RISK
AUDITING
BUSINESS CONTINUITY
GOVERNANCE
COMPLIANCE

Volume 1, 2010

ISACA® Journal

Columns

4
IS Security Matters: Cloudy Daze
Steven J. Ross, CISA, MBCP, CISSP

6
IT Audit Basics: The Minimum IT Controls to Assess in a Financial Audit (Part I)
Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA

10
Five Questions With...
Linda Kostic, CISA, CISSP, CPA

Features

12
Book Review: The Definitive Handbook of Business Continuity Management, 2nd Edition
Reviewed by A Rafeq, CISA, CGEIT, CIA, CCSA, FCA

13
Book Review: Emerging Topics and Technologies in Information Systems
Reviewed by Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA

14
Book Review: The Business Value of IT
Reviewed by Reynaldo J. de la Fuente, CISA, CISM, CGEIT

15
Did We Hear the Warning Shot?
Bok Hai Suan, CISM, CGEIT, PMP

18
Performing a Security Risk Assessment
Ron Schmittling, CISA, CIA, CPA/CITP, and Anthony Munns, CISA, CIRM, CITP, FBCS, NCC-UK

26
Risk Landscape of Cloud Computing
Vasant Raval, CISA, DBA

32
Criteria and Methodology for GRC Platform Selection
Anand Singh, CISM, CISSP, and David J. Lilja, Ph.D.

38
Availability Risk Assessment—A Quantitative Approach
Hariharan, CISA

42
Looking at IT Risk Differently
A.V. Rameshkumar, CISA, CISM, AICWA, ACS, CPM, OCP (Oracle Financials), OCP (Application Developer)

44
Compliance for Compliance's Sake?
Dan Sollis

47
Using Spreadsheets and Benford's Law to Test Accounting Data
Mark G. Simkin, Ph.D.

53
Driving New Value From IT Risk Management
George Westerman, DBA, and Brian Barnier, CGEIT

Plus

52
Crossword Puzzle
Myles Mellor

59
Help Source Q&A
Gan Subramaniam, CISA, CISM, CIA, CISSP, SSCP, CCNA, CCSA, ISO 27001 LA

61
CPE Quiz #128
Based on Volume 5, 2009
Prepared by Sally Chan, CGEIT, CMA, ACIS

63
Standards, Guidelines, Tools and Techniques: ISACA Member and Certification Holder Compliance

S1-S4
ISACA Bookstore
Price List Supplement

Journal Online

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 for their first year of release. Use your unique member login credentials to access them at *www.isaca.org/journalonline.*

Online Features

The following articles will be available to ISACA members online on February 2010.

Continuous Auditing Reexamined
Norman Marks

Gobierno de las TIC ISO/IEC 38500
Manuel Ballester, Ph.D., CISA, CISM, CGEIT, IEEE

Information Technology Compliance: Past, Present and Future
Bryan C. Kissinger, Ph.D., CISA, CISSP

Service Integration in a Multivendor Outsourced IT Environment
Jan Vromant, CGEIT, ITIL SM

Soft IT Governance
Kazuhiro Uehara, CISA, CGEIT, CIA, PMP, and Sayaka Akino, CISA

Using CobiT 4.1 to Achieve Business-IT Alignment: A Practical Approach
Juan Ignacio Rouyet, Willem Joep Spauwen, and Luis Joyanes Aguilar

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.

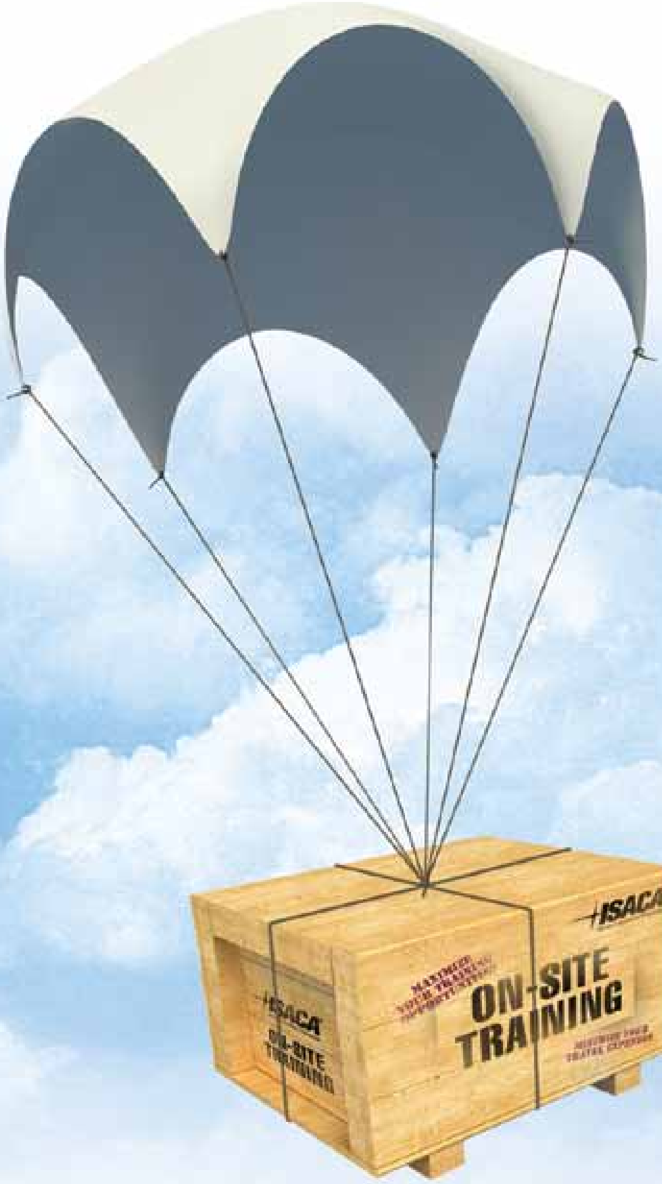
ISACA®
Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org

Please fill out the reader survey at *www.isaca.org/readersurvey* to help us improve the *Journal* to better serve our readers.

On-site Training

What you need, where you want it, when you need it.



www.isaca.org/onsitetraining2010

ISACA®

Trust in, and value from, information systems

Cloudy Daze

Steven J. Ross, CISA, MBCP, CISSP, a retired director from Deloitte, is the founder of Risk Masters Inc. He can be reached at *stross@riskmastersinc.com.*

Is cloud computing[1] really the revolutionary expansion of computing capabilities its proponents claim it to be? Or, is it the natural evolution of outsourcing trends that have been developing for decades? Is cloud computing more secure, or less?

Yes.

PLUS CA RESTE LA MÊME CHOSE…[2]

Most of the concerns about cloud computing that I have read and discussed center on one fact: the data and the software no longer reside in an organization's data center. It would appear that for many there is an internal calculation that possession equals control equals security, but is this equation meaningful? If the big change in cloud computing is the disappearance of data center walls, it is no change at all.

Almost as long as there have been computers there have been services that separate the processing of information from the possession of the equipment to do it. In the 1950s, IBM created the Service Bureau Corp. (SBC) to run programs on SBC's computers on behalf of corporate customers. It was some time before the term outsourcing came into vogue, but Ross Perot's Electronic Data Systems (EDS) was doing just that, beginning in 1962. The economies available through labor arbitrage drove many companies in the West to outsource information technology functions to organizations in Asia. Perhaps the perceptions of the problems with previous outsourcing efforts have raised fears about outsourcing to a cloud computing provider, but they are not new concerns.

Essentially, management's qualms about cloud computing can be reduced to two worries:

- My information is being processed somewhere, but I do not know where.
- My information is in the custody of someone, but I do not know who.

Scary to some, perhaps, but not much different from the fears encountered in another generation when the paper files in a desk drawer were translated to invisible bits in a data center elsewhere. Each time distance is put between the owners and processors of information, the same lessons must be relearned: transfer of custody does not equate to transfer of ownership. The basics of security and control for computing services have never changed:

- The ownership of the information (and its security) remains with the customer.
- The responsibility for executing security is shared between the owner and service provider.
- The owner of the information bears the responsibility for assuring that the provider executes and enforces security over the information.

Just because an organization does not own a data center or pay the operators does not mean that it loses control over the information and software. Reliance on physical controls over the instantiation of information is overrated. Except for backup tapes,[3] which present their own challenges, the data are neither tangible nor portable. Operators as privileged users are indeed a concern, but in today's technology—and tomorrow's—an operator does not need physical access to manipulate the data.

…PLUS CA CHANGE[4]

And yet, there are some substantial differences between older forms of outsourcing and cloud computing. The most obvious is that information is accessed via the Internet, with all that implies with regard to confidentiality and integrity. More subtle, but ultimately demanding more security, is that information technology is transformed into a dynamically scalable service, made possible by virtualization. If the promise of cloud computing is realized, an organization can rapidly expand and contract the software, infrastructure, network and storage it uses. The security that is appropriate for one set of computing resources, especially application data, may be inappropriate for another. With the context switching rapidly, it is difficult to match security with risk on a dynamic basis.[5]

There has been quite a lot written on cloud computing security that does not address this contextual change. The focus instead has been on the security threats that accompany outsourcing:

control over privileged access, difficulties with regulatory compliance, unknown location of data, segregating data among customers, investigative support and vendor viability.[6] There are a number of security considerations that go beyond outsourcing and are unique to the cloud:

- **Risk management is complicated by the dynamics of the services**. Inherent in all risk management approaches is the stability of the resources, if not their value, to be managed. If, for example, cloud computing is to be used by an online retailer for advertising most of the year and expanded for sales in peak periods, the inherent risks are quite different at various times of the year. The risks might be somewhat identifiable if the switch from advertising to sales were carried out at once, but would be much more difficult to determine if the change were effected irregularly over time.
- **Because applications and information are accessed over the Internet, browsers become access control mechanisms, in general, beyond the capabilities of most commercial browsers today.** It is possible to limit destinations and activities with many browsers, but few have the capability to identify users reliably or to limit access with sufficient granularity. Integration of browsers with identification and access management systems is a necessary precursor to widespread use of cloud computing for commercial purposes.
- **It is difficult to quantify and transfer risk through insurance.** Cloud computing providers carry insurance, to be sure, but not for consequential damages to their customers. Owners of information cannot abdicate responsibility to their servicers. At the same time, insurers cannot provide coverage for an unknown and irregularly changeable set of information resources, necessitating either over- or underinsurance. Given those two choices, it is easy to predict that management in many cases would choose the lowest premium and accept (ignore?) the remaining risk.
- **A robust encryption scheme, supported by an equally robust public key infrastructure (PKI), is necessary to achieve confidentiality and integrity for Internet-based services.** With data commingled on a provider's far-flung virtual and actual systems, encryption needs to be employed not only for data deemed sensitive, but for all data in the cloud. (Unfortunately, this opens a vulnerability to loss of data and service availability.) While there are strong encryption algorithms and key management schemes available today, cloud computing demands a global, institutionalized public key management system. Currently, the experience in using both encryption and PKI is hardly universal. There are bound to be serious missteps on the road to gaining that experience.

Information security for cloud computing, as always, comes at a cost. The difficulties mentioned with risk management also make determinations of the cost-effectiveness of security controls problematic. We are still very much in the infancy of cloud computing, and the economics of scale are running counter to this new technology being used broadly by large enterprises. Based on the experience with other new technologies, I expect that cloud computing will proceed with inadequate security, then losses will occur, and finally security will be viewed less as overhead and more as an enabler.

The greatest risk in using cloud computing, in my opinion, is the possibility of corporate amnesia, the loss of information without the possibility of recovering it.[7] This raises the whole issue of recoverability in the cloud, a subject to be addressed in a future column.

ENDNOTES

[1] An entire article could be written on definitions of cloud computing. (In fact, there are already quite a few. For example: Kennedy, Niall, "The Anatomy of Cloud Computing," 14 March 2009, *http://www.niallkennedy.com/blog/2009/03/cloud-computing-stack.html*. Bulkely, William; "How Well Do You Know…The Cloud," *The Wall Street Journal*, 12 October 2009.) For purposes of level setting, I shall define it as dynamically scalable, virtualized computing services offered internally and as a commercial service, using Internet technology for access.

[2] Jean-Baptiste Alphonso Karr (1808-1890), "plus ca change, plus ca reste la même chose," "the more things change, the more things stay the same."

[3] Ross, Steven J.; "Falling Off the Truck," *Information Systems Control Journal*, vol. 3, 2006

[4] *Op cit*, Jean-Baptiste Alphonso Karr

[5] Readers might find value in a podcast I made, "Cloud computing data security creates challenges for compliance officers," *http://itknowledgeexchange.techtarget.com/it-compliance/cloud-computing-data-security-creates-challenges-for-compliance-officers/*, 29 July 2009

[6] There are many sources for these views. See Heiser, Jay; Mark Nicolett; "Assessing the Security Risks of Cloud Computing," Gartner Inc., June 2008. I am not giving short shrift to this Gartner publication. Rather, it is representative of much that is currently published.

[7] As of the time of writing, customers of T-Mobile and Microsoft's Sidekick are experiencing a significant data loss. See "Some Users May Lose Data on a T-Mobile Smartphone," *New York Times*, 11 October 2009.

IT Audit Basics

The Minimum IT Controls to Assess in a Financial Audit (Part I)

Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA, is an associate professor of information systems (IS) at the University of Alabama at Birmingham (USA), a Marshall IS Scholar and a director of the Forensic Accounting Program. Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting IS using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998-1999 Innovative User of Technology Award. Singleton is the ISACA academic advocate at the University of Alabama at Birmingham. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications, including the *ISACA Journal*.

There are certain IT areas, IT general controls (ITGC), that systemically affect almost all financial audits because of their ubiquity and significance. They present potential risks to the financial statements associated with IT; that is, they inherently *may* introduce the risk of material misstatement (RMM) because of some potential, or actual, control deficiency and their relationship to financial reporting data or processing. Therefore, these areas could apply to any financial audit client and should be assessed as to their level of applicable risk to the audit objectives in all financial audits. It could be that all would apply to an audit, or just some, or possibly none (e.g., control risk is assessed at the maximum). But even then, these areas should be reviewed to make the determination that control risk is at the maximum (i.e., evidence it is at the max). Therefore, these areas are probably suitable for some type of review in all financial audits.

A major consideration of this risk process is related to scoping these key issues of ITGC. Because of the inherent broad scope of IT, and because of the inevitable fact that there are many potential weaknesses related to IT in even a well-controlled organization, and because there are always many things an IT auditor could judge as potential problems, it becomes difficult for some to properly scope the IT in a financial audit, especially if the IT auditor has only IT audit experience or education in the IT world (i.e., audits of IT for IT's sake; internal audits or consulting where the audit objective is to identify all of the deficiencies in a certain element of the IT space/portfolio). Thus, those who are relatively new to IT audit have to resist the natural inclination to include all of the IT "problems" as control objectives or deficiencies, when some of those problems probably lack the necessary prerequisite for a financial audit to have the potential to affect RMM on the financial statements. In any financial audit, the fact is, there will probably be some, maybe many, IT weaknesses or risks that are not relevant to the RMM of financial reports and should not lead to further audit procedures.

In a previous article, a discussion was provided on scoping the IT audit portion of a financial audit in compliance with the risk-based standards of the American Institute of Certified Public Accountants (AICPA) (SAS No. 104-111).[1] This two-part article follows up on that concept by providing a discussion on the actual thought process and activities an IT auditor would go through in properly scoping the IT audit procedures in a financial audit. First, there is a discussion of assessing the overall IT sophistication of a client in order to provide a general scope of the IT audit procedures needed. Second, five categories are suggested as the minimum areas to cover when assessing the RMM in a financial audit as it relates to the IT space of the auditee and the specific IT procedures (e.g., tests of controls) that should be performed in a particular financial audit.

THE ROLE OF THE LEVEL OF IT SOPHISTICATION

Throughout this two-part article, reference will be made to the "level of IT sophistication."[2] This concept is related to SAS No. 94, "The Effect of IT on the Auditor's Consideration of Internal Control in a Financial Statement Audit," where the guidance suggests the effect of IT is not necessarily related to the size of the entity but rather the level of sophistication of its IT. It is possible for a small company to rely heavily on IT for delivering its products or services and on IT controls in financial reporting processes. Thus, such an entity would likely be considered at a medium to high level of IT sophistication.

For example, a flexible spending account provider could use electronic funds transfer (EFT) to transfer employee deposits into its bank and debit cards for medical expenditures, and provide online access to manage all of the events. Although the entity might have fewer than 50 employees and a relatively small office space, it probably would be considered medium or high in its level of IT sophistication. Likewise, a manufacturer with hundreds of employees might use commercial off-the-shelf (COTS) applications, have a single server for financial reporting and, thus, be considered on the lower end of the spectrum of IT sophistication.

For simplicity's sake, the level of IT sophistication will be measured as low, medium or high; it may also be referred to as level 1, level 2 and level 3, respectively. Obviously, entities do not neatly and easily fall into one of these "buckets," and these levels are not discrete but rather a continuum or spectrum. Still, it is possible to rate the level of sophistication of IT and relevance of IT controls for an entity, as they relate to RMM and financial reporting, using this model. In the end, it takes some professional judgment to determine the actual level of IT sophistication, what specific IT issues are relevant (i.e., affect RMM) and, for those that are, the necessary IT audit procedures.

Generally speaking, the level of sophistication is directly related to the proper quantity and power of IT audit procedures. That is, a low level would use rather simple procedures (low-level strength such as inquiry[3] and observation) and would be rather limited as to the number of procedures. Likewise, the high end would require a relatively larger number of IT procedures, and some of the risks (RMM) would be high and, thus, require high-powered procedures and the use of stronger procedures such as reperformance and examination, rather than observation and inquiry.

While all of that may be intuitively obvious to any IT auditor, the issue is one of properly including all of the low-level auditees at the lower end of the spectrum and properly scoping (rating) auditees along the spectrum (i.e., eliminating IT weaknesses and problems that do not represent an RMM and including those that do). As mentioned earlier, it is tempting to include too many IT weaknesses as part of the financial audit's further audit procedures without taking into account a thorough thought process to ensure that the IT weakness can lead to a material misstatement where no compensating control exists. So the IT auditor must be careful to assess each IT weakness for its impact on RMM.

To assist IT auditors new to the field, a model for assessing the level of sophistication is presented here. This model could also be used to determine if a subject matter expert (SME)—an IT auditor (e.g., a CISA)—will be necessary to perform the IT procedures in a financial audit or if the "regular" financial auditors can perform the necessary procedures effectively. By default, that statement implies that at the lower end of the spectrum, it is possible for the IT procedures to be of such a nature that an SME is not always necessary.

A MODEL FOR ASSESSING THE LEVEL OF IT SOPHISTICATION

To describe some of the factors that classify an entity into one of the three levels, a model is presented that includes some quantitative IT factors (see **figure 1**). Each of these criteria is limited to those associated with the financial reporting systems, technologies and processes. Those IT elements *not* directly associated with financial reporting and the RMM are ignored in the assessment of relevant IT.

Level 1 is the lower end of the spectrum on IT sophistication and relevance. Generally speaking, there would be one server associated with financial reporting, a limited number of workstations (generally, fewer than 15 or so), no remote locations (associated with financial reporting), COTS applications and infrastructure, very few emerging or advanced technologies, and very few to no online transactions. Internal controls over financial reporting (ICFR) would not be overly reliant on IT or would be embedded in the COTS applications or limited to very few manual processes and controls. Many small to medium-sized entities would fit this description. Due to the scope of the minimum IT procedures

Figure 1—Model for IT Level of Sophistication

IT Sophistication	1: Low	2: Medium	3: High
Servers	1	2-3	>3
Network O/S	COTS	Nonstandard, or >1	Multiple/WAN
Workstations	~1-15	~15-30	~ 30+
Application	COTS	Some customizing	ERP and/or customized
Remote locations	None	~ 1-2	>2
ICFR	In COTS or few	Medium number and/or manual	Large number
Emerging/ advanced IT	None to few	Few to moderate	Moderate to many
Online transactions	None	Few	Many

for this level, limited in number and nature (inquiry and observation types), it is possible that these IT procedures could be performed by the "regular" financial auditors, albeit they may need a little training first.

Level 2 is the middle of the spectrum. Generally speaking, these entities would have more than one server associated with financial reporting, more than one network operating system (O/S) or a nonstandard one, more workstations than level 1 but fewer than about 30 in total, possibly some customizing of the application software (or relatively complex configuration of COTS, e.g., mid-size enterprise resource planning [ERP]), medium reliance on IT for ICFR or several manual controls, few to moderate number of emerging or advanced technologies, and few online transactions. This level would require an SME (i.e., a CISA or equivalent) to design and/or perform the necessary IT procedures.

Level 3 is the high end of the spectrum. This entity would have more than two servers associated with financial reporting, have remote locations, have generally more than 30 workstations associated with financial reporting, use ERP or write custom software, employ a large number of emerging or advanced technologies, and have possibly a large number of online transactions. The entity would also rely heavily on IT for ICFR. This entity will need one or more SMEs to perform the proper IT audit procedures.

> "The level of IT sophistication helps to determine the nature, extent and scope of IT procedures."

CONCLUSION

In this first part of the two-part article that addresses the minimum IT controls areas to consider in every financial audit, the discussion has focused on making a determination of the level of IT sophistication in the entity, which concomitantly measures the extent (scope) and nature of the IT procedures to include in the further audit procedures. That is, the level of IT sophistication helps to determine the nature, extent and scope of IT procedures. The more sophisticated the entity's IT, the more likely there will be more IT procedures (extent) and those procedures will be the stronger type (nature). There is also a necessary thought process to make sure any specific IT weakness identified represents RMM and not just a risk to the IT itself.

In the second part of the article (which will publish in volume 2, 2010), the next step is described, in which the IT auditor would use five areas of ITGC as the minimum areas of IT controls to examine in all financial audits, and use the concepts noted in this article in making the determination of nature, extent and timing of the proper IT audit procedures for an entity, especially identifying properly those IT risks that should be considered irrelevant and those that are relevant because they represent RMM. The end result is a proper scoping of the IT procedures to be included in a particular audit.

