back through an improved bottom line.

ENDNOTES
8. Ibid.
1 “They should be viewed as floors, not ceilings.” Steven J. Ross
6 Cloud implementation should be used as an opportunity to reduce and control ____
9 Difficulty
10 Cloud implementation promises benefits in ___, abbr.
11 Mea ___
12 ____ server
14 High-speed subnetwork of shared storage devices, for short
15 Insurance organization that developed the Model Audit Rule, abbr.
16 Upper limit
17 Computerized teller
18 Doctor, for short
22 Indicates the manufacturer
23 Violation of security or privacy for example
25 Act requiring entities to provide adequate security for private information, for short
27 Atomic number 51
28 Decline
29 Payment Card Industry Data Security Standard: ____ DSS
31 Company that produces a Security Intelligence Report that contains data on developing risk factors in the IT space
33 Exec responsible for a company’s IT security and privacy compliance
34 Vital concept in the world of risk and security
37 Close
38 Bruce Schneier’s book: “____s and Outliers”
40 Fix definitely
41 Organization that provides guidance and oversight in the financial institution sector of the US, for short
44 Organization that provided an Audit Program Protocol as a standard for auditing HIPAA compliance, abbr.
45 Type of committee (2 words)
46 Freedom from unauthorized intrusion
47 Appeal for help
48 Business management software company

DOWN
1 Powerful
2 One of the benefits driving cloud implementation
3 Place for a cell phone
4 Public announcement
5 Cloud offering that is reaching the growth level of maturity
6 Most widely used framework for IT audit tests
7 User agreements with cloud service providers
8 Budget amount
13 Block up
19 Purpose
20 Desktop
21 Rules set to solve software problems
22 British media company
24 Interface between softwares
25 Roadside sign
26 Fitting
27 Difficult position
28 Act to tighten regulations regarding financial reporting, abbr.
30 UN agency that recently voted to allow countries to close off access to the Internet in their countries, as of 2015 (abbr.)
31 12 times a year
32 Categories
35 Game arbiter
36 Visit
38 Took the initiative
39 Review
40 Institute that provides white paper “Conducting an Electronic Information Risk Assessment for GLBA Compliance”
41 Way of transferring data or software, for short
42 Third in the family
43 Finance representative

(Answers on page 54)
Q

How do you audit the effectiveness of a command centre of a crisis management plan in the context of business continuity planning? You may also elucidate steps to audit a crisis management plan.

A

A crisis management plan (CMP) is a component of the overall business continuity management (BCM) plan. A command and control centre (CCC), on the other hand, is a subcomponent of the overall CMP. An effective CMP is something that is well tested and documented.

The steps to audit a CMP, which comprise the setting up of a CCC, are as follows:

- The plan must clearly define what constitutes a crisis because a simple event or an incident may not warrant the assembling of the crisis management team (CMT) and executing the plan. It is pertinent to note that such incidents and events may also require resolution.
- The plan must contain steps that would lead to the assembling of the CMT in the CCC.
- A proper venue must be pre-identified and designated as the crisis management room to handle the crisis.
- The crisis management room or the CCC must be equipped with all kinds of communication devices and equipment.
- The communication links must be redundant links other than the primary links. Imagine a scenario where the crisis is the failure of the primary connectivity links—redundant links are a must.
- The roles for individuals comprising the CMT must be clearly identified. In particular, it is essential to identify the leader of the team. There cannot be a debate at the time of crisis as to who is going to lead the effort and take calls or make decisions.
- The CMT will not be able to deliver on its own. It will have dependencies on various other teams. Such connections must be clearly identified and documented. For example, the disaster recovery team (as it is called in the BCM world) is responsible for the recovery of the IT systems and applications. If the IT systems are outsourced and run by one or more third-party vendors, the definition of roles and responsibilities becomes much more important.
  - The CMT must interact with the communications team responsible for both internal and external communication. Policies must be in place forbidding employees from talking to external agencies. Employees giving interviews to the press during the crisis may not be helpful to the organisation.
  - There must be a notification system in place that can be deployed to assemble the CMT. In BCM parlance, this is called the ‘call tree’. It is essential that the call tree structure is well tested. If the telephone numbers prove to be invalid during actual crisis management, it may aggravate the crisis situation.
  - The CCC must be located at a reasonable physical distance from the actual location of crisis. Depending on the nature of the crisis, the CCC can be located at the same primary location from where the business functions. However, it is essential to have more than one location identified in advance. Depending on where the crisis strikes and the nature of the crisis, the CCC location can be chosen from the identified locations.
  - The lead of the CCC must have sufficient authority and mandate to make decisions. He/she must be someone who has complete knowledge of the business.
  - Individuals must be identified to interact with external agencies such as press and law enforcement.

The above is an indicative list of how to effectively operate a CCC in the event of a crisis. As always, the list is not exhaustive.
1. Being aware of how information security performance is perceived by senior management and other parts of the business is of fundamental importance to assure alignment.

2. Information security events are random, independent and are not targeted.

3. Statistical analyses using a Gaussian (normal) distribution are of use, as are most leading indicators, such as key performance indicators (KPIs).

4. In May 2005, Reid Hoffman launched LinkedIn from San Francisco, California, USA, with a focus on connecting all academic people.

5. The survey showed that some managers perceived that allowing the use of social networks at work is essential because their competition allows it.