ENDNOTES

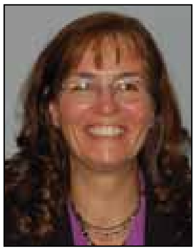
[1] Singleton, Tommie; "What Every IT Auditor Should Know About Scoping an IT Audit," *ISACA Journal*, vol. 4, 2009

[2] The use of the term "IT sophistication" implies that, as the IT portfolio becomes more sophisticated, there is more likelihood of RMM related to IT. Thus, occasionally, for clarification of reading, the term will be stated as "IT sophistication and relevance." That relevance is the back end of the IT sophistication process, where eventually the IT auditor in a financial statement audit *must* eliminate IT-related controls, problems and risks that do not represent RMM and cannot be directly linked to RMM. That is, only those IT issues that could lead to a material misstatement are *relevant* to the financial audit and are included in the IT audit procedures. But, that level of risk is invariably directly associated with the level of IT sophistication of the entity.

[3] The risk-based standards state that inquiry alone is not sufficient to gain adequate assurance over some control in the further audit procedures. Thus, some other type ("nature") of procedure would be needed to complement inquiry, and the lowest level "nature" procedure other than inquiry is observation. Thus, for a "low" level of risk where some procedure is being designed, something other than simple inquiry would need to be included. Examination and reperformance are considered "stronger" types ("nature") of procedures in a financial audit.

NOW MORE THAN EVER
GREAT COMPANIES NEED
GREAT AUDITORS
CISA
CPA
Visit our newly enhanced website www.landerint.com

Five Questions With…



Linda Kostic, CISA, CISSP, CPA

Linda Kostic began her career in accounting performing many functions, including accounts receivable, accounts payable, cost accounting, payroll and financial reporting. She then switched careers somewhat, moving into auditing—first in financial and then information technology. One IT audit role expanded into information security and quality assurance functions. Later, Kostic became a full-time information security manager, overseeing both the analysis of new systems and administration of established corporate systems. Then, she switched back into IT auditing, building an IT audit program with her current employer, before moving into enterprise risk management, where she has been involved in development, enhancement and training initiatives.

She recently began focusing on risk management disciplines, taking various related courses and working toward a professional risk management certification.

Kostic is a firm believer in getting involved in professional organizations. She is on the board of the ISACA National Capital Area Chapter, which she believes was instrumental in building both her leadership skills and a network of professional contacts at the local and international level.

Outside of her career and association with various organizations, Kostic enjoys the outdoors, taking long bicycle trips and, in recent years, running 10-milers and half marathons, primarily to raise money for various charities.

Q Regarding enterprise risk management, what do you believe is the single largest IT-related risk for businesses today? How do you see them meeting or not meeting this challenge?

A A combined security and fraud risk is the single largest IT-related risk for businesses today. Corporate networks have far-reaching boundaries and often include remote employees as well as outsourced and contracted resources. This expanded environment touching every area of the business has led to system and network complexities, exposure to ever-changing external vulnerabilities (organized exploits), competing priorities, and resource constraints increasing the risk of internal fraud. Unlike other risks, the overall success of a security program is dependent on all employees, contractors and outsourced/third-party providers complying with security policies and procedures. The various security disciplines required to identify, analyze, assess, implement and monitor security risks and related programs can be costly, resulting in competition for corporate capital to implement cost-effective programs.

> “Security awareness programs along with ongoing compliance monitoring minimize the risk of internal security vulnerabilities.”

Overall, I see the financial services industry meeting these challenges through ongoing networking with professional organizations, peers and various government agencies. Security awareness programs along with ongoing compliance monitoring minimize the risk of internal security vulnerabilities.

Q Could you describe the impact of the increasingly strict regulatory environment on the IT auditor?

A The positive impact includes strict guidance on technology-associated requirements, which typically follow best practices. This provides a tool to convince management that these best practices should be implemented. From a negative perspective, the IT auditor must remain current on the regulatory requirements and may be required to interpret them for management. More than one regulatory agency may govern a particular industry, requiring the IT auditor to evaluate the various regulatory requirements and identify the most stringent to be applied across the enterprise. This often requires the auditor to maintain key sources of information to stay current.

Q **How do you think the role of the IT auditor/professional is changing? What would be your best piece of advice for IT auditors as they plan their career path and look at the future of IT auditing?**

A In the beginning, computer systems and networks were not complex, resulting in less training and understanding of technology concepts, and minimizing the audit preparation and execution time. Now, an IT auditor must have the skills to evaluate complex systems and networks, and identify potential compensating controls in areas outside of the scope of the audit. And, since technology merely automates the business processes, it is important for IT auditors to expand their background to include financial and business processes specific to their organization as well as potential external factors, in order to fully understand the risk exposure.

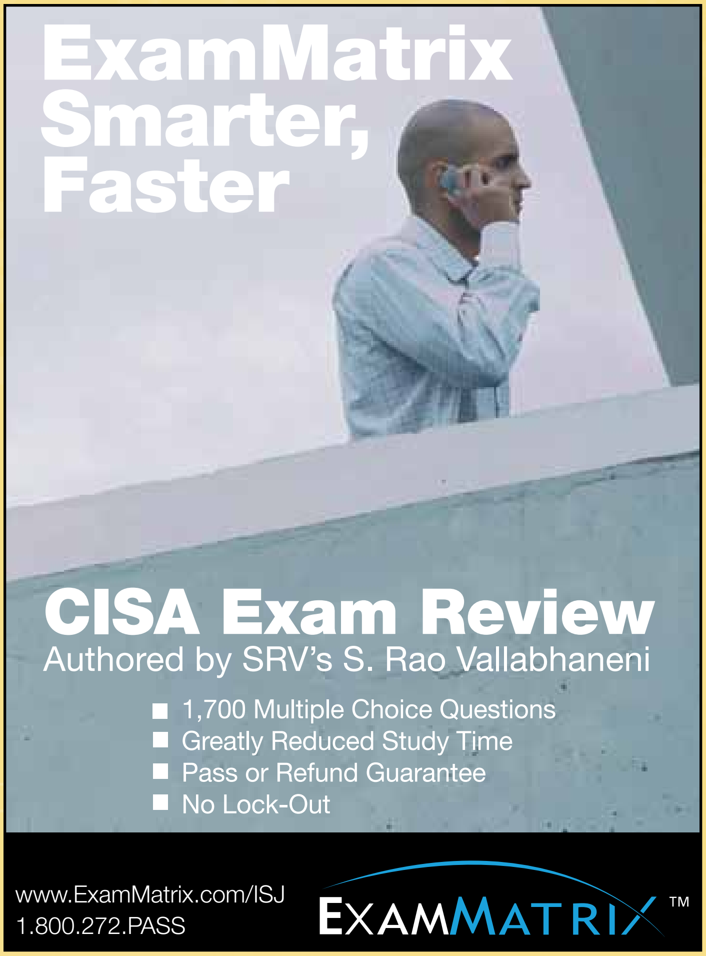
New auditors should be diverse and open to new disciplines, including managerial, financial and risk concepts, as part of their development goals. They need to be a partner with management to ensure that the most efficient and cost-effective recommendations addressing risks are reported. Last, as the business environment continues to change and resources become scarcer, IT auditors must be creative in the way they approach assignments and look for ways to add value back to the organization as part of and outside of scheduled audits.

Q **How do you believe utilizing social networking sites has helped you in your career and can help IT professionals in general?**

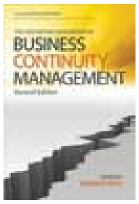
A Social networking sites provide a great forum for information sharing, especially in newer technologies or addressing general managerial challenges in today's business environment. This provides me with ideas when implementing various risk management initiatives. It also serves as a think tank forum for developing and sharing best practices. The only caution I would offer is that the source should be trustworthy; therefore, I recommend using those provided through established organizations. And, the users should be cautious not to share information that could be deemed corporate confidential or against corporate policies to reveal.

Q **What has been your biggest workplace challenge and how did you face it?**

A My biggest workplace challenge has been working with difficult individuals, which also turned out to be a great learning opportunity. In this experience, it was not sufficient to reference best practices or regulatory requirements as part of an audit recommendation; I had to "sell" the benefits as well. This forced me to analyze the risks in greater detail and consider potential compensating controls (system and manual).


ExamMatrix
Smarter,
Faster
CISA Exam Review
Authored by SRV's S. Rao Vallabhaneni
■ 1,700 Multiple Choice Questions
■ Greatly Reduced Study Time
■ Pass or Refund Guarantee
■ No Lock-Out
www.ExamMatrix.com/ISJ
1.800.272.PASS
EXAMMATRIX ™

The Definitive Handbook of Business Continuity Management, 2nd Edition



Edited by Andrew Hiles

Reviewed by A Rafeq, CISA, CGEIT, CIA, CCSA, FCA, an IT governance and assurance professional from Bangalore, India, with more than 25 years of experience in various roles such as chief financial officer, chief information officer, IT implementer, IT consultant, IT auditor and CobiT® trainer. He has been a CobiT user and implementer for more than 12 years and is a well-known CobiT evangelist. Rafeq has made presentations on IT governance, IT assurance and CobiT implementation at ISACA conferences worldwide. Rafeq is a past president of the ISACA Bangalore Chapter. He has also helped with development of ISACA's *CISA® Review Manual.*

Business continuity management is a continually evolving subject because of the rapid evolution of and critical dependence on IT, changes in business processes, emergence of new types of risks, and the continued and compelling need for enterprises to reduce the impact of disruptions and recover from interruptions. Business continuity management has progressed to becoming more holistic and focused on the business than on technology. *The Definitive Handbook of Business Continuity Management, 2nd Edition,* which features contributions from leading practitioners in the industry, is truly a handbook and is a valuable resource for anyone involved in, or looking to gain a detailed appreciation of, the rapidly emerging area of business continuity and disaster recovery within the corporate environment. The book is presented in an easy-to-follow format, explaining in detail the 10 core business continuity activities incorporated in the common body of knowledge agreed upon by the Disaster Recovery Institute International and the Business Continuity Institute. The contributors, who are from Asia, Australia, Europe, India, the Middle East and the US, provide a truly global perspective, bringing their own insights and approaches to the subject, sharing best practice from all corners of the world.

The book provides comprehensive information on business continuity practices and could be useful both as a how-to guide and as a reference book for the business library on the topic of business continuity management. The structured format, with many revealing case studies, examples and checklists, provides a clear road map, simplifying and demystifying business continuity processes for those new to its disciplines and providing a benchmark of current best practice for more experienced practitioners. These features make the book useful to business continuity managers, IT professionals, IT security and control professionals, and anyone interested in the field of business continuity management. This book makes a significant contribution to the knowledge base of business continuity and risk management.

The book has two main sections, 26 chapters and four appendices.

Section one of the book provides an executive overview of achieving and maintaining business continuity and has chapters on key concepts such as what is being planned, what a business continuity planning strategy is, a crisis management perspective of business continuity, multilateral continuity planning, marketing protection as a justification for funding of total asset protection programs, operational risk management, and business strategy and business continuity planning.

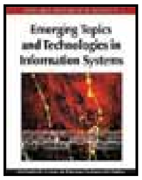
Section two of the book is a how-to guide on planning for business continuity.

The book has an inherent limitation in terms of lack of continuity resulting from contributions by different authors. An introductory chapter on business continuity management would have made the book useful to a novice reader. Sample templates are provided in some of the chapters, but the book could be even more useful if templates and practical examples had been provided for all the chapters, as relevant. Further, the chapter on business continuity audit could have been more comprehensive and focused.

EDITOR'S NOTE

The Definitive Handbook of Business Continuity Management, 2nd Edition, is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650.

Emerging Topics and Technologies in Information Systems



By Miltiadis D. Lytras and Patricia Cordonez de Pablos

Reviewed by Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA, an expert in software valuation, IS security and IS audit. A renowned faculty member at several management institutes, government academies and corporate training programs, Kanhere is a member of the Sectional Committee LITD 17 on Information Security and Biometrics of the Bureau of Indian Standards. He is currently newsletter editor and academic relations, standards and research coordinator of the ISACA Mumbai Chapter; member of the ISACA Publications Subcommittee; honorary secretary of the Computer Society of India, Mumbai Chapter; convener of a special interest group on security; chairman of WIRC of eISA; and convener of the security committee of the IT cell of Indian Merchants' Chamber. He can be contacted at *vkanhere@vsnl.com* or *vishnukanhere@yahoo.com.*

Emerging Topics and Technologies in Information Systems, a book by renowned academics with more than 100 publications in these areas, is a compilation of emerging issues, topics and challenges in information systems and technologies. It is an important reference book providing a source of knowledge for all those interested in knowing the current state-of-the-art technologies and trends in information systems.

With the growing use of information technology and systems across diverse fields and applications, and the reliance on information technology for high-end as well as routine operations and common use, knowledge of trends and technologies has become a must for those in charge of governance, operations managers, and IS professionals and auditors alike.

The authors have selected and prescribed a broad perspective and have covered a wide variety of topics. The 17 chapters cover topics ranging from measuring and reporting technological capital, knowledge management and enterprise resource planning (ERP), e-commerce and web technologies, mobile computing, wireless technologies, privacy issues, semantic models and agility in computing, virtual environments, and portals.

> "Knowledge of trends and technologies has become a must."

Each chapter is well organized, starting with an abstract followed by topic-specific discussions; is well illustrated with figures and diagrams; and includes appropriate conclusions and endnotes, where required. The book's wealth of references provides a launch pad for further reading and its index makes for easy access and usability. The chapter on technologies provides models and adaptation approaches, and discusses examples of applications and case studies, with screenshots where available.

In fact, the combined lessons of the 17 chapters provide an insight into the growing world of computing, from health care to flying and e-commerce to mobile/wireless technologies, that will help the IS professional and auditor to stay abreast of the latest advancements. The book gives a ring-side view of the challenges and issues that can add value to the exercise of IS control and IS audit.

Referring to the book prior to embarking on a new assignment will not only help in broadening the outlook, but will provide scope for lateral thinking and application of ideas, especially when information systems are being increasingly relied upon for decision support and as an integral part of human existence, business and commerce.

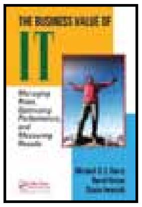
Emerging Topics and Technologies in Information Systems is a good reference book that is recommended for IS professionals who want to quickly move up the learning curve. It also provides ample material and ideas for applied research and development in cutting-edge technologies and emerging areas for future research.

EDITOR'S NOTE

Emerging Topics and Technologies in Information Systems is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650.

Book Review

The Business Value of IT



By Michael Harris, David Herron and Stasia Iwanicki

Reviewed by Reynaldo J. de la Fuente, CISA, CISM, CGEIT, chief executive officer of Datasec (*www.datasec-soft.com*), an IT governance, security and assurance company in Uruguay specializing in *ad hoc* software development. He was recognized with ISACA's 2005 John W. Lainhart IV Award for an outstanding contribution to developing the profession's common body of knowledge. He has served in several ISACA chapter and international positions since 1993.

This book provides simple, partial but rich coverage of some of the domains of the ISACA Certified in the Governance of Enterprise IT® (CGEIT®) certification, from an independent point of view.

The authors are experienced IT professionals highly aware that the cost/value relationship of IT for a business is an increasing concern of chief executive officers, chief information officers and chief financial officers, and they cleverly divide the book into four parts:

- Part I, "What Does IT Contribute to the Business?," explores important concepts on:
  - – How to measure the value of IT, using indicators such as return on investment (ROI), economic value added (EVA) and return on asset (ROA)
  - – How to use these IT value measurements for decisions, using dashboards, the business case and value visualization
  - – How to realize how much IT is enough, dealing with important decisions on IT spending in accordance with each organization
  - – How much to pay for IT, covering interesting topics regarding the always controversial issue of setting an appropriate IT budget
- Part II, "Why Should We Care About IT Governance?," deals with different but related aspects, such as who governs IT and what key elements they use; what IT governance frameworks and models, such as CobiT, IT Infrastructure Library (ITIL) and Capability Maturity Model Integration (CMMI), can be considered; how IT outsourcing can be adequately governed; and the benefit of using IT tools in the IT governance effort. This last concept is based on Howard Baetjer's book *Software as Capital*, in which he states, "In virtually all human production, we employ capital goods—tools—for the purpose. Much of our knowledge of how to produce is found not in our heads, but in those capital goods that we employ. Capital is embodied knowledge."
- Part III, "Why Should We Measure IT Performance?," discusses what performance means to IT and to the business, considers what the desired outcomes are, and looks at key measures and how to identify the key "missing measure" and the attributes of a successful measurement program. This section of the book focuses on IT development and tries to answer the question: is IT producing a high-quality product in a timely and cost-effective manner that functions according to the requirements?
- Part IV, "How Should We Change?," is a description of what changes should be made considering different angles:
  - – How can we manage IT changes?
  - – How should IT manage risk?
  - – How should IT manage its people?
  - – What should IT expect from the business?

"The cost/value relationship of IT for a business is an increasing concern of chief executive officers, chief information officers and chief financial officers."

The book is written in a very fresh and pleasant way from the perspective of authors with a deep IT background. It will be especially interesting for readers who want to understand the business value of IT.

EDITOR'S NOTE

The Business Value of IT is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, e-mail *bookstore@isaca.org* or telephone +1.847.660.5650.

Did We Hear the Warning Shot?

Bok Hai Suan, CISM, CGEIT, PMP, is the IT director of a large IT services company. He has oversight of the company's IT plan, policies, applications, security, infrastructure and operations and has many years of experience in business continuity planning (BCP). He has spoken at many regional conferences, sat on a number of IT professional committees, and published articles in books and journals.

The recent H1N1(A) flu pandemic saw companies desperately digging into their business continuity plan for a response. Some built their response plan from their severe acute respiratory syndrome (SARS) or avian flu plan. A few simply activated their cold or warm sites. Many did not do anything—they did not know what to do.

Fortunately, the fatality rate of the current H1N1(A) influenza pandemic is similar to the seasonal flu. However, the World Health Organization (WHO) warns against a second wave of deadlier mutated strains. The current wave is hence a warning shot.

Traditional business continuity planning (BCP) focuses on the loss of the use of physical and IT infrastructure and key personnel due to fire, explosion, earthquake or flood. The typical responses are activating the alternate data center, recovering data from remote backups, operating from secondary sites, repairing and rebuilding infrastructure, and switching back to normal operations. In a pandemic, the situation is drastically different (see **figure 1**). The physical and IT infrastructure are intact; the threat is in losing a large group of key personnel and key business supplies. This calls for different responses.

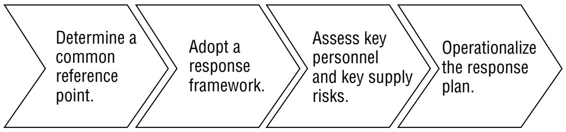
There are three key challenges in a pandemic:

1. **Uncertainties**—Unlike conventional outages where the outbreak is readily recognized and the extent of damage easily assessed, every virus has a different fatality rate, infection pattern and mutation potential. For instance, while SARS and the H1N1(A) flu pandemic are known to be transmitted between humans, avian flu is not. Without such knowledge, it is difficult to devise effective measures to prevent and contain the infection.
2. **Fear and anxiety**—The fear of life-threatening disease affects staff morale. Staff may choose to quit their job or to be absent from work. During the 2003 SARS outbreak, some medical professionals in affected areas left their jobs for fear of infection. Suppliers were also reluctant to deliver supplies to the hospitals. Similar impact was felt in the air travel and retail industries where there is a high volume of human contact. Losing key business supplies and key personnel can be catastrophic to an operation.
3. **No quick fix**—While the loss of physical and IT infrastructures may be repaired and replaced, finding a cure or vaccine to a pandemic takes time. They are subjected to stringent processes to test their effectiveness and safety before the health authorities approve their use. Companies may need to operate in crisis mode for months and this puts resources under great stress.

Figure 1—Pandemic vs. Traditional Crisis

Key Resources	Pandemic	Traditional Crisis
Key Physical and IT Infrastructure		
• Loss of key infrastructures	Not Likely	Likely
• Loss of access over a long period of time	Not Likely	Likely
• Loss of power supply over a long period of time	Not Likely	Likely
Key Personnel		
• Loss of key personnel	Likely	Likely
• Loss of access to key personnel over a long period of time	Likely	Likely
• Loss of more key personnel after the outbreak	Likely	Not Likely
Key Business Supplies		
• Disruption in supplies over a long period of time	Likely	Not Likely
Data and Equipment		
• Loss of access to data over a long period of time	Not Likely	Likely
• Loss of equipment	Not Likely	Likely
• Loss of access to equipment over a long period of time	Not Likely	Likely

Figure 2—Approach to Pandemic Key Challenges


Determine a common reference point.
Adopt a response framework.
Assess key personnel and key supply risks.
Operationalize the response plan.

In the face of these challenges, a different approach is needed (**figure 2**):

- **Determine a common reference point**—How does one know a pandemic has descended? Panic abounded when WHO raised its flu pandemic alert level from 1 to 5 within weeks following the discovery of the first case of H1N1(A) in Mexico. Different countries responded differently. Those that had suffered SARS took a cautious approach. They screened visitors' temperatures, isolated those with symptoms and tracked those who had close contact with the infected. The rest of the world took it like a seasonal flu. The different attitudes created tensions when some countries issued travel advisories and screened and quarantined visitors from affected areas. Likewise, different companies took the alert differently. Those that took it lightly were seen as irresponsible, while those that took it seriously were seen as overreacting. Similar tensions can occur among different units in a company.

  Establishing a common and reliable reference point is an important first step. While large companies may have the resources to assess the threat on their own, most companies will find it useful to look to WHO and local health authorities for guidance. A common reference point helps to defuse tensions between parties with different assessments of the gravity of the situation.
- **Adopt a response framework**—The second crucial step is to predetermine what the company will do as the pandemic alert level gets escalated. In WHO's six-phase framework, levels 1-3 indicate the need for capacity development and response planning activities, and 4-6 indicate the need for response and mitigation efforts. It is a useful framework to guide companies in their planning and execution. Companies should identify the activities, resources, investment and personnel required in each phase. This should be carried out prior to a need, as operationalizing the framework and plan into actionable steps takes much time and effort.
- **Assess key personnel and supply risks**—In a health-related contingency, companies have to assess how the loss of key personnel and business supplies increases business risks, such as not meeting contractual requirements, lost market share, impaired operations and tarnished image. Companies should systematically assess each operation to uncover and rank the risk exposures. They know who their key personnel are, what supplies are crucial and the parties upon whom they depend. The assessment helps to define the order of implementing preventive and corrective measures, and the manner by which limited resources are allotted. For companies operating in multiple geographies, the picture is a bit more complex, with different offices under different level of threats at any one time.
- **Operationalize the response plan**—The effectiveness of a response plan depends on what is known about the virus, such as whether it is airborne and how long it remains infectious on surfaces. Overreacting and underreacting are both costly to business. Consulting medical professionals and health authorities and benchmarking with peers in the same industry help to ensure the company is taking effective measures. These measures include:
  1. **Workplace diversity**—Splitting key personnel into different workplaces reduces the risk of mass infection should one workplace be infected. This requires a long-term plan as no one knows when a disease will strike and how long it will last. It is a costly solution. Telecommuting can be a viable alternative as it benefits the company in peace time and during a crisis. The infrastructure requirements include a virtual private network (VPN), broadband connection, notebook/laptop, printer, fax machine, conference bridge and video conference system. These needs should be acquired, installed and tested, and staff trained before an incident.
  2. **Human flow management**—In addition to workplace diversity, redesigning human flow within a workplace helps to reduce spreading of disease in locations where people congregate, including cafeterias, conference rooms, training rooms and presentation halls. In the recent pandemic, some companies have prohibited face-to-face meetings and staggered lunch breaks for key staff.

3. **Lights-off data center operations**—First developed as a cost-saving measure, it is a necessity in a pandemic situation. When personnel fall ill in a data center, it may not be accessible until it is disinfected. This can be problematic for operations that require frequent human operator interventions. Tools that can help to reduce such dependencies include remote console, job scheduler, large tape library and automated loaders.
4. **Health insurance coverage**—The human resources department needs to review medical and travel insurance to cover staff who get infected on official duties. This is crucial for staff working in high-risk areas such as hospitals and those traveling to areas with high infection risk and low health care standards. Engaging the service of an international emergency evacuation team may be necessary.
5. **Key business supplies**—In a worldwide epidemic, a global shortage of critical supplies is likely as supply chains may be hampered by the pandemic. Diversifying supplies, stockpiling and getting suppliers to develop their pandemic contingency plan are strategies to reduce the risk in supply disruption.
6. **Collaboration with business partners**—Companies could consider securing preferential medical care and supplies from their health care service providers. Swapping offices with business partners to achieve work-space diversification is a win-win strategy.
7. **Addressing key stakeholders' concerns**—Whatever measures the company takes, it must meet the expectations of the regulators, customers, business partners and employees. Companies must proactively listen to their stakeholders and address their concerns.
8. **Education and communication**—Companies should advise their staff whether they should travel to high-risk areas, when they should consult a doctor and what they should do to uphold a high level of personal hygiene. Setting up communication channels for staff to clarify doubts and to get assistance is good for staff morale.
9. **Incident handling**—In a pandemic situation, infection will ultimately creep into the workplace. When that happens, having a predefined and tested incident-handling procedure will help to minimize further infections, assure key stakeholders and contain business impact. An infection control mechanism typically includes setting up a well-trained and well-equipped infection control team, evacuating infected staff via a predefined isolated path, disinfecting the workplace, and tracing personal contacts.
10. **Media management**—As in any contingency, media must be handled carefully as unchecked negative rumors will hurt the company. Appointing a spokesperson helps to manage the quality and consistency of the information released. Having a communication plan and predrafted letters and e-mails help to reduce anxiety and speed up response to media queries.

CONCLUSION

The business risks of a pandemic are real. Just as companies are concerned with their key suppliers, their customers expect similar assurance from them. Failing to provide such assurance, their customers may diversify their suppliers or switch to other suppliers to lower their risks. Apart from this, a pandemic is a public health threat that may cause the local health authority to impose emergency policies and regulations to safeguard public safety. In some countries, noncompliance with these regulations may result in suspension of business licenses. The company may also be seen as socially irresponsible.

The current flu pandemic has surfaced gaps in BCP and given companies the opportunity to work on them. The problem is one does not know how much time one has.

Performing a Security Risk Assessment

Ron Schmittling, CISA, CIA, CPA/CITP, is a manager in the Risk Services practice at Brown Smith Wallace LLC, where he leads the IT security and privacy practice. Schmittling's more than 16 years of experience also include more than five years in senior-level technical leadership roles at a major financial services firm, as well as positions in IT audit, internal audit and consulting for several international organizations.

Anthony Munns, CISA, CIRM, CITP, FBCS, NCC-UK, coleads Brown Smith Wallace's risk services practice. Prior to joining the firm, he led Arthur Andersen's St. Louis (Missouri, USA)-based risk consulting practice and led the Great Plains (USA) regional business systems audit practice. His specialty is bringing major company practices to small and medium-sized companies. In his more than 20-year career, Munns has managed and audited the implementation and support of enterprise systems and processes including SAP, PeopleSoft, Lawson, JD Edwards and custom client/server systems.

Enterprise risk management (ERM)[1] is a fundamental approach for the management of an organization. Based on the landmark work of the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[2] in the 1990s, its seminal *Enterprise Risk Management—Integrated Framework*,[3] has become a primary tool for organizational risk management. Regulators in the US have recognized the value of an enterprise risk approach, and see it as a requirement for the well-controlled organization. Two primary examples of this are compliance with the US Sarbanes-Oxley Act[4] and the US Health Insurance Portability and Accountability Act (HIPAA),[5] both of which require a periodic risk assessment.

Although regulations do not instruct organizations on how to control or secure their systems, they do require that those systems be secure in some way and that the organization prove to independent auditors that their security and control infrastructure is in place and operating effectively. The enterprise risk assessment methodology has become an established approach to identifying and managing systemic risk for an organization. And, more and more, this approach is being applied in such diverse fields as environmental Superfund,[6] health[7] and corporate ratings.[8]

> "Perform security risk assessments that employ the enterprise risk assessment approach and include all stakeholders."

Classically, IT security risk has been seen as the responsibility of the IT or network staff, as those individuals have the best understanding of the components of the control infrastructure. Moreover, security risk assessments have typically been performed within the IT department with little or no input from others.

This approach has limitations. As systems have become more complex, integrated and connected to third parties, the security and controls budget quickly reaches its limitations. Therefore, to ensure best use of the available resources, IT should understand the relative significance of different sets of systems, applications, data, storage and communication mechanisms. To meet such requirements, organizations should perform security risk assessments that employ the enterprise risk assessment approach and include all stakeholders to ensure that all aspects of the IT organization are addressed, including hardware and software, employee awareness training, and business processes.

IT enterprise security risk assessments are performed to allow organizations to assess, identify and modify their overall security posture and to enable security, operations, organizational management and other personnel to collaborate and view the entire organization from an attacker's perspective. This process is required to obtain organizational management's commitment to allocate resources and implement the appropriate security solutions.

A comprehensive enterprise security risk assessment also helps determine the value of the various types of data generated and stored across the organization. Without valuing the various types of data in the organization, it is nearly impossible to prioritize and allocate technology resources where they are needed the most. To accurately assess risk, management must identify the data that are most valuable to the organization, the storage mechanisms of said data and their associated vulnerabilities.

REASONS/RATIONALE FOR PERFORMING A SECURITY RISK ASSESSMENT

Organizations have many reasons for taking a proactive and repetitive approach to addressing information security concerns. Legal and regulatory requirements aimed at protecting sensitive or personal data, as well as general public security requirements, create an

expectation for companies of all sizes to devote the utmost attention and priority to information security risks. An IT security risk assessment takes on many names and can vary greatly in terms of method, rigor and scope, but the core goal remains the same: identify and quantify the risks to the organization's information assets. This information is used to determine how best to mitigate those risks and effectively preserve the organization's mission.

Some areas of rationale for performing an enterprise security risk assessment include:

- **Cost justification**—Added security usually involves additional expense. Since this does not generate easily identifiable income, justifying the expense is often difficult. An effective IT security risk assessment process should educate key business managers on the most critical risks associated with the use of technology, and automatically and directly provide justification for security investments.
- **Productivity**—Enterprise security risk assessments should improve the productivity of IT operations, security and audit. By taking steps to formalize a review, create a review structure, collect security knowledge within the system's knowledge base and implement self-analysis features, the risk assessment can boost productivity.
- **Breaking barriers**—To be most effective, security must be addressed by organizational management as well as the IT staff. Organizational management is responsible for making decisions that relate to the appropriate level of security for the organization. The IT staff, on the other hand, is responsible for making decisions that relate to the implementation of the specific security requirements for systems, applications, data and controls.
- **Self-analysis**—The enterprise security risk assessment system must always be simple enough to use, without the need for any security knowledge or IT expertise. This will allow management to take ownership of security for the organization's systems, applications and data. It also enables security to become a more significant part of an organization's culture.
- **Communication**—By acquiring information from multiple parts of an organization, an enterprise security risk assessment boosts communication and expedites decision making.

ENTERPRISE SECURITY RISK ASSESSMENT METHODOLOGY

The enterprise risk assessment and enterprise risk management processes comprise the heart of the information security framework. These are the processes that establish the rules and guidelines of the security policy while transforming the objectives of an information security framework into specific plans for the implementation of key controls and mechanisms that minimize threats and vulnerabilities. Each part of the technology infrastructure should be assessed for its risk profile. From that assessment, a determination should be made to effectively and efficiently allocate the organization's time and money toward achieving the most appropriate and best employed overall security policies. The process of performing such a risk assessment can be quite complex and should take into account secondary and other effects of action (or inaction) when deciding how to address security for the various IT resources.

Depending on the size and complexity of an organization's IT environment, it may become clear that what is needed is not so much a thorough and itemized assessment of precise values and risks, but a more general prioritization. Determination of how security resources are allocated should incorporate key business managers' risk appetites, as they have a greater understanding of the organization's security risk universe and are better equipped to make that decision.

Each organization is different, so the decision as to what kind of risk assessment should be performed depends largely on the specific organization. If it is determined that all the organization needs at this time is general prioritization, a simplified approach to an enterprise security risk assessment can be taken and, even if it already has been determined that a more in-depth assessment must be completed, the simplified approach can be a helpful first step in generating an overview to guide decision making in pursuit of that more in-depth assessment.

> “Determination of how security resources are allocated should incorporate key business managers' risk appetites.”

If one is unsure what kind of assessment the organization requires, a simplified assessment can help make that determination. If one finds that it is impossible to produce accurate results in the process of completing a simplified assessment—perhaps because this process does not take into account a detailed enough set of assessment factors—this alone can be helpful in determining the type of assessment the organization needs.

The assessment approach or methodology analyzes the relationships among assets, threats, vulnerabilities and other elements. There are numerous methodologies, but in general they can be classified into two main types: quantitative and qualitative analysis. The methodology chosen should be able to produce a quantitative statement about the impact of the risk and the effect of the security issues, together with some qualitative statements describing the significance and the appropriate security measures for minimizing these risks.

Security risk assessment should be a continuous activity. A comprehensive enterprise security risk assessment should be conducted at least once every two years to explore the risks associated with the organization's information systems. An enterprise security risk assessment can only give a snapshot of the risks of the information systems at a particular point in time. For mission-critical information systems, it is highly recommended to conduct a security risk assessment more frequently, if not continuously.

> "An enterprise security risk assessment can only give a snapshot of the risks of the information systems at a particular point in time."

PROCESS

The objective of a risk assessment is to understand the existing system and environment, and identify risks through analysis of the information/data collected. By default, all relevant information should be considered, irrespective of storage format. Several types of information that are often collected include:

- Security requirements and objectives
- System or network architecture and infrastructure, such as a network diagram showing how assets are configured and interconnected
- Information available to the public or accessible from the organization's web site
- Physical assets, such as hardware, including those in the data center, network, and communication components and peripherals (e.g., desktop, laptop, PDAs)
- Operating systems, such as PC and server operating systems, and network management systems
- Data repositories, such as database management systems and files
- A listing of all applications
- Network details, such as supported protocols and network services offered
- Security systems in use, such as access control mechanisms, change control, antivirus, spam control and network monitoring
- Security components deployed, such as firewalls and intrusion detection systems
- Processes, such as a business process, computer operation process, network operation process and application operation process
- Identification and authentication mechanisms
- Government laws and regulations pertaining to minimum security control requirements
- Documented or informal policies, procedures and guidelines

The project scope and objectives can influence the style of analysis and types of deliverables of the enterprise security risk assessment. The scope of an enterprise security risk assessment may cover the connection of the internal network with the Internet, the security protection for a computer center, a specific department's use of the IT infrastructure or the IT security of the entire organization. Thus, the corresponding objectives should identify all relevant security requirements, such as protection when connecting to the Internet, identifying high-risk areas in a computer room or assessing the overall information security level of a department. The security requirements should be based on business needs, which are typically driven by senior management, to identify the desired level of security protection. A key component of any risk assessment should be the relevant regulatory requirements, such as Sarbanes-Oxley, HIPAA, the US Gramm-Leach-Bliley Act and the European Data Protection Directive.

The following are common tasks that should be performed in an enterprise security risk assessment (Please note that these are listed for reference only. The actual tasks performed will depend on each organization's assessment scope and user requirements.):

- Identify business needs and changes to requirements that may affect overall IT and security direction.
- Review adequacy of existing security policies, standards, guidelines and procedures.
- Analyze assets, threats and vulnerabilities, including their impacts and likelihood.

- Assess physical protection applied to computing equipment and other network components.
- Conduct technical and procedural review and analysis of the network architecture, protocols and components to ensure that they are implemented according to the security policies.
- Review and check the configuration, implementation and usage of remote access systems, servers, firewalls and external network connections, including the client Internet connection.
- Review logical access and other authentication mechanisms.
- Review current level of security awareness and commitment of staff within the organization.
- Review agreements involving services or products from vendors and contractors.
- Develop practical technical recommendations to address the vulnerabilities identified, and reduce the level of security risk.

Mapping threats to assets and vulnerabilities can help identify their possible combinations. Each threat can be associated with a specific vulnerability, or even multiple vulnerabilities. Unless a threat can exploit a vulnerability, it is not a risk to an asset.

The range of all possible combinations should be reduced prior to performing a risk analysis. Some combinations may not make sense or are not feasible. This interrelationship of assets, threats and vulnerabilities is critical to the analysis of security risks, but factors such as project scope, budget and constraints may also affect the levels and magnitude of mappings.

> “This interrelationship of assets, threats and vulnerabilities is critical to the analysis of security risks.”

Once the assets, threats and vulnerabilities are identified, it is possible to determine the impact and likelihood of security risks.

Impact Assessment

An impact assessment (also known as impact analysis or consequence assessment) estimates the degree of overall harm or loss that could occur as a result of the exploitation of a security vulnerability. Quantifiable elements of impact are those on revenues, profits, cost, service levels, regulations and reputation. It is necessary to consider the level of risk that can be tolerated and how, what and when assets could be affected by such risks. The more severe the consequences of a threat, the higher the risk. For example, if the prices in a bid document are compromised, the cost to the organization would be the product of lost profit from that contract and the lost load on production systems with the percentage likelihood of winning the contract.

Likelihood Assessment

A likelihood assessment estimates the probability of a threat occurring. In this type of assessment, it is necessary to determine the circumstances that will affect the likelihood of the risk occurring. Normally, the likelihood of a threat increases with the number of authorized users. The likelihood can be expressed in terms of the frequency of occurrence, such as once in a day, once in a month or once in a year. The greater the likelihood of a threat occurring, the higher the risk. It can be difficult to reasonably quantify likelihood for many parameters; therefore, relative likelihood can be employed as a ranking. An illustration of this would be the relative likelihood in a geographical area of an earthquake, a hurricane or a tornado, ranked in descending order of likelihood.

A systems example is the high likelihood of an attempt to exploit a new vulnerability to an installed operating system as soon as the vulnerability is published. If the system affected is classified as critical, the impact is also high. As a result, the risk of this threat is high.

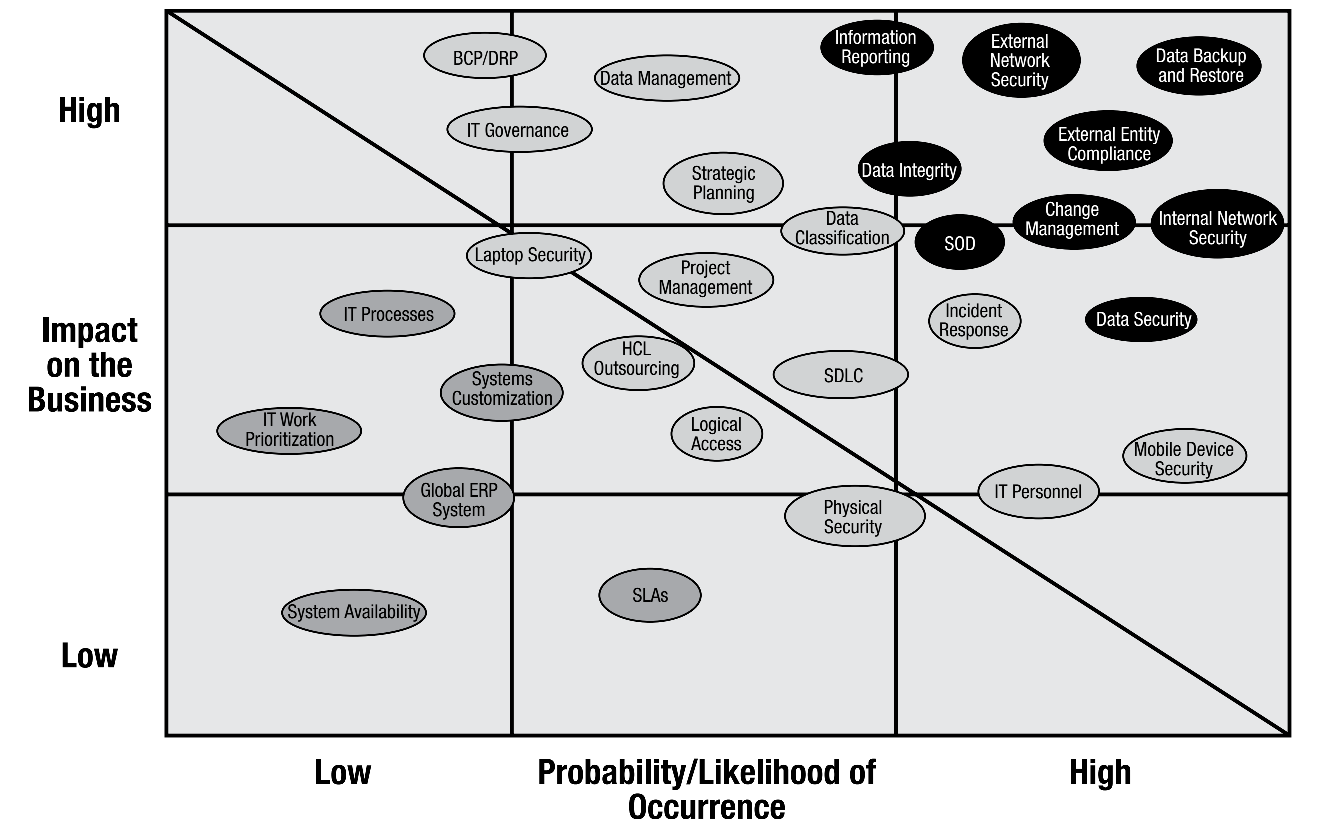
For each identified risk, its impact and likelihood must be determined to give an overall estimated level of risk. Assumptions should be clearly defined when making the estimation. This two-dimensional measurement of risk makes for an easy visual representation of the conclusions of the assessment. See **figure 1** for an example risk map.

ORGANIZATIONAL VALUE

Institutionalizing a practical risk assessment program is important to supporting an organization’s business activities and provides several benefits:

1. Risk assessment programs help ensure that the greatest risks to the organization are identified and addressed on a continuing basis. Such programs help ensure that the expertise and best judgments of personnel, both in IT and the larger organization, are tapped to develop reasonable steps for preventing or mitigating situations that could interfere with accomplishing the organization’s mission.
2. Risk assessments help personnel throughout the organization better understand risks to business operations. They also teach them how to avoid risky practices, such as disclosing passwords or other sensitive information, and

Figure 1—Risk Map



© 2008 Brown Smith Wallace LLC.

recognize suspicious events. This understanding grows, in part, from improved communication among business managers, system support staff and security specialists.

3. Risk assessments provide a mechanism for reaching a consensus as to which risks are the greatest and what steps are appropriate for mitigating them. The processes used encourage discussion and generally require that disagreements be resolved. This, in turn, makes it more likely that business managers will understand the need for agreed-upon controls, feel that the controls are aligned with the organization's business goals and support their effective implementation. Executives have found that controls selected in this manner are more likely to be effectively adopted than controls that are imposed by personnel outside of the organization.
4. A formal risk assessment program provides an efficient means for communicating assessment findings and recommending actions to business unit managers as well as to senior corporate officials. Standard report formats and the periodic nature of the assessments provide organizations a means of readily understanding reported information and comparing results between units over time.

Ultimately, enterprise security risk assessments performed with measurably appropriate care are an indispensable part of prioritizing security concerns. Carrying out such assessments informally can be a valuable addition to a security issue tracking process, and formal assessments are of critical importance when determining time and budget allocations in large organizations.

In contrast, taking a haphazard approach to security concern prioritization can lead to disaster, particularly if a problem falls into a high-risk category and then ends up neglected. IT-specific benefits of performing an enterprise security risk assessment include:

- Providing an objective approach for IT security expenditure budgeting and cost estimation
- Enabling a strategic approach to IT security management by providing alternative solutions for decision making and consideration
- Providing a basis for future comparisons of changes made in IT security measures

PITFALLS/LESSONS LEARNED

One of the key dangers of performing an enterprise security risk assessment is assuming where all the risks lie. It is important when structuring an enterprise security risk assessment to include as many stakeholders as possible. In one recent assessment, only IT management was to be interviewed, with the exception of a few internal audit organization members. While they certainly had many valid concerns, the group did not have the breadth of experience to form a complete picture of risk within the organization. By including a wider selection of operational, finance and human resources management, high-risk potentialities can be identified in areas such as research and development, HIPAA compliance, and sales management.

It is important to include personnel who are not only experienced in the complexities of systems and processes, but also have the ability to probe for areas of risk. A checklist is a good guideline, but is only the starting point in the process. With an experienced interviewer, the process can be as educational for the interviewee as it is for identifying risks.