6. The vulnerable aspect of attachments is that even if they appear to emanate from known friends, they could be potential attacks originated by hijacking users’ address books.

7. Based on the application’s profile, SALM tools generate a series of checklists of detective controls and corresponding guidelines to follow in various phases of the SDLC.

8. Each checklist item specifies an underlying security weakness, a succinct discussion of the control and a contextually tailored guideline based on the technology stack specified in the application priorities.

9. The dwell time is a measure of the time an intruder is on the network before being discovered and extricated.

10. Zero-day attacks are as prevalent as the number of successful intrusions perpetrated through vulnerabilities that remain unpatched long after the patch was released.

11. Cybercriminals sending a flood of emails containing malicious links create most botnets or attachments, which infect users’ workstations and beacon back to the command and control server for additional malware or instructions.

12. The IDS/IPS focused on signature-based measures and did not look at the heuristics to prevent anomalous behavior and network activity that behaves like malware.

13. Small organizations (less than 5,001 seats) experience a higher proportion of cybercrime costs relating to malicious insiders and malware.

14. Large organizations (greater than 15,000 seats) experience a higher proportion of costs relating to malicious insiders, stolen or hijacked devices, and denial of service.

15. Generally, the Poisson distribution for severity and the lognormal distribution for frequency are reasonable choices.

16. While Excel is a great environment for prototyping and solving less-complex problems, R is more suitable to heavy-duty work.

17. Like HTTP, WebSocket is a half-duplex, asynchronous communication protocol for delivering interactive web content.

18. WebSocket payload contains URL or application headers. This enables reputation-based defenses.

19. A comprehensive DCI solution scans through content that is packed in both existing and new standards in the network, applying advanced threat signature matching and heuristic threat analysis to detect noncompliant content and stop malicious content from sneaking in or confidential information from leaking out, thus significantly lowering the end user’s risk.

20. WebSocket allows organizations to transmit data for any application with any payload via a well-formed URL or HTTP headers.
Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current Journal subscribers. An electronic version of the quiz is available at www.isaca.org/cpequiz; it is graded online and is available to all interested parties.

If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information by email to info@isaca.org or by fax to +1.847.253.1443. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA.

Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

You will be responsible for submitting your credit hours at year-end for CPE credits.

A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.
ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE
The specialised nature of IT audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards are a cornerstone of the ISACA professional contribution to the audit and assurance community. The framework for the IT Audit and Assurance Standards provides multiple levels of guidance:

■ Standards define mandatory requirements for IT audit and assurance.

They inform:
- IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession’s expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

■ Guidelines provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.

■ Tools and Techniques provide specific information on various methodologies, tools and templates, and provide direction on how to implement and apply the information provided in the guidelines. They take a variety of forms, such as discussion documents, templates, white papers, audit programs or books (e.g., ISACA’s Technical Research Series of books: Security, Audit and Control Features SAP® ERP, 3rd Edition; Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition; Security, Audit and Control Features Oracle® Database, 5th Edition; and Security, Audit and Control Features PeopleSoft®, 3rd Edition).

COBIT® 5 is a business framework for the governance and management of enterprise IT. COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or public sector.

ISACA continually updates and expands the practical guidance and product family based on the COBIT framework. COBIT helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business. COBIT is available for download at www.isaca.org/cobit.

COBIT 5 for Assurance is currently under development and scheduled to be issued in the second quarter of 2013. It builds on COBIT 5 in that it focuses on IS audit and assurance and provides more detailed and practical guidance for IS audit and assurance professionals.

Links to current guidance are posted on the standards page, www.isaca.org/standards. Please note that the standards and guidelines are being updated for integration into the ITAF™ IS audit and assurance framework, www.isaca.org/itaf. The updated standards are scheduled to be issued in March 2013. An exposure draft of the revised guidelines is scheduled to be posted for comment on the ISACA web site in March.

The titles of issued standards documents are:

IT Audit and Assurance Standards
S1 Audit Charter Effective 1 January 2005
S2 Independence Effective 1 January 2005
S3 Professional Ethics and Standards Effective 1 January 2005
S4 Professional Competence Effective 1 January 2005
S5 Planning Effective 1 January 2005
S6 Performance of Audit Work Effective 1 January 2005
S7 Reporting Effective 1 January 2005
S8 Follow-up Activities Effective 1 January 2005
S9 Irregularities and Illegal Acts Effective 1 September 2005
S10 IT Governance Effective 1 September 2005
S11 Use of Risk Assessment in Audit Planning Effective 1 November 2005
S12 Audit Materiality Effective 1 July 2006
S13 Using the Work of Other Experts Effective 1 July 2006
S14 Audit Evidence Effective 1 July 2006
S15 IT Controls Effective 1 February 2008
S16 E-commerce Effective 1 February 2008

IT Audit and Assurance Guidelines
G1 Using the Work of Other Experts Effective 1 March 2008
G2 Audit Evidence Requirement Effective 1 May 2008
G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
G5 Audit Charter Effective 1 February 2008
G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
G7 Due Professional Care Effective 1 March 2008
G8 Audit Documentation Effective 1 March 2008
G9 Audit Considerations for Irregularities Effective 1 September 2008
G10 Audit Sampling Effective 1 August 2008
G11 Effect of Pervasive IS Controls Effective 1 August 2008
G12 Organisational Relationship and Independence Effective 1 August 2008
G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
G14 Withdrawn 14 Jan 2013; See Generic Application Audit/Accrual Program
G15 Audit Planning Revised Effective 1 Mar 2010
G16 Withdrawn 14 Jan 2013; See Outsourced IT Environments Audit/Accrual Program