Organizational executives have limited time, and it is often difficult to get on their calendars. There are three key steps to ease this part of the process:

1. Request that the executive sponsor directly address the interviewees by announcing the purpose of the risk assessment and its importance to the organization.
2. Within 48 hours of that communication, have the sponsor's office schedule the initial interview.
3. Send a tailored checklist to the executive prior to the interview and ask him/her to review it. This last step is to prepare him/her for the subject areas of the risk assessment, so that any apprehensions or reservations are allayed as he/she understands the boundaries of the interview.

It is important not to underestimate the value of an experienced facilitator, particularly for the higher-level interviews and the process of determining the ranking of risk likelihood. The use of experienced external resources should be considered to bring even more objectivity to the assessment.

CONCLUSION

An information security framework is important because it provides a road map for the implementation, evaluation and improvement of information security practices. As an organization implements its framework, it will be able to articulate goals and drive ownership of them, evaluate the security of information over time, and determine the need for additional measures.

A common element in most security best practices is the need for the support of senior management, but few documents clarify how that support is to be given. This may represent the biggest challenge for the organization's ongoing security initiatives, as it addresses or prioritizes its risks.

> "Overall, an organization must have a solid base for its information security framework."

Specifically, an enterprise security risk assessment is intended to be suitable for the following, which could be specific to any organization:

- A way to ensure that security risks are managed in a cost-effective manner
- A process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met
- A definition of new information security management processes
- Use by management to determine the status of information security management activities
- Use by internal and external auditors to determine the degree of compliance with the policies, directives and standards adopted by the organization
- For implementation of business-enabling information security
- To provide relevant information about information security to customers

Overall, an organization must have a solid base for its information security framework. The risks and vulnerabilities to the organization will change over time; however, if the organization continues to follow its framework, it will be in a good position to address any new risks and/or vulnerabilities that arise.

ENDNOTES

[1] The COSO *Enterprise Risk Management—Integrated Framework*, published in 2004, defines ERM as a "…process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

[2] COSO is a voluntary private-sector organization, established in the US, dedicated to providing guidance to executive management and governance entities on critical aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud and financial reporting.

[3] COSO, *Enterprise Risk Management—Integrated Framework Executive Summary*, September 2004, *www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf*

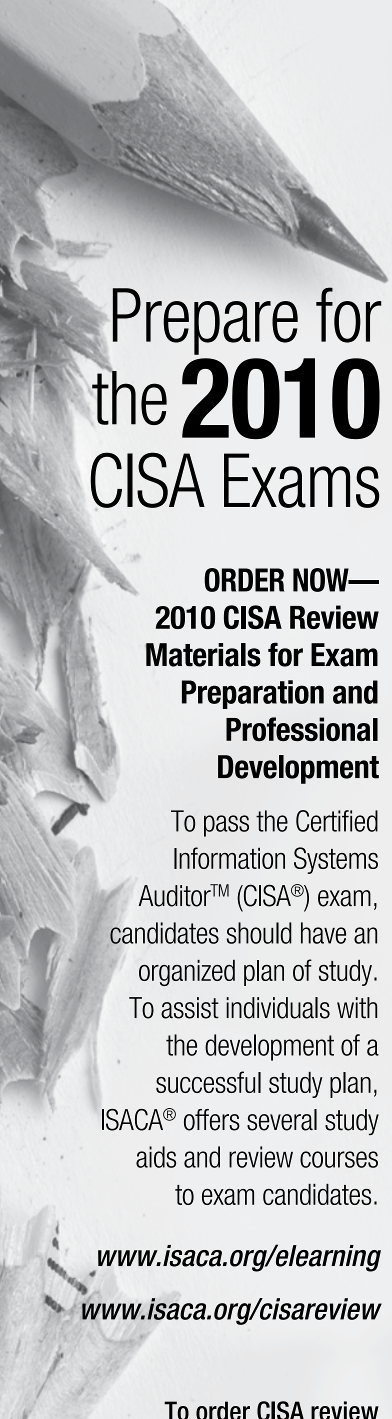
[4] US Congress, Sarbanes-Oxley Act of 2002, section 404, "Assessment of Internal Control," USA, 2002

[5] US Congress, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Title 2, "Administrative Simplification," USA, 1996

[6] US Environmental Protection Agency (EPA), "What Is Risk Assessment?," USA, *www.epa.gov/risk/basicinformation.htm#arisk*

[7] Office of Environmental Health Hazard Assessment, "A Guide to Health Risk Assessment," California Environmental Protection Agency, *http://oehha.ca.gov/pdf/HRSguide2001.pdf*

[8] Standard & Poor's, RatingsDirect® Global Credit Portal, *www.standardandpoors.com/ratingsdirect,* 7 May 2008



Prepare for the 2010 CISA Exams

ORDER NOW—2010 CISA Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Systems Auditor™ (CISA®) exam, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses to exam candidates.

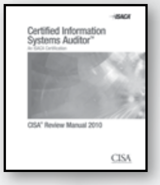
www.isaca.org/elearning

www.isaca.org/cisareview

To order CISA review material for the June/December 2010 exams, visit the ISACA web site at *www.isaca.org/cisabooks* or see pages S1-S4 in this *Journal*.

CISA Review Manual 2010

ISACA



The *CISA® Review Manual 2010* is a comprehensive reference guide designed to assist individuals in preparing for the CISA exam and individuals who wish to understand the roles and responsibilities of an information systems auditor. The manual has evolved over the past editions and now represents the most current, comprehensive, globally peer-reviewed information security management resource available.

The *CISA Review Manual 2010* features a new format. Each of the six chapters has been divided into two sections for focused study. The first section of each chapter contains the definitions and objectives for the six areas, with the corresponding tasks performed by information systems (IS) auditors and knowledge statements (required to plan, manage and perform IS audits) that are tested on the exam.

Section 1 is an overview that provides:
- Definitions for the six areas
- Objectives for each area
- Descriptions of the tasks
- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in section 2 for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section 2 consists of reference material and content that supports the knowledge statements. Material included is pertinent for CISA candidates' knowledge and/or understanding when preparing for the CISA certification exam. In addition, the *CISA Review Manual 2010* includes brief chapter summaries focused on the main topics and case studies to assist candidates in understanding current practices. Also included are definitions of terms most commonly found on the exam.

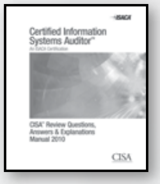
This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses.

The 2010 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:
- IS audit process
- IT governance
- Systems and infrastructure life cycle management
- IT service delivery and support
- Protection of information assets
- Business continuity and disaster recovery

CRM-10	English Edition
CRM-10F	French Edition
CRM-10I	Italian Edition
CRM-10J	Japanese Edition
CRM-10S	Spanish Edition

CISA Review Questions, Answers & Explanations Manual 2010

ISACA



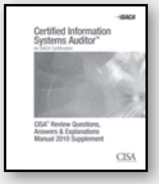
The *CISA® Review Questions, Answers & Explanations Manual 2010* consists of 800 multiple-choice study questions that have previously appeared in the *CISA® Review Questions, Answers & Explanations Manual 2008* and the 2008 and 2009 supplements. Many questions have been revised or completely rewritten to recognize a change in job practice, be more representative of the current CISA exam question format, and/or provide further clarity or explanation of the correct answer. These questions are not actual exam items, but are intended to provide CISA candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISA Review Manual 2010.*

To assist candidates in maximizing study efforts, questions are presented in the following two ways:
- Sorted by job practice area
- Scrambled as a sample 200-question exam

QAE-10	English Edition
QAE-10I	Italian Edition
QAE-10J	Japanese Edition
QAE-10S	Spanish Edition

CISA Review Questions, Answers & Explanations Manual 2010 Supplement

ISACA



Developed each year, the *CISA® Review Questions, Answers & Explanations Manual 2010 Supplement* is recommended for use when preparing for the 2010 CISA exam. This supplement consists of 100 new sample questions, answers and explanations based on the current CISA job practice areas, using a process for item development similar to the process for developing actual exam items. The questions are intended to provide CISA candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISA exam.

QAE-10ES	English Edition
QAE-10FS	French Edition
QAE-10IS	Italian Edition
QAE-10JS	Japanese Edition
QAE-10SS	Spanish Edition

CISA Practice Question Database v10

ISACA

The CISA® Practice Question Database v10 combines the *CISA Review Questions, Answers & Explanations Manual 2010* with the *CISA Review Questions, Answers & Explanations Manual 2010 Supplement* into one comprehensive 900-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions. The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:
- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

CDB-10	English Edition—CD-ROM
CDB-10W	English Edition—Download
CDB-10S	Spanish Edition—CD-ROM
CDB-10SW	Spanish Edition—Download

CISA Online Review Course

ISACA

A complete web-based exam review course is available at *www.isaca.org/elearning.*

Risk Landscape of Cloud Computing

Vasant Raval, CISA, DBA, is professor of accountancy at Creighton University, Omaha, Nebraska, USA. A coauthor of two books on information systems and security, his areas of teaching and research interests include information security and corporate governance.

Over time, as computing ease and functionality have grown, the IT industry has experienced from its users an ever-expanding desire for more information. With the web presence today, one can hardly imagine a day going by without accessing the web many times. Data are generated by the minute and are growing in variety and size; there appears to be no limit to where this appetite for more will finally face a "No, you cannot have it."

To serve this appetite, costs should decrease and/or value of information should increase. For example, early installations of client-server configurations resulted in poor server utilization (because a server was dedicated to processing a limited number of applications). The costs of servers grew as the server farms grew. To ease the pains of underutilization, virtualization[1] emerged, which made it possible for servers to attend to more than one application. Capacity utilization thus improved and cost of services came under some degree of control.

> "The wheels are in motion for a tectonic shift in the world of information systems."

Even as the idea of virtualization as applied to desktops and servers matured, the passion for virtualization lingered. If storage can be virtualized, why not applications, services, platforms and infrastructures? So the concept of sharing or abstracting through virtualization beyond just servers grew and produced a bigger picture, known as cloud computing. Conceptually, cloud computing is a network of information systems resources (hardware, software, knowledge, etc.) that provides web-centric online services. Broadly, it is a "generic infrastructural fabric"[2] leveraged on the web for providing all kinds of services in a flexible manner. In the past, power infrastructures and highway transportation infrastructures, for example, have changed society and the economy. For power, people do not need to have their own generators, they can use any amount they want at any time and for any purpose. The highway networks provide a means to go from anywhere to anywhere, using any kind of vehicle, and for any purpose. For sharing power, first a power grid was needed, and the highway network was designed by connecting various road networks so they could be shared for travel. For cloud computing, computational grids will need to be used to support huge data centers.

Although a lot needs to be accomplished before advanced use of cloud computing will occur, the wheels are in motion for a tectonic shift in the world of information systems. Call it a "disruptive technology"[3] or "the next black swan,"[4] cloud computing is here to change the entire spectrum of information systems domain. The cloud infrastructure, much like other infrastructures, will bring a sea change in business and life. According to *The Economist*, the rise of cloud computing is "more than just another platform shift. It will undoubtedly transform the IT industry, but it will also profoundly change the way people work and companies operate."[5]

Gartner predicts that the market for cloud products and services will vault from US $46.4 billion in 2008 to US $150.1 billion in 2013.[6] In light of constant pressures to reduce IT budgets, this is a welcome relief, though some of this growth may be funded by cutting existing IT outlays in other areas of information systems. Overall, it appears that a dynamic reallocation of information-systems-related outlays will occur due to potential advances in cloud computing.

GROWTH IN DEMAND FOR SOFTWARE SERVICES

While virtualization physically supported the notion of sharing and optimizing resource utilization, the logical driver of cloud computing has been software services. In recent years, Software as a Service (SaaS) has grown exponentially, thanks to the notion of sharing a centrally available computing resource. The simplest examples of SaaS include the offering of a wireless telecom company, U.S. Cellular, to store, maintain and back up contacts (for upload in the event one loses his/her device), and Amazon's Kindle services, where the company keeps track of the entire library of every Kindle buyer. The customer does not need to own, maintain or operate the software, and yet, the benefits of the software accrue to the customer. The combined effect of virtualization and SaaS can be seen in cloud computing.

Among the early cases of cloud computing are Amazon's Elastic Compute Cloud (Amazon EC2) (an infrastructure), Google's App Engine (a platform), and Microsoft's Live Mesh (an infrastructure).

Cloud Example One—Amazon's EC2

This article will focus on Amazon EC2 as one example of cloud computing.[7] Amazon EC2 allows people to set up and configure their own virtual machine on Amazon's cloud. This means everything about their instances, from their operating system to their applications. Central to this infrastructure is what is called an Amazon Machine Image (AMI), which is a packaged environment that includes all the necessary logic to set up and boot one's own virtual machine. A unit of deployment can be used to create several building-block AMIs for one's unique needs (e.g., an application server, database, a web server). Once a custom AMI is created, it needs to be uploaded to Amazon S3 (Simple Storage Service).[8] Amazon EC2 uses Amazon S3 to provide reliable, scalable storage of AMIs, so that Amazon can boot them when asked to do so. The size and complexity of a customer's virtual existence depends on the customer. Most everything is scalable, and users pay for what they use, and no more. Over time, as a user's needs increase, the user may buy more services, including storage or processing, and will be charged based on use at that time.

Cloud Example Two—Evernote

Evernote's main function is to allow users to take notes in any form, for example, by snapping pictures, recording audio, capturing web pages or typing words. They cannot lose or misplace these notes because they reside in a cloud. Every file sent to Evernote is uploaded to a server farm somewhere. From there, files are accessible via just about anything connected to the web—the user's home and office computers, laptop, and cell. Say the user is browsing for recipes and finds a good one. He/she can clip it into Evernote and view it on his/her phone while shopping for ingredients. Back at home, he/she can pull it up on his/her laptop and start making the new recipe. Aside from place and media independence, what really distinguishes Evernote is its uncanny ability to "read" text contained in images, which allows the user to, say, take a shot of a business card and send it to Evernote, which will index the information and render it searchable.[9]

LOGICAL CHARACTERISTICS OF CLOUDS

Although clouds vary in their functionalities and complexity, some commonalities among them can be traced. Technically, these are centralized data center(s) with all information resources available for users to meet their own information requirements. The example of Amazon illustrates the elastic nature of such data centers, where a vast array of different user needs can be met in a flexible manner. The following four logical characteristics are evident in cloud computing:

- **Sharing**—A predominant feature of cloud computing is that it is a high-performance machine built to address user needs at the lowest common denominator, thus allowing users to share the provider's resources. For example, for developing one's own programming applications, a multitude of subroutines is provided; the user then embeds into his/her own logic those subroutines that are needed, and thus creates a customized piece of logic without having to write monolithic code. The reusable components will be numerous and at the most basic level possible in order for users to pick and embed in their own constructs. In 2003, SAP introduced service-oriented architecture (SOA) into its software. It replaced its monolithic enterprise resource management (ERM) with a collection of reusable components that could be integrated into a whole according to the customer's need.[10]
- **Communication bandwidth**—Historically, the sharing of software systems by credit unions, for example, has been done through dial-up systems. In this case, each credit union relies on a monolithic software solution and dedicated data storage at the provider's location to conduct its operations, make queries, update data and generate reports. This hub-and-spoke approach to sharing now belongs mostly to history.[11] The new way of sharing is through the Internet in the web environment. Consequently, communication

bandwidth should be adequate and reliable. Very little will exist at the customer's end, for most everything will be in the cloud and not much will be able to be done without the pipeline.

- **Flexibility**—Historically, "sharing" implies use of resources in a relatively confined manner. For example, a customer's applications could be run by an external entity on a shared computer operated by the entity's staff. Now, sharing takes a deep dive into granularity. New ways of sharing mean anything can be ordered in any amount and to the minutest requirements. It is like going into a restaurant and choosing one's own bread, condiments, whether to toast the sandwich or not—all these decisions rest with the customer. Choice will be predominant and visible, and the results will not be like a precooked meal.[12] For example, SAP has now granularized its ERM logic components to a degree where customers can determine what to use and even, within selected components, how to modify them to fit their own needs. Ingredients are made available to users for their own recipe.
- **Scalability**—Scalability here means that users will not have to worry about getting a second server or another storage device in case their needs grow. It is all provided in a seamless manner by the cloud, regardless of whether the customer's needs increase or decrease. The elapsed time between the customer's need and supply of resources to meet the need will be insignificant. Equally important, the customer will not have to worry about selecting specifications, acquiring and installing resources, testing them for reliability, etc. It is all in one place without the customer having to worry about time lags, functionality and interoperability.

> "Characteristics of cloud computing lead to enormous opportunities as well as risks."

RISK LANDSCAPE

The characteristics of cloud computing lead to enormous opportunities as well as risks. Some of the risks already exist, but will be elevated, and others are new. Taking stock of these risks is as important as knowing how to leverage this development for one's company.

Because it is too early to know the exact configuration of a cloud, it is difficult to predict precisely what risks would be present at the forefront of this development. Depending on whether the cloud provides SaaS, Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), the risk scenario could be different for each case. Also, a great deal depends on whether the cloud services are provided by an internal cloud (having a cloud environment within the organization) or an external cloud (outsourcing to a vendor's cloud environment), with the latter likely posing greater risks. However, it is not too early for IT auditors to begin to monitor cloud developments to grasp in a timely manner the changing risks. The discussion of broad areas of risks in cloud computing is divided into six categories:

- **Authentication**—The single most critical concern in the use of web-based services is the authentication of users. While technology for authentication has improved over time, there still are grave concerns about untrusted parties posing as authentic users and, if successful, causing data compromises. If most everything in terms of information resources resides in the cloud, this will be a significant risk to be addressed. Presumably, internal clouds may face lower risks of authentication than external clouds simply because of the differences in the customer universe.
- **Data security and privacy**—Control over data on the web-managed vendors has been a matter of concern over the years. Even though the outsourcing option has gained popularity, customer organizations not only watch over the data protection standards their vendors use, but also mandate certain requirements of their own, and even perform their own audit. Despite this, the residual risks of losing data on the web remain high, and the customer organization could run into a crisis unless an in-depth security strategy is implemented for the cloud environment.
- **Interfacing with internal systems**—Most firms may not be able to outsource everything to an external cloud (e.g., systems that address strategic initiatives, have intellectual property that comprise the core of its competitive strength or are so diverse that there are no viable options in the external cloud). If these residual systems and applications are diverse in nature, it will be a significant challenge to build interfaces for them. And even when such interfaces are in place, risks of data consistency and interoperability are likely to remain. Moreover, anything in-house, if connected to an external cloud, is subject to additional exposures from outside.

- **System availability**—Businesses have moved from simple data crunching to integrated systems that are productive, seamless and strategic. Because they are lifelines for businesses, availability of such systems needs to be almost guaranteed. This means additional processes, data backups and redundancy; controls testing for availability requirements; and recovery strategies in the event of data loss. Not only will all this cost more, but it has to be reliable. Perhaps cloud vendors will be at an advantage in building a shared utility that provides for data availability for customers. Nevertheless, users' concern for loss of control will continue to surface as more is handed over to the clouds.

> "Users' concern for loss of control will continue to surface as more is handed over to the clouds."

- **Business continuity**—Business continuity in the cloud environment depends on the cloud vendor. Consequently, if using an external cloud, one must be prepared to ask the question: "What if the vendor does not exist tomorrow?" Thus, the financial and operational viability of the vendor is at the center of the risk landscape. Add to this the facts that cybercrime is on the rise and there is a possibility that the clouds being used are somewhere around the globe in a risky region. Such risks are heightened because when most of the user's resources reside in the cloud, he/she is almost totally dependent on the cloud.
- **Ownership of content and other legal requirements**—When all systems' resources, including data and related applications, are outsourced into a cloud, serious questions emerge. For example, who owns these data? Can one get these data back if the vendor ceases to exist? What will be the legal jurisdiction in the event of disputes and disagreements? Whose property will the applications be if the applications are made through a unique assembly of granular subroutines of a software vendor? Who is responsible for data breaches? Legal complications could become a serious drag on a business and could potentially result in disruption in business continuity.

CONTROL ENVIRONMENT

There is little, if any, likelihood that physical and virtual worlds will exactly coincide. Not all locations of an organization are necessarily included in the virtual entity, but the virtual organization may extend beyond its physical perimeters into business partners, customers, service providers and the like.[13] Thus, the articulation of a control environment must include significant and careful consideration of the virtual worlds—in this case, the clouds.

Because clouds are "shared" by many customers using the electronic highway, it is crucial that IT auditors and control experts pay attention to not just protection and security within the perimeter, but also on the highway. It is important to have seat belts, rearview mirrors and air bags in a car, but it is critical to also have highway controls, such as stop signs, traffic lights, guard rails and traffic cops.[14] Similarly, air traffic control systems and safety requirements protect travelers from mid-air collision and other disasters. The cloud computing environment should include a careful and thorough consideration of controls over communication with the outside world.

Whereas outsourcing has until now been a matter of choice, the presence of clouds will elevate outsourcing as a matter of need. Therefore, the articulation of the cloud control environment must include all pertinent sources of risks of outsourcing of IT services. This focus on outsourcing may be limited in the case of internal clouds; however, the scenario is similar in that an internal cloud is also an outsourcing service for internal customers. Consequently, concerns about using internal cloud services are likely to be similar, if not heightened to the same level, as those in using external clouds.

> "The presence of clouds will elevate outsourcing as a matter of need."

CONCLUSION

It is too early to say what specific risks will emerge with the implementation of cloud computing. However, it certainly is time to begin mapping such risks to learn about the related risks and planning to mitigate them proactively.

Strategic, tactical and operational aspects of sourcing decisions should be carefully and comprehensively identified and addressed. Potential risks with outsourcing information systems lies in the facts that the customer is dependent on the third-party outsourcing firm and there are likely to be significant exit barriers.[15] Project planning and management risks, contracting and negotiation risks, transition and start-up

risks, and provider performance risks must be addressed.[16] Finally, the process of gaining assurance of services and related controls should be documented and appropriate aspects of it should be included in the outsourcing contract.

Requisite variety in the service level agreement (SLA) is the key to managing risks of external clouds. In other words, for every foreseeable out-of-control situation, an appropriate control response should be identified. Every aspect of risk must be considered, and its possible effect should be determined. Risk scenarios should be built and discussed with the prospective vendors to learn how well the information resources are secured. A similar exercise for an internal cloud can be used to develop an internal SLA for cloud services to gain assurance of risk mitigation.

ENDNOTES

[1] Virtualization is an approach to separating (abstracting) systems' resources in terms of physical and logical dimensions. Thus, the same physical resource could serve more than one logical need. Such a separation could occur at any level, e.g., desktop, network, application, platform, infrastructure.

[2] Delic, K.A.; "Emergence of Academic Computing Clouds," *ACM Ubiquity*, vol. 9 (31), 2008

[3] Christensen, C. M.; *The Innovator's Dilemma*, Harper Collins, USA, 2003. He distinguished between established technologies that allow an entity to grow in a linear mode (sustaining technologies) from those that start out as simple, cheap and even inferior, but grow over time into innovative and new uses that generate exceptional economic value.

[4] Taleb, N.N.; *The Black Swan: The Impact of the Highly Improbable*, Random House, USA, 2007. Taleb describes events—the black swans—that defy historical pattern and are unpredictable in timing and impact.

[5] "Let It Rise," *The Economist*, vol. 389 (8603), Special Section, 25 October 2008, p. 3-4

[6] Hamm, S.; "Cloud Computing's Big Bang for Business," *BusinessWeek*, 15 June 2009, p. 42-44

[7] Amazon Web Services, Amazon Elastic Compute Cloud (Amazon EC2), *www.amazon.com/ec2*

[8] Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites.

[9] Samiljan, Tom; "You Must Remember This," *Hemisphere Magazine*, August 2009

[10] "Creating the Cumulus," *The Economist*, vol. 389 (8603), Special Section, 25 October 2008, p. 8-10

[11] Hayes, B.; "Cloud Computing," *Communications of the ACM*, vol. 51 (7), July 2008, p. 9-11

[12] *Op cit.*, "Creating the Cumulus," *The Economist*

[13] Axelrod, C. Warren; "Cyber Security and the Critical Infrastructure," *Information Systems Control Journal*, vol. 3, 2006, p. 24-28

[14] *Ibid.*

[15] Wright, Catherine; "Top Three Potential Risks With Outsourcing Information Systems," *Information Systems Control Journal*, vol. 5, 2004, p. 41

[16] Benvenuto, N.A.; David Brand; "Outsourcing—A Risk Management Perspective," *Information Systems Control Journal*, vol. 5, 2005, p. 35-40

EDITOR'S NOTE

ISACA recently released a white paper, "Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives." The complimentary white paper is available for download at *www.isaca.org/cloud.*

The best stories have a happy ending...

Chapter I - Data Warehouse Software

Once upon a time... Our audit data was stored in different documents that didn't talk to each other.

But now... Audit Leverage gives us a single data warehouse to enter, store, analyze, and retrieve all of our risk assessments, audits, time charges, budgets, workpapers, findings, and follow-up entries.

Chapter II - Workpapers & Audit Programs

Once upon a time... We used to print out all our workpapers and sign off on them manually.

But now... Audit Leverage maintains electronic links between audit steps, workpapers, audit recommendations, and review notes. Audit managers can sign off electronically.

Chapter III - Timesheets & Budgets

Once upon a time... We used to fill out timesheets in Excel, then print or e-mail them for approval.

But now... We enter each day's hours directly into Audit Leverage, where our supervisor can approve it electronically and analyze it by audit, by auditor, by time period, and more. Budget-to-actual comparisons tell us where our time is really going.

Chapter IV - Staffing & Scheduling

Once upon a time... Schedule changes caused confusion.

But now... Audit Leverage's Visual Scheduler™ allows us to manage each auditor's calendar and to deal with schedule changes in real-time.

Chapter V - Risk Assessment & Annual Planning

Once upon a time... One year's risk assessment results weren't linked with previous years'.

But now... Audit Leverage lets us use our own risk criteria and recommends an audit plan based on prior years' activity. During the year, it shows us actual progress against our plan.

Chapter VI - Audit Committee Reporting

Once upon a time... We used to waste dozens of hours preparing for an Audit Committee meeting.

But now... We use Audit Leverage to generate those labor-intensive reports that the Audit Committee wants to see.

Chapter VII - Remote Audit Supervision

Once upon a time... My manager had to wait until I returned to the office to review workpapers and time charges.

But now... Audit Leverage's remote synchronization feature allows our audit manager to make mid-course corrections to the fieldwork - before it's too late.

Chapter VIII - Audit Follow-up

Once upon a time... After issuing our audit report, we pasted the findings into a separate follow-up spreadsheet.

But now... When we type our audit findings and management responses into Audit Leverage, it generates the audit report for us - and also tracks our follow-up efforts for each issue.

Chapter IX - Issue Analysis

Once upon a time... Identifying the the most common audit issues meant days of sifting through audit reports.

But now... Audit Leverage's powerful reports provide statistics on the most common audit recommendations by topic, division, region, and more. We can maintain our own library of best practices.

Audit™ Leverage
by IAD Solutions

Work happily ever after.

Write your own happy ending. Contact us.
E-mail: info@AuditLeverage.com
Phone: 1-866 AL by IAD (Toll Free) or 215-713-0378
Visit us on the Web at www.AuditLeverage.com

Criteria and Methodology for GRC Platform Selection

Anand Singh, CISM, CISSP, is a senior consultant with extensive background in information security and compliance, as a practitioner and a researcher. He specializes in IT risk management and its use as a decision-support system to determine the economics of security investment. He is a highly sought-after speaker on information security issues. He can be reached at *anand.singh@gmail.com.*

David J. Lilja, Ph.D., is the Louis John Schnell Professor and head of electrical and computer engineering at the University of Minnesota in Minneapolis (USA). He also serves as a member of the graduate faculties in computer science and scientific computation, and is a fellow of the Minnesota Supercomputing Institute. His research interests include security, computer architecture and performance analysis. He has been elected a fellow of the Institute of Electrical and Electronics Engineers (IEEE) and a fellow of the American Association for the Advancement of Science (AAAS). He is the author of the book *Measuring Computer Performance: A Practitioner's Guide.*

More than a decade ago, the acclaimed management philosopher Peter Drucker stated, "the diffusion of technology and commodification of information transforms the role of information into a resource equal in importance to land, labor and capital."[1] The exponential growth of information after the Internet boom of the 1990s shows the accuracy of his foresight. In today's world, the fortunes of most organizations are tied to the information they possess and the sophistication with which they are able to manage it. As a consequence, governance, risk management and compliance (GRC) issues around information have become central to organizational strategies. Investment in these areas has been increasing steadily, topping US $32 billion in 2008, a growth of 7.4 percent over 2007.[2]

GRC platforms provide a single, federated framework that integrates organizational processes and tools, supporting those processes for the purpose of defining, maintaining and monitoring GRC. An appropriately chosen GRC platform can lead to reduced complexities and increased efficiencies. Selecting a GRC platform is a complex endeavor, though, and requires extensive collaboration among business, IT, compliance and audit. It requires a substantial investment of time and effort in addition to the capital investment required for purchasing and maintaining the platform. Making the task of selecting a platform even more complex is the fact that this space is populated with a large number of competing products—AXENTIS, MetricStream, OpenPages, Paisley, Modulo and Archer, to name a few. Thus, it is imperative that the platform selection is done intelligently, to ensure positive return on investment (ROI).

The following sections provide comprehensive criteria that can be used to evaluate and select a GRC platform for an enterprise. These criteria have been determined through interviews with experts in different industry segments, examination of industry best practices, the experiences in evaluating GRC platforms for multiple enterprises and the use of requirements engineering techniques. They can be used as building blocks to which the unique requirements of the organization can be added to arrive at a complete set of requirements that need to be considered. While they are being defined here for GRC platforms in totality, they can easily be adapted for tool sets addressing individual areas of governance, risk or compliance. The criteria are structured in three major sections: general considerations, functional requirements and nonfunctional requirements. How to use the criteria to arrive at a decision is described further through a scoring model and a case study.

GENERAL CONSIDERATIONS

The criteria are general in nature and applicable to all enterprises, irrespective of regulations applicable to them, their size or the business sector in which they operate. These are must-haves and, hence, are generally used for exclusionary purposes, i.e., to narrow the field of proposals that would be considered. **Figure 1** summarizes the parameters and artifacts that can be used to evaluate vendors against the criteria:

- **Cost**—GRC solutions can vary significantly in cost. While considering cost, it is important to consider the total cost of ownership (TCO). Some important TCO components are hardware, implementation and consulting fees, training, customization, maintenance, security, and operational costs. Also, this is a useful metric to have for ROI calculations.
- **Vendor reputation**—With the growing popularity and demand of GRC platforms, a significant number of vendors have jumped into this space. In addition to there being a surfeit of genuine vendors, the picture is further clouded by some vendors that market GRC solutions that are thinly disguised versions of their existing product suite targeting a different space. As competition heats up and market forces weed out weaker players, only the

stronger players will survive. Hence, it is important not to get stuck with a solution that might become unsupported in the future, either because the vendor has ceased to exist or because it has exited this space. This can be accomplished through a thorough appraisal of the vendor's installed base, references and financial viability.

- **Product scope, strategy and vision**—Threats and vulnerabilities are ever changing. The recent financial meltdown is leading to a change in regulatory landscape. All of this is a stark reminder that GRC is an ongoing process that might require an expansion of scope. Another driver for this is the fact that many countries are still working toward maturing their regulations and compliance regimes—J-SOX[3] being one such example. Finally, as organizations enter new market segments, they have to adapt to GRC requirements in that space. All of these factors mean that it is important to examine the product scope, strategy and vision to make sure that the vendor has a long-term view of its product offering and has mechanisms to adapt and expand as the landscape changes. Product road map and research and development (R&D) strength (measured in terms of R&D head count and investment) are some examples of how to further this examination.

Figure 1—Evaluating General Considerations

General Considerations	Example Evaluation Parameters and Artifacts
Cost	Software, hardware, licensing, training, customization, consulting, maintenance, security and operations
Vendor reputation	References, installed base and financial viability (market capitalization, financial results, annual reports)
Product strategy and vision	Product road map, R&D head count and R&D budget

FUNCTIONAL REQUIREMENTS

Functional requirements are used to define the behavior of the target software, including features and capabilities that determine what a system is supposed to accomplish. The following sections define high-level requirements for each of the three principal components—governance, risk management and compliance—as well as for other general functionality:

- **Governance**—The IT Governance Institute (ITGI) defines governance as "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that the objectives are achieved, ascertaining that the risks are managed appropriately and verifying that the enterprise's resources are being used responsibly."[4] In light of this definition, it is clear that the governance component of the GRC platform must be evaluated for the requirements presented in **figure 2**.

Figure 2—Governance Requirements

Requirement	Explanation
Business alignment	Facilitate alignment of governance with organization's business objectives
Policy, standard and procedure management	Policies are the medium through which management communicates its direction and intent. Standards and procedures are the vehicles used to implement policies across the organization. Therefore, the GRC platform must support the development, maintenance and communication of these.
Oversight	Enable executive management oversight through appropriate reporting mechanisms such as a security and/or compliance dashboard
Decision support	Provide cost/benefit and other data to the executive management for decision-making purposes (e.g., risk data can be used to determine the economics as well as justify the security investment)

- **Risk management**—Risk management is activity directed toward assessing, mitigating (to an acceptable level) and monitoring risk. The principle goal of an organization's risk management process should be to protect the organization and its ability to perform its mission, not just its IT assets.[5] **Figure 3** presents the high-level requirements for risk management.
- **Compliance**—Compliance is an increasingly complex task given the global footprints of organizations, the increase in regulatory environment (which is likely to become even more stringent given the opportunities exposed by the current economic crises) and local regulations. **Figure 4** presents the requirements to ensure that these needs are supported by the GRC platform.

Figure 3—Risk Management Requiremetns

Requirement	Explanation
Risk baseline	It should facilitate development of the risk baseline based on an organization's risk appetite.
End-to-end risk management	Risk management is a continual process. It should begin at the conception stage, be considered throughout the software development life cycle (SDLC) and end only when the system is retired. The GRC platform must support this ongoing management of risk.
Adaptability	Since an organization's risk profile, threats and vulnerabilities change frequently, it is important for risk management to be adaptive to these changes.
Consistency	It must provide consistency, i.e., different areas of the same organization should manage their risks in a consistent fashion. This makes the task of risk consolidation simpler and more manageable.
Metrics	It must facilitate collection of metrics about incidents, vulnerabilities and threats. These data in turn can be used for monitoring losses and assigning cost-effective controls to remediate or mitigate future losses.

Figure 4—Compliance Requirements

Requirement	Explanation
Regulatory intelligence	Report on global events, regulatory changes and linkage with legal databases such as WestLaw and LexisNexis
Requirements and controls library	Ensure authoritative libraries of all applicable compliance-driven requirements and associated controls
Correlation	Provide ability to correlate similar requirements across different compliance regulations for efficiency purposes
Remediation management	Facilitate the ability to track identified remediation measures and their progress
Reporting	Deliver the ability to generate reports, including *ad hoc* reports, needed for audits

- **Vendor oversight**—Regulators are increasingly focused on personally identifiable information (PII) and how organizations manage such data among vendors that have access to the data. For example, healthcare providers to most organizations have access to PII. They require organizational due diligence to ensure that their vendors have mature information security practices to protect their data. GRC platforms should facilitate this effort. Support for shared assessments, the industry standard for determining the maturity of information security practices at a vendor, is one way a GRC platform can demonstrate its strength.
- **Workflow**—A good workflow engine is essential to the success of a GRC platform. Given the large number of areas and users involved in the GRC platform, there is a need to manage and distribute work and monitor its progress through all of these steps.
- **Document management**—GRC platforms are used for organization and management of an extensive body of documentation. In addition to policies, standards and procedures, they are used for housing organizational controls, tests conducted to verify the robustness of these controls and custom attributes. Therefore, strong document management features are essential to success.

NONFUNCTIONAL REQUIREMENTS

Nonfunctional requirements are used to define the operation of the system or the environment in which the software should run. Since the spectrum of nonfunctional requirements is very large, the field has been narrowed to the requirements that are most applicable to the selection of a GRC platform:

- **Security**—GRC platforms house critical information about the security posture of the enterprise, including information about vulnerabilities, risks and data as well as their classification. The consequences of a security breach are great and include exploitation of vulnerabilities, damage to credibility, financial loss and legal liability. As such, strong security measures should be provided in the platform to enforce not only protection from external breaches (e.g., through encryption), but also from insider misuse of information by allowing enforcement of the two fundamental principles of security: least privilege (i.e., individuals should have just enough permissions and rights to fulfill their roles) and need to know (i.e., individuals should have access to specific information only if it is essential for them to carry out their roles).
- **Scalability**—The amount and the complexity of information resources within organizations are increasing at an exponential rate. In addition, it might be necessary for organizations to scale their GRC platform for new risks and compliance regimens. This could be necessitated by their foray into new market segments, expansion of their global footprints making them subject to local regulations, or new regulations coming into existence. Determining scalability requirements

appropriately upfront provides flexibility for future growth. Because scalability is based on future needs, it requires a certain amount of prediction and estimation to plan for it. An examination of the strategic business plan of the organization for the next few years might provide this insight.

- **Interface**—To achieve maximum efficiency from the GRC platform, it is important that it provide interfaces for integration with enterprise applications used to drive business processes (e.g., integration with an identity management system or configuration management database [CMDB]). This will help automate data collection, controls and processes and, hence, simplify analysis, reporting and remediation.
- **Usability**—Usability requirements specify the ease of use of a system. Given that a GRC platform would be used by a broad spectrum of users including business, IT, audit and compliance, it is important that their input is sought in evaluating the usability of any platform under consideration. The five parameters that should be considered for this purpose are ease of learning (evaluated through training and documentation provided), task efficiency (efficiency of the system for frequent users), ease of remembering, understandability and subjective satisfaction.[6]

Figure 5—Requirements Solicitation Questions

1.	What is your biggest GRC area of concern?
2.	What compliance regulations are applicable to your area?
3.	Have you failed any areas of compliance audits in the past? If so, what were the findings?
4.	What improvements would you like to see in your current mechanism for prioritizing the security budget?
5.	How do you rate the effectiveness of your security controls?
6.	What would you like to see in the reports indicating the current status of compliance?
7.	How do you evaluate your risk currently? What are possible areas of improvement?
8.	What are critical threats to your area?
9.	How many times have you experienced these threats in the past 12 months?
10.	What area are you more concerned about, insider abuse or external threat? Please provide specifics.
11.	Have any of your end users expressed dissatisfaction with the extra steps they have to go through because of the security controls?
12.	Do you have a good data classification mechanism?

- **Support**—Supportability deals with the ease of customization to meet the unique needs of the organization, incorporation of new features or enhancements, and bug fixes. A good example of a supportability requirement is, in the case of an organization that has to adhere to Payment Card Industry (PCI) standards, the GRC platform vendor should provide updates when the new versions of PCI get released. Maintenance, updates, consulting services and customization are some areas to consider when evaluating vendors against this dimension.

EXAMPLE SELECTION PROCESS WALK-THROUGH

The criteria presented previously can be combined with a weighting mechanism to arrive at a decision on which GRC tool to select. An example case study is presented here.

A medium-sized retail organization is looking to strengthen the governance and risk management of its information. It has been classified as a tier-2 vendor for PCI. In addition, it offers pharmacy services in its stores and, hence, has to be compliant with the US Health Insurance Portability and Accountability Act (HIPAA). It has budgeted TCO of US $750,000 for a GRC solution to manage these efforts for a five-year period. It is not looking to include US Sarbanes-Oxley Act compliance in the ambit of this GRC tool because it intends to continue leveraging its existing point solution for that. The following is a step-by-step description of how the organization arrived at a decision using the criteria defined previously (**figure 7** shows the results of these steps):

1. It created a request for proposal (RFP) defining the GRC needs of the organization and invited vendor responses. Based on exclusionary criteria, it narrowed the vendor choices to A, B and C.
2. It partitioned its stakeholders into primary (those who are directly impacted by the platform choice) and secondary (those who are intermediaries in the selection process) stakeholders. Its primary stakeholders were office of the

Figure 6—Criteria Weight Determination

Stakeholder Interest	Score
1-2 secondary stakeholders	1
3 secondary stakeholders or more	2
At least one primary stakeholder	3
More than 2 (but not all) primary stakeholders	4
All primary stakeholders	5

Figure 7—Decision Table

Requirements	Weight (W)	Explanation/Comments	Vendor A		Vendor B		Vendor C	
			Rating R(A)	R(A)*W	Rating R(B)	R(B)*W	Rating R(C)	R(C)*W
Governance								
Business alignment	5		4.1	20.5	4.7	23.5	2.8	14.0
Policy, standard and procedure management	5		4.7	23.5	3.5	17.5	3.5	17.5
Oversight	4		3.4	13.6	3.7	14.8	4.4	17.6
Decision support	3	Intention to rely on existing tool set as much as possible	4.1	12.3	3.3	9.9	4.4	13.2
Risk Management								
Acceptable risk baseline	4		4.7	18.8	4.8	19.2	3.3	13.2
End-to-end risk management	3	Mostly off-the-shelf software means that managing risk across SDLC is not critical.	4.5	13.5	2.1	6.3	4.7	14.1
Adaptability	4		2.1	8.4	3.1	12.4	2.3	9.2
Consistency	5		1.8	9.0	4.3	21.5	2.1	10.5
Metrics	5		4.2	21.0	3.0	15.0	2.9	14.5
Compliance								
Regulatory intelligence	4		3.3	13.2	4.4	17.6	4.3	17.2
Requirements and controls library	5		4.1	20.5	4.0	20.0	3.8	19.0
Correlation	3	Since HIPAA and PCI are mostly nonoverlapping, being able to correlate across the two is not critical.	3.1	9.3	2.1	8.3	1.9	5.7
Remediation management	4		4.3	17.2	3.9	15.6	2.8	11.2
Reporting	5		4.3	21.5	4.2	21.0	3.3	16.5
Vendor oversight	2		2.3	4.6	1.5	3.0	3.5	7.0
Workflow	5		3.9	19.5	5.0	25.0	0.9	4.5
Document management	5		4.5	22.5	4.1	20.5	4.5	22.5
Security	5		5.0	25.0	5.0	25.0	4.5	22.5
Scalability	2	Does not anticipate a change in its regulatory environment	3.8	7.6	5.0	10.0	4.9	9.8
Interface	4		2.2	8.8	4.1	16.4	3.8	15.2
Usability	5		4.5	22.5	4.3	21.5	4.2	21.0
Support	5		4.1	20.5	1.9	9.5	3.0	15.0
Other Requirements								
Import existing HIPAA controls	5		4.0	20.0	2.7	13.5	1.3	6.5
Automatic evidence collection	5		4.0	20.0	4.0	20.0	2.9	14.5
Project management	4		3.9	15.6	4.2	16.8	3.3	13.2
Exceptions management	4		1.3	5.0	3.7	14.8	3.6	14.4
Fit in existing infrastructure	3	Hardware is a small part of the overall allocated budget.	3.4	10.1	1.9	5.7	1.2	3.6
Support for ISO Guide 73	3	Risk calculation method used in some departments	1.5	4.5	5.0	15.0	4.2	12.6
Background check of vendor consultants	1	Most vendors would comply if selected.	4.0	4.0	3.3	3.3	4.8	4.8
Segregation of duties	4	Not a strength of the organization currently	4.1	16.4	3.2	12.8	4.4	17.6
Total				**448.85**		**455.4**		**398.1**

Legend:
➧ Functional requirement
➧ Nonfunctional requirements
➧ Unique organizational requirements

CISO, IT, internal audit and pharmacy process owners. Its secondary stakeholders were vendor management, the business continuity planning (BCP) team and finance.