G17 Effect of Non-audit Role on the IS Auditor’s Independence Effective 1 May 2010
G18 Withdrawn 14 Jan 2013
G19 Withdrawn 1 September 2008
G20 Reporting Effective 16 September 2010
G21 Withdrawn 14 Jan 2013; See Security, Audit and Control Features SAP ERP, 3rd Edition, Audit Programs and ICQs
G22 Withdrawn 14 Jan 2013; See E-commerce and PKI Audit/Assurance Program
G23 Withdrawn 14 Jan 2013; See Systems Development and Project Management Audit/Accrual Program
G24 Withdrawn 14 Jan 2013
G25 withdrawn 14 Jan 2013; See VPN Security Audit/Assurance Program
G26 Withdrawn 14 Jan 2013
G27 Withdrawn 14 Jan 2013; See Mobile Computing Security Audit/Assurance Program
G28 Withdrawn 14 Jan 2013
G29 Withdrawn 14 Jan 2013; See Systems Development and Project Management Audit/Accrual Program
G30 Competence Effective 1 June 2005
G31 Withdrawn 14 Jan 2013; See Personally Identifiable Information Audit/Accrual Program
G32 Withdrawn 14 Jan 2013; See Business Continuity Management Audit/Accrual Program
G33 Withdrawn 14 Jan 2013; See E-commerce and PKI Audit/Assurance Program
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G36 Withdrawn 14 Jan 2013; See Biometrics Audit/Accrual Program
G37 Withdrawn 14 Jan 2013
G38 Withdrawn 14 Jan 2013; See Identity Management Audit/Assurance Program
G39 Withdrawn 14 Jan 2013
G40 Withdrawn 14 Jan 2013; See Security Incident Management Audit/Accrual Program
G41 Withdrawn 14 Jan 2013
G42 Continuous Assurance Effective 1 May 2010

Code of Professional Ethics Effective 1 January 2011
RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

Over 350 titles are available for sale through the ISACA® Bookstore. This insert highlights the new ISACA research and peer-reviewed books. See www.isaca.org/bookstore for the complete ISACA Bookstore listings.

**FEATURED...**

www.isaca.org/featuredbooks

**Auditor’s Guide for IT Auditing + Software Demo, 2nd Edition**

53WAG2

- Member: $95.00
- Nonmember: $105.00

**Cyber Security Policy Guidebook**

96WCSP

- Member: $90.00
- Nonmember: $100.00

**The Definitive Guide to the C + A Transformation**

13ITCAT

- Member: $70.00
- Nonmember: $80.00

**Information Technology Control and Audit, 4th Edition**

4CRC4

- Member: $90.00
- Nonmember: $100.00


5AS13

- Member: $275.00
- Nonmember: $285.00

**Official Certified Ethical Hacker Review Guide: For Version 7.1, 1st Ed**

15-IT

- Member: $40.00
- Nonmember: $50.00

**New Books...**

www.isaca.org/newbooks

**Internet and Related Security**

Official Certified Ethical Hacker Review Guide: For Version 7.1

416 pages, 2012—15-IT

- Member: $40.00
- Nonmember: $50.00

**SOC 2: A Users Guide**

58 pages, 2012—SOC

- Member: $35.00
- Nonmember: $75.00

2012, 58 pages. e-book (PDF download—purchase online only). WSOC

- Member: FREE
- Nonmember: $75.00

**New 2013 Study Aids**

CISA/CISM/CGEIT/CRISC—Page S-4

* Published by ISACA and ITGI

ISACA member complimentary download www.isaca.org/downloads

All prices are listed in US Dollars and are subject to change.
NEW/FEATURED BOOKS


By Richard E. Cascarino

Step-by-step guide to successful implementation and control of IT systems—including the Cloud

Many auditors are unfamiliar with the techniques they need to know to efficiently and effectively determine whether information systems are adequately protected. Now in a Second Edition, Auditor’s Guide to IT Auditing presents an easy, practical guide for auditors that can be applied to all computing environments.

- Follows the approach used by the Information System Audit and Control Association’s model curriculum, making this book a practical approach to IS auditing
- Serves as an excellent study guide for those preparing for the CISA and CISM exams
- Includes discussion of risk evaluation methodologies, new regulations, SOX, privacy, banking, IT governance, COBIT, outsourcing, network management, and the Cloud

As networks and enterprise resource planning systems bring resources together, and as increasing privacy violations threaten more organization, information systems integrity becomes more important than ever. Auditor’s Guide to IT Auditing, Second Edition empowers auditors to effectively gauge the adequacy and effectiveness of information systems controls.

464 Pages, 2012. 53WAG2

Member $95.00  Nonmember $105.00

Cyber Security Policy Guidebook

By Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss

Drawing upon a wealth of experience from academia, industry, and government service, Cyber Security Policy Guidebook details and dissects, in simple language, current organizational cyber security policy issues on a global scale—taking great care to educate readers on the history and current approaches to the security of cyberspace. It includes thorough descriptions—as well as the pros and cons—of a plethora of issues, and documents policy alternatives for the sake of clarity with respect to policy alone. The Guidebook also delves into organizational implementation issues, and equips readers with descriptions of the positive and negative impact of specific policy choices.