3. It identified its other requirements, primarily using the requirements solicitation questions, shown in **figure 5** (also included in **figure 7** under "Other Requirements").
4. It weighted all criteria on a scale of 1 to 5 (see **figure 6**). (Note that since this article focused on identifying essential requirements in the previous sections, most of those would be weighted 3 or more; when unique organizational requirements are added, the spread from 1 to 5 would likely be observed). **Figure 7** reflects the weights along with explanations where the choice of a weight is not obvious.
5. It created a committee drawn from primary and secondary stakeholder teams. For vendors still under consideration, this committee rated them against each requirement on a scale of 0 to 5, using consensus method (some stakeholders chose to recuse themselves on occasions, as they were not knowledgeable about the requirement under consideration). A vendor should be disqualified if it has a score of 0 on any criteria rated 3 or above (i.e., any criteria of significant interest to the primary stakeholders). The following were used as raw data to arrive at a decision:
   – Vendor demonstrations
   – White papers, spec sheets and other documentation
   – Data from research organizations such as Gartner, Forrester and Burton Group
6. It computed a total weighted score for each vendor. Since the scores of vendor A and vendor B are close to each other, it had those vendors bid against each other to reduce costs and ended up choosing vendor B as a result.

CONCLUSION

Businesses are increasingly relying on GRC platforms to achieve synergies across governance, risk and compliance. In the crowded landscape of GRC platforms, arriving at the right choice for an enterprise is a complex decision. It is imperative that all applicable criteria are considered to ensure positive return on investment (ROI). It is also necessary to make the evaluation process as objective as possible.

The proposed approach helps facilitate business and IT in understanding the essential criteria to consider when evaluating GRC platforms. In addition, it illustrates how these criteria can be rolled into a scoring model to arrive at an objective decision. This ROI-driven approach will improve an organization's ability to select the right GRC platform that fits its need and, in turn, will help it manage the complexities associated with GRC efficiently.

ENDNOTES

[1] Drucker, P.; *Management Challenges of 21st Century*, Harpers Business, 1993

[2] Hagerty, John, *et al.*; "The Governance, Risk Management and Compliance Spending Report, 2008-2009: Inside the $32B GRC Market," *www.amrresearch.com*

[3] Uehara, K., *et al*.; "J-SOX Challenge: Efforts to Comply With the New Japanese Regulation," *Information Systems Control Journal,* vol. 5, 2008, p. 34-37

[4] IT Governance Institute, *Board Briefing on IT Governance, 2nd Edition*, 2003

[5] Stoneburner, Gary; Alice Goguen; Alexis Feringa; *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, National Institute of Standards and Technology (NIST), 2001

[6] Lauesen, Soren; Houman Younessi; "Six Styles of Usability Requirements," Proceedings of REFSQ'98, Presses Universitaires de Namur, 1998

AUTHORS' NOTE

The authors would like to thank Greg Handrick, R&D manager at Boston Scientific, and Kim Pender, security compliance manager at Target Corp., for reviewing the article and providing valuable feedback and suggestions.

Availability Risk Assessment— A Quantitative Approach

Hariharan, CISA, is head of IT infrastructure and security for a leading media company in India. He has more than 18 years of experience in setting up IT departments and introducing IT governance practices within the organization. He has worked in diverse environments covering remote sensing, geographic information systems, automobile manufacturing, heavy engineering and media. He is a guest lecturer to management institutes and a member of curriculum review committees of academic institutions.

Increased corporate governance requirements are causing enterprises to examine their internal control structures closely to ensure that controls are in place and operating effectively.[1] Enterprises are becoming sensitized toward business risks and are actively engaging IS auditors and IT governance professionals to fulfill the governance, risk and compliance requirements. Enterprise risk management (ERM) frameworks in general and ISACA's Risk IT: Based on CobiT® framework in particular are valuable contributions that are assisting practicing auditors and IT governance professionals in delivering standards-based audit programs and providing assurance on internal controls.

IS auditors and governance professionals are required to assess availability risk as part of the audit and review process, because system availability is an important parameter found in most ERM frameworks and IS security standards. The Risk IT framework considers "availability" risk as part of IT service delivery-related risks,[2] and ISO 27001 considers it as part of overall security risk, where security risk consists of "confidentiality," "integrity" and "availability"(CIA) risk.[3]

> "Availability percentage of a system or service is a good measure to quantify availability risk."

Currently, an availability risk assessment is done by conducting failure mode and effects analysis (FMEA)[4] on the inventoried information assets. The FMEA exercise provides a risk value and risk priority number (RPN) for every item listed in the inventory. Risk is a function of likelihood and impact where "likelihood" is the frequency or probability of occurrence of the incidence and "impact" is the effect on business. By assigning a cardinal value for "likelihood" and "impact," the risk value is determined using the equation: risk value = likelihood × impact. For example, if the likelihood that a system will be unavailable is scored at 3 in a scale of 0-6, and the corresponding impact is scored at 2 in a scale of 0-5, then the risk is valued as 6, which may be interpreted as medium risk. The risk value (i.e., 6 in this case) on its own does not mean anything. It only helps to relatively rank the availability risk of inventoried systems and services. As the scores for likelihood and impact are assigned intuitively, the risk value of the same asset is likely to vary across audits if the scores are assigned by different persons. A high-level survey of literature shows that system availability has attracted marginal attention by researchers.[5] The proposed methodology is an attempt to bridge this gap by providing a quantitative approach for performing an availability risk assessment.

It can be argued empirically that the availability percentage of a system or service is a good measure to quantify availability risk. For example, if a system or service is rated for 99.5 percent availability, the risk is clearly reflected. The value can be used to calculate and commit uptime. The information systems (IS) auditor can audit the current availability percentage against the committed percentage and report accordingly.

The availability of a service depends on how often the service fails and how much time it takes to restore the service. The frequency of failure reflects the quality of the system, which is an offshoot of the system's architectural capability, and the restoration time is dependent on the support capability. Mean time between failure (MTBF) measures average failure rate, and mean time to repair (MTTR) measures average restoration time. Using MTBF and MTTR, the availability percentage can be calculated as follows: MTBF / (MTBF + MTTR) × 100.[6]

This article puts forth a method for deriving MTBF and MTTR by assessing the system and support architectural capabilities, and then using this to calculate availability percentage.

Based on the principles established previously, the following structured approach is suggested for performing the risk assessment of IT systems using a quantitative method:

1. Create a service catalog.
2. Assess the system and service support capabilities.
3. Calculate availability percentage.

CREATE A SERVICE CATALOG

The business views IT as a service provider. Taking a service-oriented approach to risk assessment[7] enables the business process owner to relate the IT systems directly with the business area for which they are operating. This approach helps provide a business view of risk rather than a technology view. The proposed methodology uses a service catalog instead of an information asset inventory (**figure 1**), which is the traditional approach followed in an IT risk assessment exercise. The service catalog is prepared by listing the services offered to the users from various IT systems. For example, the e-mail system might offer e-mail access using an Outlook client, web client or BlackBerry. Similarly, all the IT systems are scrutinized to create a comprehensive service catalog.

Figure 1—Service Catalog vs. Information Asset Inventory

Service Catalog
E-mail access via Outlook
BlackBerry service
Video conferencing
Internet browsing
Corporate intranet
Outlook web access
Customer subscription

SI No.	Information Asset	Asset Category	Asset Subcategory
1	Hardware	Server	ERPAppsSvr-1
2	Hardware	Server	ERPAppsSvr-2
3	Hardware	Server	ERPDBCLus-1
4	Hardware	Server	ERPDBCLus-2
5	Hardware	Storage	SANStore
6	Hardware	Server	ERPWebSvr

ASSESS THE SYSTEM AND SERVICE SUPPORT CAPABILITIES

IT systems are essentially an outcome of the software engineering process. Research in the field of software engineering has established that software architecture has a decisive role in meeting various quality attributes, e.g., system availability. Research also prescribes the use of software architecture in evaluating quality attributes,[8] such as availability, performance and modifiability.

The architectural approach to risk assessment provides a platform for deriving risk indicators for both existing and new systems. The Capability Maturity Model (CMM) developed by the Software Engineering Institute (SEI) of Carnegie Mellon University[9] can be used as a reference to evaluate the system and support capability of a service by assessing their architectural maturity. The maturity level shown in **figure 2** is proposed to be used in this methodology.

Figure 2—Maturity Model for System and Support Architecture

Maturity Level	Meaning for System Architecture
1	*Ad hoc* (single system)
2	Repeatable (standby can be arranged)
3	Defined (standby part of landscape)
4	Managed (high availability environment)
5	Optimized (could not be defined)
Maturity Level	**Meaning for Support Architecture**
1	*Ad hoc* (firefighting)
2	Repeatable (skill set available)
3	Defined (process/escalation available)
4	Managed (SLA-based)
5	Optimized (proactive improvement)

Using the maturity levels shown in **figure 2**, the identified service catalog items are evaluated. This is done by understanding the system landscape and support services available for respective services. Say, for example, in an audit of an e-mail system, it is found that the BlackBerry service is running on a single system architecture, the administrator demonstrates that in case of server failure a standby server can be made available to install the BlackBerry application and, further, the auditor is convinced that the administrator

has skills to restore the application. In such a scenario, the BlackBerry service can be presumed to be at level 2 (standby can be arranged) in system architecture maturity and level 2 (skill set available) in support architecture maturity. A similar exercise of the entire service catalog results in output as shown in **figure 3**.

Figure 3—Service Maturity as per System and Support Architectural CMM

Service Catalog	System Maturity Level	Support Maturity Level
E-mail access via Outlook	3	4
BlackBerry service	2	2
Video conferencing	1	1
Internet browsing	2	3
Corporate intranet	2	3
Outlook web access	2	3
Customer subscription	3	3
Payroll and PF trust accounting	3	2

CALCULATE AVAILABILITY PERCENTAGE

In the proposed availability risk assessment methodology, an MTBF and MTTR matrix is created. **Figure 4** shows the template that is used for creating the matrix. This matrix is created empirically by assigning acceptable uptime hours against each of the system architecture maturity levels under the MTBF column. A corresponding acceptable repair time value (MTTR) is assigned for every support capability maturity level. The MTBF value for the first three levels of system architecture maturity will be the same, as effectively the service is operating on a single system. The difference in maturity level is an indicator of the capability that exists in the environment to arrange standby or alternate systems.

The repair time (MTTR) is dependent not only on the support architectural maturity but also on system architectural maturity. This implies that, given a particular level of support maturity, the time taken to restore a service would decrease with an increase in the system maturity level.

While assigning values, it should be noted that the values are not biased by the existing system and vendor-specific experiences; rather, the values should be an indicator of what the organization considers as "enterprise grade" for its system's uptime and acceptable resolution time from its support service. A practical approach in creating this matrix would make the availability percentage closer to reality.

Using the MTBF and MTTR matrix, respective MTBF and MTTR values for each service catalog item are derived. Continuing with the earlier example, the BlackBerry service has system architecture maturity level 2; hence, the corresponding MTBF value of 4,380 hours is taken and, as the support architecture maturity level is 2, the MTTR value is derived from the intersection of the maturity levels, which in this case is 16 hours. Using the availability percentage formula, i.e., "MTBF / (MTBF+MTTR) x 100," the availability percentage for BlackBerry service is rated at 99.636 percent.

Applying the aforementioned approach to the entire service catalog, an availability risk assessment sheet is prepared, quantifying the availability percentage against each service as shown in **figure 5**.

CONCLUSION

The availability risk assessment methodology provides a quantitative approach for conducting availability risk assessment of IT services. This methodology helps in engaging with management to derive an acceptable level of service and gives prescriptive input for achieving the desired service levels. Using this methodology, the desired availability

Figure 4—MTBF and MTTR Matrix

			Support Architecture Maturity				
			MTTR (Values in Hours)				
System Architecture Maturity Level		MTBF	1	2	3	4	5
Ad hoc (single system)	1	4,380	48.00	24.00	16.00	8.00	4.00
Repeatable (standby can be arranged)	2	4,380	24.00	16.00	8.00	4.00	2.00
Defined (standby part of landscape)	3	4,380	8.00	4.00	2.00	1.00	1.00
Managed (high availability environment)	4	26,280	0.10	0.10	0.10	0.10	0.10
Optimized (could not be defined)	5						

Figure 5—Availability Risk Assessment Sheet

Service Catalog	System Maturity Level	Support Maturity Level	MTBF	MTTR	Availability %
E-mail access via Outlook	3	4	4,380	1.00	99.977
BlackBerry service	2	2	4,380	16.00	99.636
Video conferencing	1	1	4,380	48.00	99.916
Internet browsing	2	3	4,380	8.00	99.818
Corporate intranet	2	3	4,380	8.00	99.818
Outlook web access	2	3	4,380	8.00	99.818
Customer subscription	3	3	4,380	2.00	99.954
Payroll and PF trust accounting	3	2	4,380	4.00	99.909

percentage can be achieved by appropriately focusing on improving system or support maturity. The baseline provided by the availability risk assessment exercise can also be used for benchmarking and reporting the performance of IT operations. In addition, this methodology can assist the IS auditor in performing availability risk assessment of new systems that are in the design stage, thereby providing valuable input to management at an early stage of system development.

ENDNOTES

[1] Tipton, Harold F.; Micki Krause; *Information Security Management Handbook, 6th Edition*, Auerbach Publications, 2007

[2] Fischer, Urs; "Risk IT: Based on CobiT Objectives and Principles," *ISACA*, vol. 4, 2009

[3] Singleton, Tommie W.; "What Every IT Auditor Should Know About Auditing Information Security," *Information Systems Control Journal*, vol. 2, 2007

[4] International Electrotechnical Commission (IEC), "Analysis techniques for system reliability—Procedure for failure mode and effects analysis (FMEA)," IEC 60812, 2006

[5] Tryfonas, T.; D. Gritzalis; S. Kokolakis; "A Qualitative Approach to Information Availability," *Proceedings of the IFIP Tc11 15th Annual Working Conference on Information Security for Global Information Infrastructures*, S. Qing and J. H. Eloff, Eds., IFIP Conference Proceedings, vol. 175, Kluwer B.V., The Netherlands, 2000, p. 37-48

[6] Bass, Len; *et al*; *Software Architecture in Practice, 2nd Edition*, Pearson Education, 2003, p. 79

[7] Miler, Jakub; "A Service-oriented Approach to Identification of IT Risk," *Proceedings of the TEHOSS' 2005 First IEEE International Conference on Technologies for Homeland Security and Safety*, 2005

[8] *Op cit*, Bass 2003

[9] Carnegie Mellon University, *Systems Security Engineering—Capability Maturity Model: Model Description Document, Version 2.0*, 1 April 1999

Looking at IT Risk Differently

A.V. Rameshkumar, CISA, CISM, AICWA, ACS, CPM, OCP (Oracle Financials), OCP (Application Developer), is the head of IT for Al Aqili Group in Dubai, UAE. He has specialized in finance, corporate law, enterprise resource planning implementations, IT security, IT governance and solution architecture.

Risk is defined as the possibility of damage or loss. The word risk denotes that a decision maker knows the possible consequences of a decision and their relative likelihood at the time he/she makes that decision.

The ultimate decisions to be made in IT investments are:

- What IT assets should be held?
- How much money should be allocated to each?

These decisions are made in two steps.

1. Estimates are prepared of the risk and return over the investment holding period. This is called investment analysis.
2. Risk-return estimates are compared to decide how to allocate available funds among these investments on a continuing basis. This may be called IT portfolio analysis, selection and management.

The primary purpose of this article is to explore the notion of risk in IT, examine what creates risk and provide a quantitative measure of risk.

WHAT CREATES RISK?

Forces that contribute to loss or damage constitute elements of risk. Some influences are external to the enterprise and other influences are internal to the enterprise. These forces cannot be completely eliminated, and, hence, the enterprise has to take a calculated risk on its IT investment. IT risks are somewhat peculiar to each industry and/or firm.

Risk can be classified into systematic and unsystematic risk.[1] Systematic risk refers to that portion of risk caused by external factors; this is common and may affect all firms. Virus, hacking, fire, natural disasters and power loss are sources of systematic risk. Their effect is felt by many of the companies that are placed in the same position. For example, a loophole in the Internet browser that is vulnerable for hacking affects all of the firms that use the browser.

Unsystematic risk is the portion of total risk that is unique to the firm. The factors such as misuse of data, loss of data, application error, human interaction, inside attack and equipment malfunction can be cited for unsystematic risk. Unsystematic factors are largely independent of factors affecting the IT industry in general. Since these factors affect one firm, they must be examined for each firm.

The proportion of systematic and unsystematic risk denotes degree of vulnerability of the firm to the external or internal factors. Systematic risk is also known as generic risk, and unsystematic risk is also known as specific risk. Even though systematic risk is common for all firms of similar nature, its effect is not the same across all firms. This may be due to differences in the level of exposure and countermeasures taken by firms.

SCIENTIFIC PREDICTIONS

Uncertainty involves a situation about which the likelihood of the possible outcomes is not known. The existence of uncertainty necessitates careful and reasonable estimates of impact and some measure of the degree of uncertainty associated with these estimates of loss. Therefore, the risk needs to be quantified.

The quantification of risk is necessary to ensure uniform interpretation and comparison. Risk can be determined by calculating the product of likelihood and impact. The likelihood of an outcome can be stated in fractions or decimals. This is known as probability. A probability distribution is when the individual events are assigned probabilities. The total of probabilities assigned to individual events in a group of events must always be equal to 1.00. Assigning probabilities moves the abstract concept of likelihood to a mathematically amenable concept of probabilities, converting qualitative risk assessment (likelihood) to quantitative risk assessment (probability). Based upon the trend data available, the assessor can assign probabilities.

Similar to the likelihood, the impact has to be quantified. It is recommended that the assessor assign a percentage for each probability, 100 percent being the highest and 0 percent being the lowest. The impact may be:

- Loss of life
- Loss of money
- Loss of prestige
- Loss of market share
- Other factors

To quantify impact, there is a two-stage process:

1. Specify the impact percentage for every probability.
2. Specify the impact cost (e.g., asset value, loss of life, loss of money).

HYPOTHETICAL RISK ANALYSIS

Risk can be measured by calculating the standard deviation of probability distribution. **Figure 2** shows the variance and standard deviation of the probability distribution in **figure 1**.

Figure 1—Loss Due to Fire

Probability	Impact %	Probability Multiplied by Impact
0.4	0	0
0.3	5	1.5
0.2	10	2.0
0.1	20	2.0
		Mean: 5.5

The standard deviation is the square root of the variance, which in the case of the example here is 6.10.[2]

Variance is calculated by squaring each difference from the mean, multiplying the resultant sum by the related probability and summing the resulting amounts. Therefore, taking the square root of the variance results in the standard deviation. Risk can be denoted by standard deviation, which is a reasonable surrogate of risk.

Looking at the calculation of standard deviation, the following features can be stipulated. The difference between various possible values and the mean are squared. The values that are far away from the mean have a much greater effect on standard deviation than values that are close to the mean.

The squared differences are multiplied by the related probabilities. This means that the smaller the probabilities, the lower the effect on standard deviation.

Standard deviation is obtained as the square root of the sum of squared deviations. This means that mean and standard deviation are measured in the same units and the two can be used for comparison.

Assuming the value of the asset that is exposed to the previously mentioned risk is US $150,000, the impact cost in monetary terms is:

$$(6.10 \times 150{,}000)/100 = \text{US } \$9{,}150$$

CONCLUSION

Risk and return are two sides of a coin. When measuring return quantitatively, a quantitative measure for risk is needed. The method explained previously is one such measure for quantification of risk. This measure of risk can be considered with return, and a calculated decision on the risk-weighted return can be considered for any decision making where a risk-return scale is required.

Figure 2—Variance and Standard Deviation

Impact %	Expected Impact %	Difference	Difference Squared	Probability	Difference Multiplied by Probability
0	5.5	-5.5	30.25	0.4	12.1
5	5.5	-0.5	0.25	0.3	0.075
10	5.5	4.5	20.25	0.2	4.05
20	5.5	14.5	210.25	0.1	21.025
					VARIANCE: 37.25

ENDNOTES

[1] Reilly, F.K.; K. Brown; *Investment Analysis and Portfolio Management*, Harcourt College Publishers, 2002

[2] Probability and calculation of standard deviation can be found in any standard textbook on statistics, e.g., Levin, R.I.; D.S. Rubin; *Statistics for Management, 7th Edition*, Prentice Hall, 1997.

Compliance for Compliance's Sake?

Dan Sollis is group leader of business development at Infogix. Sollis supports business development activities including marketing and strategic partnerships. Previously, he served as senior vice president for Sanchez Computer Associates and general manager for Digital Equipment of Canada.

Many businesses consider compliance a cost of doing business, rather than an opportunity to implement operational excellence with effective automated internal controls. When the right automated internal controls are implemented, compliance is no longer a costly burden. What a business does to comply adds tremendous value, offsetting the cost of compliance.

Imagine it is the third quarter and the IT staff is preparing to roll a new enterprise resource planning (ERP) system into production to replace an out-of-date homegrown legacy system. As an online retailer, the goal has been to aggressively push the implementation deadlines with consultants to ensure operations are up and running prior to the holiday shopping season. To the delight of many, the implementation goes off without any major incidents—the manual fixes in the accounting system worked and the company sails through the holiday shopping season with ease. Five-and-a-half years later, an accounting error in the customer refunds system is discovered, proving that not all customer return codes in the new system have been recorded and shipping revenue for canceled orders has not been reversed out. Now, an embarrassing letter to shareholders explaining what caused the five-and-a-half year earnings restatement and the 1.7 percent reduction in revenue is required.[1]

> "Compliance is viewed as a mandatory requirement, not as an opportunity to proactively implement operational excellence."

Where were the internal controls that could have detected and prevented this error from going unnoticed and causing so much damage?

COMPLIANCE FAILURE—THE FALLOUT

Despite their best efforts to prevent system, process or human errors that result in restating financial reports or overcharging customer accounts, companies continue to experience the fallout of deficient internal controls. For example, more than 8,000 Macy's customers were debited up to three times for a single transaction during a recent holiday season. According to the retailer, a computer glitch in its payment processing systems caused the error. Macy's soon discovered it was an internal problem, and not an external problem as originally announced.[2]

Many companies, in fact, are seeing a continued stream of information errors that have gone undetected for periods of time and result in embarrassing headlines. Software giant Microsoft, for instance, discovered that a payroll error caused the overpayment of a number of recently terminated employees by an average of US $4,500 each. After initially sending letters requesting repayment within 14 business days, Microsoft retracted the request after a flurry of worldwide news headlines. It was also discovered during that time that another error caused Microsoft to underpay severance packages for a number of others.[3] Once discovered, these errors required additional effort by way of implementing additional manual controls and creating accounting spreadsheets to clean up information errors. In addition, auditors' jobs are made more difficult as they are required to look more closely at business processes, and internal controls are seen as deficient.

WHAT OPTIONS ARE AVAILABLE?

Since the US Sarbanes-Oxley Act was enacted in 2002, many companies have found Sarbanes-Oxley compliance too burdensome. Fulfilling Sarbanes-Oxley requirements is costly and time-consuming, often lacking immediate financial benefit for the company. In fact, companies that fail Sarbanes-Oxley compliance may suffer not only from hefty fines, embarrassing headlines and a tarnished brand; they are also at risk of having executives face prison terms of up to 20 years. As a result, many are moving their headquarters offshore to offset

the jurisdiction of compliance and consequences of failed compliance. Companies would rather relocate than comply with Sarbanes-Oxley.[4] It is no wonder most companies perceive compliance as a non-value-added activity but rather simply a cost of doing business. Compliance is viewed as a mandatory requirement, not as an opportunity to proactively implement operational excellence.

These missed opportunities are truncated as external auditors are consulted to identify what companies need to be able to prove compliance. This "phoning it in" method of operating results in extended auditing and consulting hours. For these, businesses' audit costs continue to rise, and there is a greater possibility of continued, unchecked information errors.

Internal controls that are implemented as a solution to hedge the risk of the cost of information errors are not a viable option. Manual processes that once worked can no longer keep up with the volume, pace and complexity of information.

Current methods of finding information errors are costly. A large staff of auditors may find the errors, but not in time to prevent them from propagating downstream, resulting in unavoidable and potentially disastrous operational consequences. In fact, studies show that the top 15 financial firms in the US are collectively involved in 70 percent of investment markets embeds, on average, between US $83.3 million to $600 million for direct costs, losses and operational risk resulting from erroneous information.[5]

> "Current methods of finding information errors are costly."

AUTOMATED INFORMATION CONTROLS—A VIABLE SOLUTION

Leading companies are pursuing a different strategy that will detect and prevent information errors from occurring, thereby saving the costs, embarrassment and headaches so frequently associated with these errors. These companies have recognized that their processes are information-intensive and have decided to automate the controls that ensure them. In these companies, automated information controls implemented in an enterprisewide controls environment add tremendous value. By creating and implementing a set of automated information controls for basic compliance checks, value is added through the streamlined auditing process. Additionally, these controls, when implemented accurately, detect and prevent information errors from occurring, providing the value of reliable information throughout the business processes, systems and applications. As a result, critical business decisions are based on accurate and reliable information through operational excellence. Businesses do things right the first time instead of going through the hassle, and sometimes embarrassing steps, of rework, reruns and restatements.

Automated information controls add tremendous value to a business because they ensure the integrity of critical information and processes, thereby saving money, enhancing efficiency, mitigating risk and streamlining the auditing process. Some examples[6] of how automated information controls have helped businesses are:

- Immediate return on investment (ROI) recognized by automating general ledger (GL) matching processes manually performed by 8-10 full-time employees, according to one leading investment services provider
- Revenue assurance, service accuracy, and continuity by prevention and detection of more than US $190 million in GL discrepancies, according to one *Fortune* 200 retailer
- Prevention of a US $32 million duplicate payment, according to a leading health insurer
- Significant operational cost reduction by automating 95 percent of manual processes, according to a large credit union
- Prevention of a US $57 million retail sales overstatement at a *Fortune* 200 retailer

Most companies that embark on an automated information controls journey do so with a specific business process in mind and a single team member or two piloting the effort. These team members train on the technology and author a few dozen controls, depending on the needs of the selected business process. This effort results in automated information controls for a specific system, while equipping the company with knowledge on costs, resource needs, skills and benefits for continuing to implement automated information controls for additional business systems.

KEY ASPECTS OF AUTOMATED INFORMATION CONTROLS

To ensure that automated information controls meet the criteria to streamline compliance and risk management, it is important to recognize the key attributes that are essential in automated information controls to provide greater value than options and alternatives available in the marketplace or via in-house development. Some of these attributes include:

- Information controls must be continuous. Although the term "continuous" may seem like an obvious attribute for these controls, this term is not defined consistently by all software vendors. Many vendors, in fact, apply the term "continuous" to mean the control is run on a frequent and recurring scheduled basis, as opposed to running as often as the underlying information and processes dictate. In yesterday's "batch process" world, frequent and recurring may have been sufficient. In today's distributed processing world, a continuous control must always be available to control in real time.
- The best information controls are independent from the applications, processes and systems that are being controlled. Conversely, embedded controls built into an application, process or system, by definition, cover a limited scope. These controls are subject to errors and failures of the specific system within which they are embedded (i.e., ERP systems, databases). For example, embedded controls will run only when the system in which they are embedded runs. Consequently, when that system fails, the controls embedded within it may also fail.
- It is important that information controls provide full, verifiable audit trails of control execution data and results. By doing so, they speed up the diagnosis of detected errors and detail what went wrong, when it went wrong, what business rules were violated, the source data and the location the error occurred. These verifiable controls streamline compliance by keeping an audit trail and providing documentation on not just the controls themselves, but on each control's execution as well. Verifiable information controls enable people to diagnose and correct information errors more easily.
- It is essential that information controls monitor business processes end to end, to validate critical business information that spans multiple processes, applications, databases and systems across the enterprise. Conversely, more limited-scope controls, such as account reconciliation controls, "see" only the information specific to the application where it is embedded. Therefore, these limited controls may not reconcile information as it travels across a series of applications, systems and business units.
- Successful information controls must be automated. Gone are the days of taking a sample set of accounts or transactions to manually verify the integrity of information. Automated information controls automatically validate all instances of controlled information and execute all transactions, resulting in 100 percent validation of the information without human intervention. They perform control checks as the information is generated or updated, and detect errors before they propagate downstream and cause more damage.
- Additionally, *ad hoc* automated controls may appear to be the most immediate quick-fix; however, they are typically comprised of hacked together programs and scripts. A set of *ad hoc* controls is usually anything but standardized. The time and resources required to train auditors and maintain *ad hoc* controls on multiple systems—with multiple access requirements—and processes are ineffective and costly and do not fundamentally improve the cost-benefit equation for automated control ownership. Imagine the IT effort required to keep a significant set of *ad hoc* controls in sync with changing business needs and regulations.

CONCLUSION

Regulatory compliance does not have to be painful and costly for businesses. With the proper information controls that are automated, independent, continuous, verifiable and end-to-end, compliance can be viewed as an added value to a business. Compliance is streamlined, risk is mitigated, efficiency is enhanced, and external audit costs are reduced. Automated internal controls can detect and prevent information errors from going unnoticed and causing damage. Transactions are no longer duplicated, payroll is accurate, compliance is streamlined, reports are reliable, and leadership has confidence in the integrity of business processes and information.

ENDNOTES

[1] Kanaracus, Chris; "Update: Overstock.com Restates Earnings, Cites ERP Implementation," *ComputerWorld*, 27 October 2008, *www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9118205*

[2] Schuman, Evan; Fred J. Aun; "Duplicate Debit Debacle Hits Best Buy, Macy's. Who's Next?," 18 March 2009, *www.storefrontbacktalk.com/securityfraud/duplicate-debit-debacle-hits-best-buy-macys-whos-next*

[3] Kincaid, Jason; "Oops: Microsoft Asks Some Laid Off Workers to Send Back Part of Their Severance (Updated)," 21 February 2009

[4] Morici, Peter; "Smash Sarbanes-Oxley Law," *Global Politician*, 16 June 2006, *www.globalpolitician.com/21867-america-economics*

[5] Grody, Allan D.; Fotios C. Harmantzis; Gregory J. Kaple; "Operational Risk and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation," *Journal of Operational Risk*, February 2007 (revised)

[6] All of the stated examples are based on Infogix customer testimony and identities cannot be disclosed due to contractual confidentiality.

Using Spreadsheets and Benford's Law to Test Accounting Data

Mark G. Simkin, Ph.D., is a professor of information systems at the University of Nevada (USA). He can be reached at *markgsimkin@yahoo.com.*

Accounting systems are popular targets of financial frauds because, in the words of bank-robber Willie Sutton, "that's where the money is." One common method thieves use to commit such fraud is to create fictitious accounting entities, e.g., bogus employee records or vendor payments, and then manipulate the fictitious records to their advantage. The success or failure of such scams rests in the ability to blend the bogus entries with legitimate data and, therefore, escape the notice of supervisors and auditors.

An interesting observation here is that most people are not very good at creating "natural data," making it possible for good auditors to apply fairly simple statistical tools to reveal such inabilities. One such test is to see how well the data follow Benford's Law.

Benford's Law involves the distribution of lead digits in "naturally occurring numbers," e.g., vendor payments, customer invoices, and similar financial values that occur in the normal course of business. For example, the lead digit in the vendor payment $123.45 is 1, the lead digit in a customer invoice amount of $4,231.55 is 4, and so forth. (All figures are provided in US dollars)

What Frank Benford discovered is that these lead digits are not uniformly distributed, as one might surmise. Rather, the number 1 is by far the most likely to occur, followed by 2, 3 and so forth. To apply Benford's Law, therefore, an accountant must count the number of times a 1 appears as the lead digit in the data values, the number of times a 2 appears, etc., and then examine the resulting frequency distribution. The distribution is "natural" if it follows Benford's distribution, and suspect otherwise.

Several professional accounting journals have published articles about Benford's Law (see the suggested readings at the end of this article). But, most of these papers have been theoretical in nature or required users to download additional software to perform the requisite statistical tests. For Excel users, such add-ins are unnecessary. This paper explains how to perform the tasks required to apply Benford's Law with simple Excel formulas.

TESTING LEAD DIGITS USING BENFORD'S LAW

Take the case of someone who wants to evaluate corporate purchase invoices—a popular target of corporate abuse. Although the amount of information contained in each invoice is likely to be considerable, this example will focus only on the purchase amounts. The goal of applying Benford's Law here is to know how "natural" such transactions are. **Figure 1** illustrates the required steps, which are further discussed in the sections that follow.

Step 1: Select the Sample Data

The first task is to obtain sample test data and store them in an Excel spreadsheet—the more observations included, the better. Using the data for a complete year is best, but if the number of items is large, smaller samples are permissible. For statistical reasons, however, there should be at least 100 observations. (**Figure 1** shows an example with fewer than 100 observations for illustrative purposes only.)

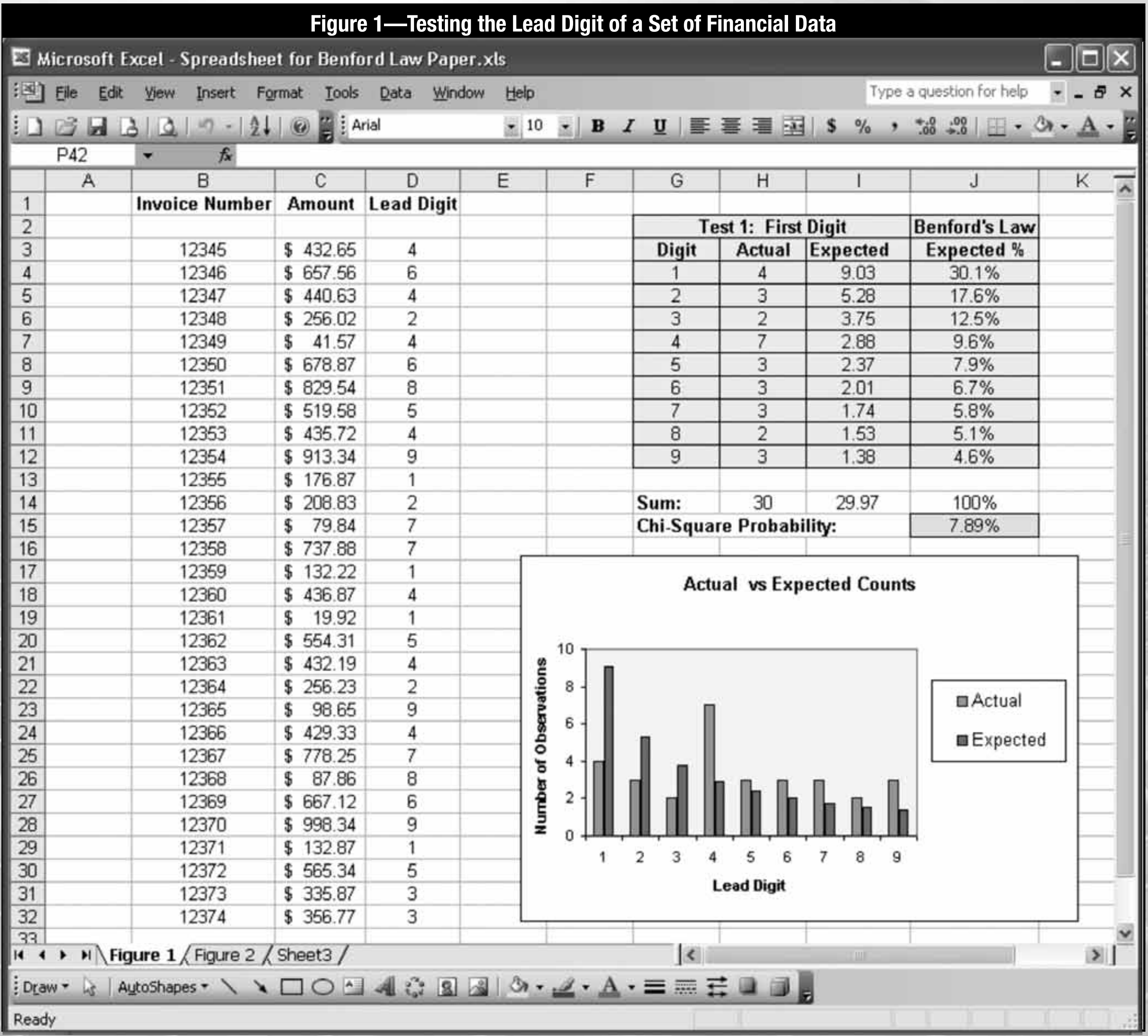
Step 2: Parse the Lead Digit

As noted previously, Benford's Law focuses on the lead digit in sets of naturally occurring numbers. The actual magnitude of the data (i.e., whether an amount is $10, $100 or $1,000) is unimportant. In a spreadsheet, one can select or "parse" the lead digit for each dollar amount (see **figure 1**), using Excel's LEFT formula. The general form of this formula is:

=LEFT(Data Item, Number of Characters)

Here, the term "Data Item" is a cell reference and "Number of Characters" indicates how many characters to parse (starting from the left side of the name or number). If Number of Characters is 2, for example, Excel will parse the two left-most

Figure 1—Testing the Lead Digit of a Set of Financial Data



Invoice Number	Amount	Lead Digit
12345	$ 432.65	4
12346	$ 657.56	6
12347	$ 440.63	4
12348	$ 256.02	2
12349	$ 41.57	4
12350	$ 678.87	6
12351	$ 829.54	8
12352	$ 519.58	5
12353	$ 435.72	4
12354	$ 913.34	9
12355	$ 176.87	1
12356	$ 208.83	2
12357	$ 79.84	7
12358	$ 737.88	7
12359	$ 132.22	1
12360	$ 436.87	4
12361	$ 19.92	1
12362	$ 554.31	5
12363	$ 432.19	4
12364	$ 256.23	2
12365	$ 98.65	9
12366	$ 429.33	4
12367	$ 778.25	7
12368	$ 87.86	8
12369	$ 667.12	6
12370	$ 998.34	9
12371	$ 132.87	1
12372	$ 565.34	5
12373	$ 335.87	3
12374	$ 356.77	3

Test 1: First Digit			Benford's Law
Digit	Actual	Expected	Expected %
1	4	9.03	30.1%
2	3	5.28	17.6%
3	2	3.75	12.5%
4	7	2.88	9.6%
5	3	2.37	7.9%
6	3	2.01	6.7%
7	3	1.74	5.8%
8	2	1.53	5.1%
9	3	1.38	4.6%
Sum:	30	29.97	100%
Chi-Square Probability:			7.89%

digits from the cell indicated and if this value is 3, it will parse the three left-most digits. Only one character should be parsed for the task at hand, so the formula for cell C3 is:

=LEFT(C3, 1)

Because the value in cell C3 is "432.65," the result is "4." The reason the displayed result is not a dollar sign ($) is because this character is simply a formatting symbol, which Excel ignores when performing the parsing task required. Once the formula for the first cell has been created in the spreadsheet, it can be copied to the subsequent cells in the column. **Figure 1** shows the results in column D.

Step 3: Create a Frequency Distribution

The next step is to create a frequency distribution of the lead digits that have been parsed from the sample data. To do this, the headings of the table shown on the right side of **figure 1** should be created, and the numbers "1," " 2," … , "9" should be stored in the first column under the heading "Digit."

Now it can be known how many invoice amounts start with each of these nine digits. (Zeros are ignored because amounts beginning with zero can be reduced to numbers beginning with the digits 1 through 9.) Although it is possible to use Excel's frequency formula for this task, it is just as easy to use the COUNTIF formula, which counts the number of elements in a data range that match a specific value. The general form of this formula is

=COUNTIF(Data Range, Criteria)

In this formula, the Data Range refers to the set of data one wishes to evaluate, and the Criteria parameter is typically either a literal value or a cell reference to such a value. For example, the formula COUNTIF(Z1:Z100, "Smith") would return the number of cells that contain the name "Smith" in the data range Z1:Z100 while the formula COUNTIF(Z1:Z100, X3) would return the number of cells matching whatever value is stored in cell X3.

For the illustration at hand, the desire is to know how many times each of the nine lead digits appears in the test data. Thus, the formula for cell H4—the first cell in the column with heading "Actual"—is:

=COUNTIF($D$3:$D$32, G4)

In this formula, the Data Range identifies the cells in column D, i.e., the column containing the lead digits. It is important to note that the formula uses absolute references—$D$3:$D$32—instead of D3:D32. This makes it possible to copy this formula to the other cells in the table. The Criteria for this formula is the reference to cell G4, which contains the value "1." Thus, the COUNTIF formula returns "4"—the number of cells in column D that contain this value. This can be verified by inspecting the data in column D.

Once the COUNTIF formula has been created for the first digit, this formula can be copied to the remaining cells in the table. **Figure 1** illustrates the results. Thus, for this example, the number 1 appeared four times as the lead digit in the sample data, the number 2 appeared three times as the lead digit in the sample data, and so forth.

Step 4: Compute the Expected Distribution

What would be expected for the distribution of these lead digits? Benford's Law predicts that approximately 30.1 percent of lead digits will be a 1,17.6 percent of the lead digits will be a 2, and so forth. Column J of **figure 1** shows the complete list of such percentages, which come from a logarithmic distribution and are explained more fully in the Nigrini article (see Suggested Readings).

From the percentages shown in column J of **figure 1**, one can work backward and compute the number of observations one would expect to find in the sample of 30. For each lead digit, the expected number is the percentage times the sample size. For example, for the lead digit of 1, the expected number of observations is 30.1 percent times 30 observations, or 9.03. Because cell H14 stores the total number of observations, the formula for the first number in column I (I4) is:

=J4*$H$14

In this formula, cell J4 contains the percentage amount (i.e., 30.1 percent for the first item) and cell H14 contains the total number of elements in the sample—in this case, 30. If one uses an absolute cell reference for cell H4 (i.e., $H$4) one can copy this formula to the other cells in column I. The results are as shown, e.g., an expected value of 5.28 for a lead digit of 2, an expected value of 3.75 for a lead digit of 3, and so forth. Of course, it is impossible ever to observe exactly 9.03 invoices with a lead digit of 1, or 5.28 invoices with a lead digit of 2. As any other average, what is being computed here is what might be found if one conducted this experiment over and over, using different sample data each time.

Step 5: Plot the Results

Now there are two sets of values—the actual distribution of lead digits from the sample and the theoretical distribution of such digits as dictated by Benford's Law. What one wants to know is how well these distributions match.

One way to answer this question is to plot these two sets of data and observe the results. To perform this task one can use Excel's charting tools and create a bar graph like the one in the inset portion of **figure 1**. The expected values show the pattern one would expect to see according to Benford's Law—an exponential decay pattern with a lead digit of 1 the most likely, a lead digit of 2 the next most likely, and so forth. The actual values show the distribution of lead digits actually found in the sample.

This charting work performs two useful tasks. First, the graph provides a visual answer to the question "how well do the sample data match the expected values?" For the example, at hand, the answer is "not very well." One sees, for example, that the lead digit of 1 occurred only about half as often as is expected, while the lead digit of 4 appeared much more often.

Second, the graph provides pictorial evidence of data spikes—in this case, for digit 4. Data spikes do not necessarily signal underlying problems such as fraud, but they do alert the accountant to the possibility of such problems. If the invoices illustrated here were for corporate purchases, for example, the data spike for a lead digit of 4 might be especially important if purchasing agents had a spending limit of $500. In one situation, auditors found that department heads were writing multiple checks for just under $5,000 to avoid a mandatory bidding process for items costing $5,000 or more.

Step 6: Perform a Chi-square Test

Although the sample data do not graphically match the expected values very well, the question remains "how far off are they?" To answer this question statistically, auditors can use Excel's CHITEST function—a chi-square test—to provide some guidance.

The chi-square test is a "goodness-of-fit" test, i.e., a statistical test that measures how well the data distribution from a sample matches a hypothetical distribution dictated by theory. For the example at hand, one wants to know how well the sample data in column H of **figure 1** match the expected values of Benford's distribution in column I of the figure. Excel's CHITEST has the general form:

> =CHITEST(Data Range of Actual Values, Data Range of Expected Values).

In this formula, the Data Range of Actual Values reflects the values derived from a sample, while the Data Range of Expected Values shows the expected values dictated by the theoretical distribution. The values required for this test have been computed in columns H and I of the table. Thus, the formula for cell J15, which computes the chi-square test statistic, is:

> =CHITEST(H4:H12,I4:I12)

Step 7: Reach a Conclusion; Are the Data "Natural?"

The chi-square statistic from Excel's CHITEST indicates the likelihood that the actual values in the sample follow the prescribed (Benford) distribution. High values such as 93 percent indicate a good match between actual and expected distributions, while small values such as 3 percent indicate a poor match. If one enters the test data shown in **figure 1** into a spreadsheet and changes some invoice amounts so that the actual bars come closer in pattern to the expected bars, the value for the CHITEST formula will increase accordingly.