Inside are detailed chapters that:
- Explain what is meant by cyber security and cyber security policy
- Discuss the process by which cyber security policy goals are set
- Educate the reader on decision-making processes related to cyber security
- Describe a new framework and taxonomy for explaining cyber security policy issues
- Show how the U.S. government is dealing with cyber security policy issues

With a glossary that puts cyber security language in layman’s terms—and diagrams that help explain complex topics—Cyber Security Policy Guidebook gives students, scholars, and technical decision-makers the necessary knowledge to make informed decisions on cyber security policy.

288 Pages, 2012. 95-WCSP

Member $90.00  Nonmember $100.00

The Definitive Guide to the C & A Transformation

by Dr Julie Mehari, Waylon Krush

The Definitive Guide to the C & A Transformation provides an authoritative guide to authorization for person with knowledge of information systems and/or information systems security, but not necessarily the same level of expertise with certification and accreditation (C&A) standards and best practices; it points to reference for further knowledge. It is scoped to present the information needed to meaningfully recognize, implement, and manage authorization requirements and achieve compliance with federal, local and agency laws and policies.

608 pages, 2009. 13ITCAT

Member $70.00  Nonmember $80.00

* Published by ISACA and ITGI  ISACA member complimentary download www.isaca.org/downloads  All prices are listed in US Dollars and are subject to change
by Michael Wallace, Larry Webber

IT Governance Policies and Procedures, 2013 Edition is the premier decision-making reference to help you to devise an information systems policy and procedure program uniquely tailored to the needs of your organization. Not only does it provide extensive sample policies, but this valuable resource gives you the information you need to develop useful and effective policies for your unique environment.

IT Governance Policies and Procedures provides fingertip access to the information you need on:
- Policy and planning
- Systems analysis and design
- And more!

IT Governance Policies and Procedures, 2013 Edition has been updated to include:
- A new chapter covering service level agreements
- Updated information and new policy covering Agile project management
- Updated information on managing mobile devices such as tablets and smartphones
- New policies for managing user devices including “bring your own device” policy, flash drive usage, and loaning out hardware for temporary use
- New information and policy for managing the use of public and private “app stores” for downloading software on mobile devices such as tablets and smartphones
- Updated information and new policy covering Agile project management
- And much more!

1136 Pages, 2012. S-3

Official Certified Ethical Hacker Review Guide: For Version 7.1, 1st Ed
by Steven DeFino

Official Certified Ethical Hacker Review Guide: For Version 7.1 is a valuable resource to help you pursue the most recognized, respected hacking certification in the world. As experienced instructors of the International Council of Electronic Commerce Consultants (ED-Council), the authors draw on firsthand experience training top-caliber information security professionals for success on the council’s Certified Ethical Hacker (CEH) exam. The only exam review guide officially endorsed by the EC-Council, this proven resource focuses on the core concepts that are covered on the newest certification course (version 7.1), as well as a wide array of useful learning tools, including chapter objectives, step-by-step tutorials, “Try it Out” exercises and challenges, group discussion topics, short lab examples, and practice exam questions and answers with explanations. The official CEH course teaches the latest hacking techniques, exploits, automated programs, and defensive recommendations, preparing students to audit organizations’ protection of their information assets through a deep understanding of the methodologies and tools of the attack process. The official CEH Exam review guide can be used to either preview and prepare for this comprehensive course or review afterwards to prepare for the challenging exam. It is the perfect complement that gives any student a real advantage toward success with this certification.

416 pages, 2012. 15-IT

SOC 2: A User Guide
by ISACA

SOC 2 is a Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy. This guide is intended for those evaluating a service organization’s SOC 2 report as part of a governance, risk and compliance (GRC) program; vendor assessment; security evaluation; business continuity plan, or other control evaluation. It may also be useful to those considering requesting a SOC 2 report from an existing vendor that does not currently provide a report or from a new vendor as part of the due-diligence or request-for-proposal (RFP) process. Users of this guide might include:
- Management of the user entity
- Those in procurement and contract negotiation
- Those overseeing vendor management
- Practitioners evaluating or reporting on controls at a user entity
- Independent auditors of user entities
- Regulators

Those performing services related to controls at the service organization, such as a service auditor reporting on controls at a user entity that is also a service provider to other user entities. AICPA and ISACA have jointly released this guide to provide user entities with the information they need when interpreting the SOC 2 reports received from service organizations. This guide also complements the companion piece for the SOC 1 guide, which can be found at www.isaca.org/service-auditor-standard.

2012, 58 pages. SOC

2012, 58 pages. e-book

* Published by ISACA and ITGI  ISACA member complimentary download www.isaca.org/downloads  All prices are listed in US Dollars and are subject to change
To prepare for the June or December 2013 CISA exam, order:

- CISA Review Manual 2013:
  - CRM-13 English Edition: $135.00
  - CRM-13C Chinese Simplified Edition: $135.00
  - CRM-13F French Edition: $135.00
  - CRM-13I Italian Edition: $135.00
  - CRM-13J Japanese Edition: $135.00
  - CRM-13S Spanish Edition: $135.00

- CISA Review Questions, Answers & Explanations Manual 2013:
  - QAE-13 English Edition: (950 Questions) $130.00
  - QAE-13C Chinese Simplified Edition: (950 Questions) $130.00
  - QAE-13I Italian Edition: (950 Questions) $130.00
  - QAE-13J Japanese Edition: (950 Questions) $130.00
  - QAE-13S Spanish Edition: (950 Questions) $130.00

- CISA Practice Question Database v13 (.100 Questions)*:
  - CDB-13 English Edition—CD-ROM: $225.00
  - CDB-13W Download—English Edition: $225.00
  - CAN* Candidate’s Guide to the CISA Exam and Certification: $15.00

To prepare for the June or December 2013 CISM exam, order:

- CISM Review Manual 2012:
  - CM-12J English Edition: $115.00
  - CM-12J Italian Edition: $115.00
  - CM-12J Japanese Edition: $115.00

- CISM Review Manual 2013:
  - CM-13 English Edition: $115.00
  - CM-13J Japanese Edition: $115.00
  - CM-13S Spanish Edition: $115.00

- CISM Review Questions, Answers & Explanations Manual 2012:
  - CQA-12 English Edition: (700 Questions) $90.00
  - CQA-12J Japanese Edition: (700 Questions) $90.00
  - CQA-12S Spanish Edition: (700 Questions) $90.00

  - CQA-12S English Edition: (100 Questions) $60.00
  - CQA-12S Japanese Edition: (100 Questions) $60.00
  - CQA-12S Spanish Edition: (100 Questions) $60.00

- CISM Practice Question Database v13 (.1000 Questions)*:
  - MDB-13 English Edition—CD-ROM: $160.00
  - MDB-13W Download—English Edition: $160.00
  - CSG* Candidate’s Guide to the CISM Exam and Certification: $15.00

To prepare for the June or December 2013 CGEIT exam, order:

- CGM-13* CGEIT Review Manual 2013: $115.00

- CGM-13S CGEIT Review Questions, Answers & Explanations Manual 2013 (60 Questions): $60.00

- CGM-13S* CGEIT Practice Questions, Answers & Explanations Manual 2013 Supplement (60 Questions): $60.00

- CSG* Candidate’s Guide to the CGEIT Exam and Certification: $15.00

To prepare for the June or December 2013 CRISC exam, order:

- CPR-13* CRISC Review Manual 2013: $115.00

- CPR-13S CRISC Review Questions, Answers & Explanations Manual 2013 (200 Questions): $60.00

- CPR-13S* CRISC Practice Questions, Answers & Explanations Manual 2013 Supplement (100 Questions): $60.00

- XMCR13-6M* CRISC Exam Self-Study Subscription—6 Months: $225.00

- CSG* Candidate’s Guide to the CRISC Exam and Certification: $15.00
### Code Title | Nonmember | Member
--- | --- | ---
WITAF* | Comprehensive software for implementing COBIT 4.1 as an IT governance, security or assurance tool. (See www.isaca.org/cobitbooks for components included in each Focus Set) |  |

**Meycor COBIT Suite**

See **NON-ENGLISH RESOURCES** for additional COBIT material.

### Enterprise Value: Governance of IT Investments

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITM*</td>
<td>Getting Started With Value Management</td>
<td>$40.00</td>
<td>$25.00</td>
</tr>
<tr>
<td>WITF*</td>
<td>The Val IT Framework 2.0</td>
<td>$90.00</td>
<td>$45.00</td>
</tr>
<tr>
<td>WITB*</td>
<td>The Business Case Guide—Using Val IT 2.0</td>
<td>$40.00</td>
<td>$25.00</td>
</tr>
<tr>
<td>WITAG*</td>
<td>Value Management Guidance for Assurance Professionals—Using Val IT 2.0</td>
<td>$40.00</td>
<td>$25.00</td>
</tr>
<tr>
<td>WITS*</td>
<td>Complete Set</td>
<td>$185.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>39-CRC</td>
<td>The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results</td>
<td>$90.00</td>
<td>$80.00</td>
</tr>
<tr>
<td>5-R0</td>
<td>A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>5-RTP</td>
<td>The Risk IT Framework</td>
<td>$95.00</td>
<td>$45.00</td>
</tr>
<tr>
<td>5-RTPG*</td>
<td>The Risk IT Practitioner Guide</td>
<td>$115.00</td>
<td>$55.00</td>
</tr>
</tbody>
</table>

### Risk Related Topics

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>78-WRM</td>
<td>The Failure of Risk Management: Why It’s Broken and How to Fix It</td>
<td>$60.00</td>
<td>$50.00</td>
</tr>
<tr>
<td>70-WFR</td>
<td>Fraud Risk Assessment: Building a Fraud Audit Program</td>
<td>$84.00</td>
<td>$74.00</td>
</tr>
<tr>
<td>11-CRCB</td>
<td>How to Complete a Risk Assessment In 5 Days or Less</td>
<td>$98.00</td>
<td>$88.00</td>
</tr>
<tr>
<td>84-WRM</td>
<td>Information Technology Risk Management in Enterprise Environments</td>
<td>$110.00</td>
<td>$100.00</td>
</tr>
<tr>
<td>2-HBS</td>
<td>IT Risk: Turning Business Threats Into Competitive Advantage</td>
<td>$45.00</td>
<td>$35.00</td>
</tr>
<tr>
<td>1-HHP</td>
<td>The Operational Risk Handbook for Financial Companies</td>
<td>$63.00</td>
<td>$53.00</td>
</tr>
<tr>
<td>5-PL</td>
<td>Risk Management &amp; Risk Assessment</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
</tbody>
</table>

### Audit, Control and Security—Essentials

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>48-CRC</td>
<td>Access Control, Security, and Trust: A Logical Approach</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>1-ITQ</td>
<td>Accounting Information Systems, 5th Edition</td>
<td>$162.00</td>
<td>$131.00</td>
</tr>
<tr>
<td>93-WAAS</td>
<td>Auditing and Assurance Services: Understanding the Integrated Audit</td>
<td>$235.00</td>
<td>$225.00</td>
</tr>
<tr>
<td>6-PL</td>
<td>Auditing IT Infrastructures</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>55WAI2</td>
<td>Auditor’s Guide for IT Auditing + Software Demo, 2nd Edition</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>76-WSL</td>
<td>Build Your Own Security Lab: A Field Guide for Network Testing</td>
<td>$60.00</td>
<td>$50.00</td>
</tr>
<tr>
<td>43-CRC</td>
<td>Building an Effective Information Security Policy Architecture</td>
<td>$94.00</td>
<td>$84.00</td>
</tr>
<tr>
<td>31-CRC</td>
<td>Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI</td>
<td>$140.00</td>
<td>$130.00</td>
</tr>
<tr>
<td>79-WCAF</td>
<td>Computer Aided Fraud Prevention and Detection: A Step by Step Guide</td>
<td>$74.00</td>
<td>$64.00</td>
</tr>
<tr>
<td>51-CRC</td>
<td>Data Protection: Governance, Risk Management, and Compliance</td>
<td>$86.00</td>
<td>$76.00</td>
</tr>
<tr>
<td>13-ITCIA</td>
<td>The Definite Guide to the C&amp;A Transformation</td>
<td>$80.00</td>
<td>$70.00</td>
</tr>
<tr>
<td>50-WRMP</td>
<td>Effective Project Management: Traditional, Agile, Extreme, 6th Edition</td>
<td>$70.00</td>
<td>$60.00</td>
</tr>
<tr>
<td>1-ABES</td>
<td>Enterprise Security for the Executive: Setting the Tone from the Top</td>
<td>$45.00</td>
<td>$35.00</td>
</tr>
<tr>
<td>92-WA</td>
<td>The Essential Guide to Internal Auditing, 2nd Edition</td>
<td>$65.00</td>
<td>$55.00</td>
</tr>
<tr>
<td>71-WOF</td>
<td>Essentials of Corporate Fraud</td>
<td>$58.00</td>
<td>$48.00</td>
</tr>
<tr>
<td>62-WACL</td>
<td>Fraud Analysis Techniques Using ACL</td>
<td>$221.00</td>
<td>$211.00</td>
</tr>
<tr>
<td>11-IT</td>
<td>Guide to Firewalls and VPNs, 3rd Edition</td>
<td>$180.00</td>
<td>$170.00</td>
</tr>
<tr>
<td>7-ART</td>
<td>Implementing the ISO/IEC 27001 Information Security Management System Standard</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>2-ABA</td>
<td>Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists</td>
<td>$130.00</td>
<td>$120.00</td>
</tr>
<tr>
<td>4-CRC4</td>
<td>Information Technology Control and Audit, 4th Edition</td>
<td>$100.00</td>
<td>$90.00</td>
</tr>
<tr>
<td>95-WIQA</td>
<td>Interpretation and Application of International Standards on Auditing</td>
<td>$115.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>8-PL</td>
<td>IT Auditing: The Process</td>
<td>$105.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>90-WACS</td>
<td>IT Audit, Control, and Security</td>
<td>$100.00</td>
<td>$90.00</td>
</tr>
</tbody>
</table>

### IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITCCO*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>$50.00</td>
<td>FREE</td>
</tr>
<tr>
<td>ITCCO*</td>
<td>Print Format</td>
<td>$60.00</td>
<td>FREE</td>
</tr>
<tr>
<td>STDK*</td>
<td>IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals</td>
<td>$20.00</td>
<td>$15.00</td>
</tr>
<tr>
<td>ITAF*</td>
<td>IT Audit. A Professional Practices Framework</td>
<td>$45.00</td>
<td>FREE</td>
</tr>
<tr>
<td>15-MT2</td>
<td>IT Auditing Using Controls to Protect Information Assets, 2nd Edition</td>
<td>$80.00</td>
<td>$70.00</td>
</tr>
</tbody>
</table>

### IT Control Objectives for Baseline II

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITCCB*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>$35.00</td>
<td>FREE</td>
</tr>
<tr>
<td>ITCCB*</td>
<td>Print Format</td>
<td>$50.00</td>
<td>$20.00</td>
</tr>
<tr>
<td>FSOX*</td>
<td>IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition</td>
<td>$7.00</td>
<td>$7.00</td>
</tr>
</tbody>
</table>

### Knowledge Areas

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>22-SM</td>
<td>Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists</td>
<td>$60.00</td>
<td>$50.00</td>
</tr>
</tbody>
</table>
**Security Considerations for Cloud Computing**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSCC</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>75.00</td>
<td>FREE</td>
</tr>
<tr>
<td>SCC*</td>
<td>Print Format</td>
<td>75.00</td>
<td>35.00</td>
</tr>
<tr>
<td>24-MSEM</td>
<td>Information Security and Event Management (SEM) Implementation</td>
<td>75.00</td>
<td>65.00</td>
</tr>
<tr>
<td>27-MSC</td>
<td>Securing the Cloud: Network Security in the Age of Social Media</td>
<td>50.00</td>
<td>40.00</td>
</tr>
<tr>
<td>2-BSF</td>
<td>System Forensics, Investigation, and Response</td>
<td>100.00</td>
<td>90.00</td>
</tr>
<tr>
<td>29-MIWAS</td>
<td>Web Application Security: A Beginner’s Guide</td>
<td>50.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

**IT GOVERNANCE AND BUSINESS MANAGEMENT**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>94-WIERS</td>
<td>An Executive Guide to ITRS: Content, Costs and Benefits to Business</td>
<td>50.00</td>
<td>40.00</td>
</tr>
<tr>
<td>3-PAGE</td>
<td>7 Steps to Better Written Policies and Procedures</td>
<td>30.00</td>
<td>20.00</td>
</tr>
<tr>
<td>4-PAGE</td>
<td>Best Practices in Policies and Procedures</td>
<td>36.00</td>
<td>26.00</td>
</tr>
<tr>
<td>1-ITG*</td>
<td>Board Briefing on IT Governance, 2nd Edition</td>
<td>7.00</td>
<td>7.00</td>
</tr>
<tr>
<td>6-SYN</td>
<td>Business Continuity and Disaster Recovery Planning for IT Professionals</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>BMIS*</td>
<td>The Business Model for Information Security</td>
<td>60.00</td>
<td>45.00</td>
</tr>
<tr>
<td>54-WCO2</td>
<td>CIO Best Practices: Expanding Strategic Value with Information Technology, 2nd Edition</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>WCSS*</td>
<td>Creating a Culture of Security (e-book)</td>
<td>50.00</td>
<td>FREE</td>
</tr>
<tr>
<td>11-ITDG</td>
<td>The Data Governance Imperative</td>
<td>50.00</td>
<td>40.00</td>
</tr>
<tr>
<td>89-WEG</td>
<td>Empowering Green Initiatives with IT: A Strategy and Implementation Guide</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>13-IT</td>
<td>Ethics in Information Technology, 4th Edition</td>
<td>110.00</td>
<td>100.00</td>
</tr>
<tr>
<td>3-VH</td>
<td>Frameworks for IT Management</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>85-WF101</td>
<td>Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>64-WGRC</td>
<td>Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices</td>
<td>173.00</td>
<td>163.00</td>
</tr>
<tr>
<td>20-MHE</td>
<td>Hacking Exposed Malware and Rootkits: Malware &amp; Rootkits Secrets &amp; Solutions</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>67-WHF</td>
<td>Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation</td>
<td>62.00</td>
<td>52.00</td>
</tr>
<tr>
<td>WGIALS*</td>
<td>Identifying and Aligning Business Goals and IT Goals (E-book—PDF purchase online only)</td>
<td>35.00</td>
<td>20.00</td>
</tr>
</tbody>
</table>

**IT GOVERNANCE AND BUSINESS MANAGEMENT (cont.)**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-ID</td>
<td>Implementing Information Technology Governance: Models, Practices and Cases</td>
<td>110.00</td>
<td>100.00</td>
</tr>
<tr>
<td>46-CRC</td>
<td>Implementing the Project Management Balanced Scorecard</td>
<td>94.00</td>
<td>84.00</td>
</tr>
<tr>
<td>11-ITSD</td>
<td>Implementing Service Quality based on ISO/IEC 20000, 3rd Edition</td>
<td>35.00</td>
<td>25.00</td>
</tr>
<tr>
<td>2-ITG*</td>
<td>Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition</td>
<td>7.00</td>
<td>7.00</td>
</tr>
</tbody>
</table>

**Information Security Governance: Guidance for Information Security Managers**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSTG*</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>45.00</td>
<td>FREE</td>
</tr>
<tr>
<td>WSPP*</td>
<td>Information Security Harmonization: Classification of Global Guidance (E-book—PDF format purchase online only)</td>
<td>40.00</td>
<td>FREE</td>
</tr>
<tr>
<td>50-CRC</td>
<td>Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement</td>
<td>90.00</td>
<td>80.00</td>
</tr>
<tr>
<td>1-BSD2</td>
<td>Information Security Policies Made Easy, Version 12</td>
<td>805.00</td>
<td>705.00</td>
</tr>
<tr>
<td>2-PS3</td>
<td>Information Security Roles &amp; Responsibilities Made Easy, Version V3</td>
<td>505.00</td>
<td>495.00</td>
</tr>
<tr>
<td>3-IGI</td>
<td>Information Technology Governance and Service Management: Frameworks and Adaptations</td>
<td>205.00</td>
<td>195.00</td>
</tr>
</tbody>
</table>

**FIND OUT MORE ABOUT INFORMATION SECURITY GOVERNANCE**

- **Global Guidance (E-book—PDF format purchase online only)**
- **FREE**

**RETURN POLICY**

All purchases are final. No refunds or exchanges.

**DELIVERY**

Orders normally ship within 2-3 business days upon receipt of payment. Once shipped, delivery time can vary between 2-7 business days.

**CUSTOMS**

Customers are responsible for any custom duties/taxes/VAT charges levied by the country of destination. See www.isaca.org/shipping for further information.
Customer Order Form
Order Online at www.isaca.org/bookstore

PLEASE NOTE: READ PAYMENT TERMS AND SHIPPING INFORMATION BELOW. ALL ORDERS MUST BE PREPAID.

Please return to: ISACA, 1055 Paysphere Circle, Chicago, IL 60674, USA
Phone: +1.847.660.5650   Fax: +1.847.253.1443   E-mail: bookstore@isaca.org

Your contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. To learn more, please visit www.isaca.org and read our Privacy Policy.

Customer Information

Name ________________________________

ISACA Member:  □ No  □ Yes  Member Number __________________________

Company Name ____________________________

Address:  □ Home  □ Company

City __________________ State/Province __________________

Country __________________ Zip-Mail Code __________________

Phone Number ( ) _________________________

Fax Number ( ) ____________________________

E-mail Address ____________________________

Code __________________ Title/Item __________________ Quantity __________________

Unit Price __________________ Total __________________


Thank you for ordering from ISACA. All purchases are final.

Payment Information—Prepayment Required

□ Payment enclosed. Check payable to "ISACA" in US dollars, drawn on US bank.

□ Bank wire transfer in US dollars. Date of transfer ____________________________

□ Charge to ____________

□ Visa  □ MasterCard  □ Discover

□ American Express  □ Diners Club

Credit Card # ____________________________

Exp. Date ____________________________

Print Cardholder Name ____________________________

Signature of Cardholder ____________________________

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

<table>
<thead>
<tr>
<th>For Orders Totaling</th>
<th>Outside US</th>
<th>Within US</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to US $30.00</td>
<td>US $10.00</td>
<td>US $5.00</td>
</tr>
<tr>
<td>US $30.01 to US $50.00</td>
<td>US $15.00</td>
<td>US $7.00</td>
</tr>
<tr>
<td>US $50.01 to US $80.00</td>
<td>US $20.00</td>
<td>US $8.00</td>
</tr>
<tr>
<td>US $80.01 to US $150.00</td>
<td>US $26.00</td>
<td>US $10.00</td>
</tr>
<tr>
<td>Over US $150.00</td>
<td>17% of Total</td>
<td>10% of Total</td>
</tr>
</tbody>
</table>

No shipping charges apply to Mycor C200T.
No shipping charges apply to CSA Practice Question Database v13—download.
No shipping charges apply to CISM Practice Question Database v13—download.

Shipping Information (If different from customer information)

If shipping to a PO Box, please include street address to ensure proper delivery.

Name ________________________________

ISACA Member:  □ No  □ Yes  Member Number __________________________

Company Name ____________________________

Address:  □ Home  □ Company

City __________________ State/Province __________________

Country __________________ Zip-Mail Code __________________

Phone Number ( ) _________________________

Fax Number ( ) ____________________________

E-mail Address ____________________________

Code __________________ Title/Item __________________ Quantity __________________

Unit Price __________________ Total __________________


Sales Tax: Add sales tax if shipping to:

Louisiana (LA), Oklahoma (OK)—4%

Wisconsin (WI)—5%

Florida (FL), Minnesota (MN), Pennsylvania (PA), South Carolina (SC), Texas (TX), Washington (WA)—6%

California (CA), New Jersey (NJ), Puerto Rico (PR), Tennessee (TN)—7%

Illinois (IL)—9%

For all orders please include shipping and handling charge—see chart below.

Subtotal __________________

Shipping details www.isaca.org/shipping

International customers are solely responsible for paying all custom duties, service charges, and taxes levied by their country.

All purchases are final. Pricing, shipping and handling, and tax are subject to change without notice.
In Berlin, INSIGHTS Brings Down Walls!

See how IT can Build YOUR Business at ISACA’s INSIGHTS Conference Berlin 2013

Insights 2013 Leadership Forum puts you in smart company with unprecedented access to CEOs, CIOs and other business leaders from around the world.

- Get inspired and see how organizations are integrating IT into business strategies to drive innovation and results
- Gain vital information through spotlights and networking sessions with industry leaders
- Explore the intersection where SMART business meets SMART IT
- Preview tomorrow’s headlines, trends and how to build a SMARTER future with keynote speaker, renowned trend watcher and founder of the leading trend and research company Pocket Marketing/nxt, Dr. Herman Konings

INSIGHTS 2013, ISACA’s Exclusive Leadership Forum
10-12 June Berlin, Germany
Reserve your seat today at isaca.org/insights2013
Your GRC obligations span beyond your network into cloud, social media, suppliers and mobile devices

So does AdaptiveGRC

"WHAT I REALLY LIKE ABOUT THIS SOLUTION IS THAT IT COMBINES CONTROL MATERIAL AND FUNCTIONALITY THAT YOU DON'T FIND ANYWHERE ELSE"

HEAD OF TECHNOLOGY AUDIT & ASSESSMENT FROM A FORTUNE 50 COMPANY

<table>
<thead>
<tr>
<th>Does your system have these features?</th>
<th>AdaptiveGRC</th>
<th>Your System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can you instantly present a visual dashboard that concisely summarizes your company’s state of operational compliance?</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Can you instantly report the state of compliance for multiple stakeholder perspectives? E.g. Data Protection Office, CFO, CISO etc.</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Was your system up and running in days, rather than months or years?</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Can you instantly correlate the results of different assessments across multiple regulations?</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Can you rapidly profile your riskiest vendors, technologies and departments to identify your audit and assessment priorities?</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

www.adaptivegrc.com