As shown in cell J15 of **figure 1**, the chi-square test statistic for the sample data, formatted to a percentage, is 7.89 percent—a relatively small value. Does this value signal fraud? Not necessarily. But, generally speaking, values of less than 5 percent suggests that there is little likelihood that the data match the hypothesized (Benford) distribution, while values of 10 percent or less suggest that there is at least a 90 percent probability that the data are unnatural.

What to conclude? The low value for the chi-square test computed here suggests that the data in this sample are artificial. Before reaching this conclusion, however, there is another option: repeat the experiment using new sample data. This is one advantage of using a spreadsheet model for this work—one can overlay new data in columns B and C and the spreadsheet will perform every computation shown in **figure 1** automatically and immediately.

What if a chi-square test on the new data again results in a small value? This would be particularly meaningful because the results are multiplicative. If the chi-square test statistic for both samples were 10 percent, for example, the probability that the underlying data are "natural" would be (10 × .10 = .01) only 1 percent. Such a result signals a strong need for further investigation.

BENFORD'S LAW DO'S AND DON'TS

The idea that the lead digits of "naturally occurring data" are not uniformly distributed is counterintuitive to many people. After all, if the digits 1 through 9 were painted on a perfectly balanced spinning wheel, each digit would have an equal chance of occurring. But natural accounting data are not comparable to the numbers on a spinning wheel because they are not limited to specific ranges of values. Think of it this way: as a bank balance grows, for example, from a few hundred US dollars to more than a thousand dollars, which lead digits appear first in the new balance? The answer is first "1" (for a thousand dollars), then "2" (for two thousand dollars) and then "3" (for three thousand dollars). Thus, each time values increase by an order of magnitude, the number 1 appears first, followed by 2 and then 3. Benford's Law says exactly this, which is the reason why the probabilities for lead digits 1, 2 and 3 in Benford's distribution collectively account for more than 60 percent of the total probability distribution—not 30 percent as one might think (refer back to column J in **figure 1** to verify this larger percentage).

This explanation also suggests some important considerations when performing investigations using Benford's Law. One is that the law applies only to naturally occurring data. Purchase amounts, payment amounts, stock prices, accounts payable data, inventory prices and customer refunds are all good examples of such data. So are baseball statistics, areas of lakes, and the populations of towns—all of which Benford examined in his research but which are usually of less interest to accountants. The Law does not apply to assigned values, e.g., telephone numbers, lottery tickets, sequential customer numbers or check numbers (all of which, by definition, cannot repeat).

Second, it is important to avoid using financial data that are not natural. For example, the purchase amounts at a discount store might not lend themselves to Benford analysis, because there often is a single price point per item. Similarly, values with upper limits, such as airline passenger counts per plane or employee days worked per year, do not lend themselves to such analyses.

Third, it is important to sample "fairly" when selecting a set of data for analysis. For example, limiting a sample of invoices to values between US $100 and US $999 defeats the tests described here, because the data are limited to a narrow range. For small companies, using the complete data for an entire month or for a random day of each month is a better option.

Fourth, it is useful to know that Frank Benford did not limit his study to the lead digits of naturally occurring numbers. He also developed frequency distributions for secondary digits, i.e., the second or third digits in such numbers. Further analysis similar to the one in this article can be performed using Benford's distribution for such secondary digits and Excel's Mid function to parse them from the numbers one wants to test.

Finally, as a technical matter, it is important to obtain a set of test data that is large enough to obtain useful statistical results. The rule for chi-square tests is that the expected number of observations for each cell should be at least five. Because the smallest percentage in the Benford distribution is 4.6 percent, this requires a sample size of at least 100 observations. (Again, the reason a smaller set of observations was used in **figure 1** was to enable readers to see all the data tested.)

CONCLUSION

Benford's Law provides a powerful tool with which to determine how "natural" a given set of financial data is likely to be. The tests are both straightforward and easily implemented on spreadsheets without the need of add-in or supplemental software. But, it is also important to remember that not all financial data lend themselves to such tests and that care must be exercised when performing the analysis.

SUGGESTED READINGS

Benford, Frank; "The Law of Anomalous Numbers," *Proceedings of the American Philosophy Society*, vol. 78, 1938, p. 551-572

Browne, Malcolm W.; "Following Benford's Law, or Looking Out for No. 1," *New York Times*, 4 August 1998

Cleary, Richard; Jay C. Thibodeau; "Applying Digital Analysis to Benford's Law to Detect Fraud: The Dangers of Type I Errors," *Auditing*, vol. 24, no. 1, May 2005, p. 77-81

Hill, T.P.; "The First-Digit Phenomenon," *American Scientist*, vol. 86, no. 4, July-August 1998, p. 358-364

Johnson, Peter; "Fraud Detection with Benford's Law," *Accountancy Ireland*, vol. 37, no. 4, August 2005, p. 16-17

Nigrini, Mark; "I've Got Your Number," *Journal of Accountancy*, vol. 187, no. 5, May 1999, p. 79-83

Rodriguez, Ricardo; "Reducing False Alarms in the Detection of Human Influence on Data," *Journal of Accounting, Auditing, and Finance*, vol. 19, no. 2, 2004, p. 141-159

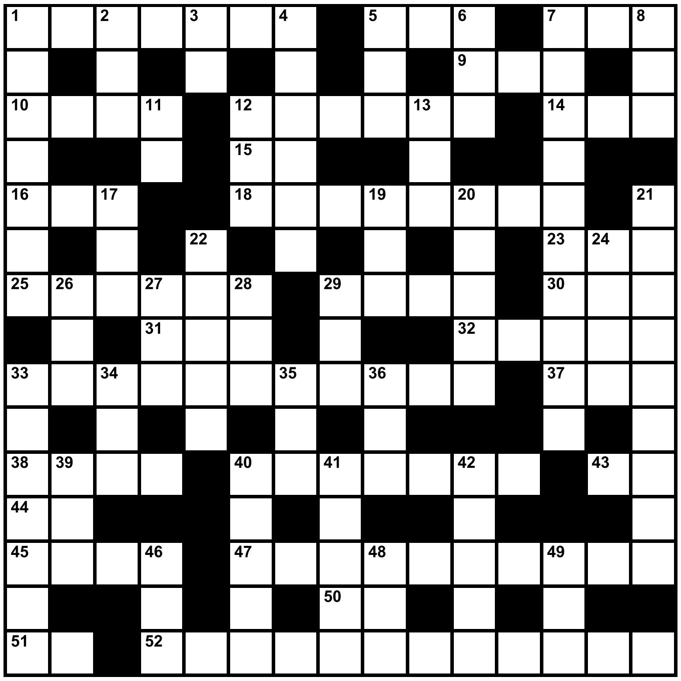
Rose, Anna M.; Jacob M. Rose; "Turn Excel Into a Financial Sleuth," *Journal of Accountancy*, vol. 176, no. 2, August 2003, p. 58-60

Stone, Amey; "Using Software to Sniff Out Fraud," *Business Week Online*, 30 September 2003, p. N

Williamson, Duncan; "Vital Statistics," *Accountancy*, vol. 133, no. 1327, March 2004, p. 108-110

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Rating
5. Three key factors relating to information that have become central to organizational strategies (abbr.)
7. The forerunner to outsourcing, from Ross Perot (abbr.)
9. Arbor starter
10. Possibility of damage or loss
12. It's expected from investment
14. Security risk consists of three factors, represented by these letters
15. The interactions between systems and technology, for short
16. One indicator of the value of IT (abbr.)
18. Key concept in CMM, developed by Carnegie Mellon's Software Engineering Institute
23. Expert
25. Bad-mouths
29. Hint
30. Haul off
31. GPS ___ NAV
32. Down East
33. Data duplicates (3 words)
37. Sculler's need
38. Leave out
40. Speakers' places
43. Control objective, for short
44. Madison locale
45. Headliner
47. Idea generators (2 words)
50. Promissory note, for short
51. Touring vehicle
52. Example of a factor in unsystematic risk (3 words)

DOWN

1. The number of these is one factor in assessing the IT level of sophistication of a company
2. VP title
3. Internet address
4. Attacks (2 words)
5. Computer operating system composed of free software
6. Deep-six
7. This is a vital part of security for all data in the cloud
8. ____ architecture improves the flexibility and scalability of business solutions
11. Unit of information, for short
12. BlackBerry maker
13. Proprietary archive file format developed by Eugene Roshal
17. Get outmoded
19. Internet address
20. Agenda points
21. One of the sources of systematic risk (2 words)
22. A major security risk factor
24. Net income divided by fixed assets plus net working capital (abbr.)
26. Entrepreneur's deg.
27. Pump
28. Process improvement that was developed in the field of securities transactions for lessening risk and increasing efficiency in securities clearance (abbr.)
29. Tax prep. expert
33. It becomes an access control mechanism in cloud computing
34. ___-square tests
35. Amazon's EC __
36. This has to be robust to achieve confidentiality and integrity for Internet-based services (abbr.)
39. A top tech school
40. Routes
41. Falls, as liquid
42. Design
46. A financial auditor must be careful to assess each IT weakness for its impact on ____ (abbr.)
48. Compass direction
49. Secrecy agreement, for short

(Answers on page 62)

Driving New Value From IT Risk Management

George Westerman, DBA, is a research scientist at the Massachusetts Institute of Technology Sloan Center for Information Systems Research (MIT CISR) and faculty chair for the IT for the Non-IT Executive course. His research and executive-level teaching examine management challenges at the interface between IT and business units such as risk management, innovation and communicating about value. He is coauthor (with Richard Hunter) of *IT Risk: Turning Business Threats Into Competitive Advantage* and *The Real Business of IT: How CIOs Create and Communicate Value*. He can be reached at *georgew@mit.edu.*

Brian Barnier, CGEIT, advises business and IT executives on getting better business results from IT through improved risk-return balance—whether cost cutting or building capabilities for recovery. He is also a teacher, writer and member of multiple best practices committees, including ISACA's IT Enterprise Risk Management Task Force, which oversaw the development of ISACA's Risk IT: Based on CobiT® framework. His writing includes contributing to the recent Wiley & Sons book *Risk Management in Finance*.

The economic downturn has created a dual problem for IT organizations. IT risk management is more important than ever, yet spending cuts mean that IT risk management investments must compete for limited funds with initiatives that appear more interesting to business executives. As organizations struggle to squeeze the most value from all monies invested, they find themselves asking how to get more value from their risk management activities. This goes beyond cutting risk management costs and includes using risk management insights to improve the way IT and business processes are managed.

Unfortunately, improving the value of IT risk management is far from straightforward. IT risk management has many faces, with managers in different silos (such as security, business continuity, project management and regulatory compliance) often operating independently.

For too long, IT risk management has been caught in a tenuous middle ground between enterprise risk and specialized silos of IT risk efforts. Technology risk managers have had to adapt general risk management guidance to the specialized domain of IT or try to generalize and integrate domain-specific guidance. Both approaches provide some help, but neither can generate the holistic view of IT risk as business risk that is becoming more important in an increasingly digitized and interconnected world. While ISACA's new Risk IT: Based on CobiT framework is crossing silos of risk management, it can also be seen as creating a larger menu of possible actions from which to select. This leaves professionals asking, "Where should we focus to improve the effectiveness and value of IT risk management?"

This article describes the three disciplines of IT risk management, their implications for risk management value and their context in ISACA frameworks. Companies that achieve maturity on the disciplines not only manage risk better, but also can use IT risk management to improve IT management and business outcomes. Their risk management investments pay new value in four ways: fewer incidents, more efficient IT processes, better alignment with the business and higher agility.

THREE DISCIPLINES OF IT RISK MANAGEMENT

In many organizations, the goal of IT risk management is to ensure that the company does not experience any bad incidents because of IT, whether from unplanned downtime, hacker attack, project overruns or a compliance problem. Organizations have already taken many basic actions in different areas of IT risk management. However, the focus is often on protection, not improvement, on spending, not value. In addition, they often fail to examine how their risk protection activities may decrease agility.

A recent Massachussetts Institute of Technology (MIT) research study found that three IT risk management disciplines work together to address risks to four key enterprise objectives: availability, access, accuracy and agility.[1] Companies that get higher value from IT risk management investments are mature in all three disciplines:

- An **IT foundation** that is well managed and only as complex as necessary
- A **risk governance process** to understand what risks the enterprise faces and to decide what to do about them
- A **risk-aware culture** where people have appropriate awareness of risks and are comfortable talking about them

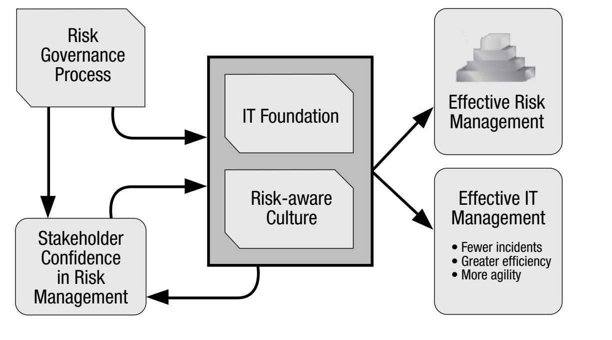
These three disciplines work together to ensure that an organization understands the IT risks it faces, makes good decisions about them and starts to reduce risk over time.

In mid-2008, the authors of this article surveyed 258 senior executives (100 IT, 158 non-IT) in six countries.[2] Respondents represented a balanced set of executives who self-identified as the most senior IT or business executive involved with IT risk. Survey questions were based on well-defined concepts from prior research, including the MIT Center for Information Systems Research (CISR) research

cited previously.[3] Survey items were statistically examined and combined to develop key research constructs, and then correlated and controlled to examine relationships between risk management maturity and important outcomes.

The analysis found that each of the three disciplines makes its own contribution to improving the value of IT risk management (see **figure 1**). Mature risk governance is necessary but not sufficient. It raises attention to risk, increases stakeholder involvement and provides information for decision making. However, actual improvement comes from driving change in the IT foundation and risk-aware culture. Firms with a more mature culture or foundation report statistically fewer incidents than other firms, but the benefits go farther. They also report statistically significantly higher efficiency, IT-business alignment and agility.

Figure 1—How the Three Risk Disciplines Relate to Business Performance



The IT risk management survey of 258 IT and non-IT executives finds firms that are more mature in the foundation and risk-aware culture (not just the risk governance process) also have higher business performance, not just fewer incidents.

Source: MIT Sloan Center for Information Systems Research & IBM

Although protecting the foundation and building awareness are familiar elements to CobiT[4] users, IT risk managers should go beyond these protections.

The goal of the risk governance process should be to improve the foundation and create a risk-aware culture, not just protect a shaky foundation or conduct awareness training. To cite a non-IT example, risk governance has been credited with reducing deaths in commercial aviation. That benefit was delivered not directly through the risk governance process, but through better design and maintenance of airplanes, plus creation of a risk-conscious culture among crew members. In IT terms, CobiT provides guidance on planning, implementing delivering and monitoring investments in, and operations of, an organization's IT foundation, including investments that reduce risk. In many IT situations, enterprises add protection and sometimes help to prevent maintenance issues. This is not enough. Enterprises frequently get only limited value from risk management because they invest only in protecting a poorly designed foundation instead of working to make the foundation less complex. Back to the airline example, more gauges in an airplane cockpit give pilots a better view of performance and problems, but they do not fix design problems in the engines.

What Does It Mean to Be More Mature in the Three Disciplines?

The risk governance process is the set of policies, processes and roles that enables an organization to exercise oversight and make better decisions about IT risks. In most firms, a central group creates policies and processes for the enterprise. Local managers identify and address the risks while notifying the central group about the highest risks. An enterprisewide committee prioritizes how to invest in mitigating the firm's highest risks, while local managers address lower risks on their own. Firms that are more mature in risk governance have clear risk categories, guidelines to assess risk consistently, formal exception processes and key risk indicators. They have also taken action to integrate their IT and enterprise risk processes.

No process improves without a process owner, but only half (48 percent) of firms have placed a single person in charge of IT risk management, according to the authors' survey. Only about a third of companies have either formal categories of risk or a formal exception process. Formal categories help to identify and compare risks in an apples-to-apples way. The exception process is even more important, since exceptions are how organizations learn. Exceptions also increase operations risk in the IT foundation by increasing complexity, meaning they should get special attention both during projects and afterward.

Only 28 percent of respondents to the survey say they use key risk indicators (KRIs) effectively.[5] A fully integrated KRI dashboard is difficult to achieve, but firms can start with simpler measures. Financial services firm PFPC (now PNC Global Investment Servicing) started by tracking trouble-ticket volume and employee turnover.[6, 7] Other firms track

indicators such as password resets, project completion rates, reconciliation failures, recovery times and intrusion attempts. In the current environment, it is essential to become more sophisticated in gathering, trending and acting upon KRIs, as well as in linking these to control design.

An important issue is the 66 percent of firms that have not effectively integrated IT risk into enterprise risk management (ERM). General-purpose ERM frameworks such as *A Risk Management Standard* (ARMS),[8] AS/NZS 4360[9] or the COSO ERM framework[10] do not explicitly address IT risk, but Risk IT enables companies to map from broader ERM frameworks to business process dependencies on technology.

The IT foundation is the set of infrastructure, applications, supporting technology and IT people who enable business processes to run. Firms with a mature IT foundation have a well-managed infrastructure, a well-defined business continuity plan, and a solid understanding of the links between technology and business process. But, they go beyond this. They also have enterprise architecture in place and are working to ensure that the IT foundation is no more complex than necessary.

An immature IT foundation—overly complex or poorly managed—is a recipe for risk. Inconsistent software updates and overly complex interdependencies cause it to fail often, make it difficult to recover, and make it more difficult to change. An immature IT foundation eats up maintenance resources and restricts agility.

While three-fifths of respondents reported that they maintain infrastructure well and have a working business continuity plan, it is important to stay vigilant. One firm experienced the same virus at three offices, six months apart, because IT staff in the affected sites did not inform other sites of the vulnerability. At another firm, IT staff routinely missed a set of servers when installing patches. Key to keeping the IT foundation well maintained are well-designed and well-maintained controls, such as those in COBIT, and operational management processes, such as those in the IT Infrastructure Library (ITIL).[11] In COBIT terms, these are the Deliver and Support (DS) and Monitor and Evaluate (ME) processes.

Although the majority of firms are satisfied with their infrastructure maintenance, not as many are taking the important step of reducing complexity in their IT foundation. Only about 40 percent believe their IT foundations are no more complex than necessary, or that their people understand the links between IT and business processes. Risk Evaluation (RE) processes in Risk IT can be helpful here, especially RE3.1 (*Map IT resources to business processes*) and those immediately following. Managers can use a risk-return approach to justify some investments that might not have a clear return-only business case. They can also use risk evaluation activities to identify ways to improve business processes, not just protect or control them. Then, they can use project-level IT governance mechanisms (such COBIT's Acquire and Implement [AI] processes and Val IT's[12] Investment Management [IM] processes) to gradually reduce complexity in the foundation over time.

For example, in prioritizing and conducting projects, several firms have begun to include architectural standards and complexity issues in their decisions. Intel prioritizes projects not only based on strategic alignment and expected financial return, but also on alignment with the firm's architectural direction. A consumer food manufacturer gives projects extra points in the prioritization process if they reduce complexity in the architecture. Further, PFPC introduced risk-focused checkpoints into its project demand management and delivery processes.

> "A mature risk-aware culture does not happen accidentally."

The risk-aware culture is the third discipline. This is not a risk-averse culture, and it is not a company that just does awareness training. It is a culture where people recognize the risks inherent in their activities, can openly discuss their risks, and are willing to work together to resolve risks or incidents. Having a mature risk-aware culture makes a firm both safer and more agile. People know how to avoid overly risky behaviors and resolve conditions that introduce unnecessary risk. However, they constantly balance this ability with the recognition that too much protection can introduce agility risks (i.e., rigidity). When people understand which risks are worth taking and understand which conditions and behaviors introduce unwanted risk, the firm can take on more risk in pursuit of return.

A mature risk-aware culture does not happen accidentally. It must be consciously built and reinforced by the company's leaders. Companies with a mature risk-aware culture have employees who understand risk and controls relevant to their jobs, who can talk openly about risk without fear of reprisal, who include risk in their business conversations, and who are encouraged through frequent reminders and top leadership reinforcement.

Three-fifths of respondents said their employees are comfortable talking openly about IT risks, but only about a third had effective risk training or reinforced it with reminders. Still fewer used risk awareness to improve the way they make IT decisions, as only 27 percent said most IT-business discussions include risk. Discussing IT risk issues, such as how tightly to integrate an acquired unit's IT assets or whether to use a nonstandard set of technologies in a project, can be a useful way to identify approaches that achieve the intended business benefit while also reducing operational risks. Furthermore, making clear the risk implications of a new mobile device, rather than just saying "it is too risky," can go a long way to not only making better decisions, but also to improving risk awareness and alignment.

The goal is to make the risk-aware culture in IT as prevalent as the safety culture in high-risk industries. Nearly every big oil company requires that meetings start with a short discussion on a safety topic. There are frequent safety reminders. Executives in these firms make a point of discussing risk and noting when people are being risk-unaware. IT leaders can use similar practices to make their units' cultures more risk-aware. This discipline corresponds to the risk culture discussion in section 3 of ISACA's *The Risk IT Practitioner Guide* and to Risk IT's Risk Governance (RG) processes 1 and 2 (especially RG1.5).

Driving New Value Through Risk Management Maturity

Most enterprises have made some progress on each of the disciplines, but maturity varies. To an ISACA member and CobiT user, the importance of controlling the IT foundation is clear. However, CobiT places less emphasis on reducing complexity in the foundation, building a risk-aware culture and increasing risk governance maturity. Risk IT extends CobiT with significant emphasis on risk governance and culture, but neither CobiT nor Risk IT specializes in architectural simplification.[13] The survey findings suggest actions IT risk managers can use to drive more business value from IT risk management activities—improving IT management, not just protecting against IT incidents.

First, balanced maturity matters. Maturity in one or two of the three disciplines was not as strongly associated with positive outcomes as maturity across all three. For example, focusing on CobiT DS processes without sufficient investment in, say, Risk IT RE processes creates the potential for misdirected or even wasted spending on various fixes. Similarly, building great risk governance without going on to improve the IT foundation and risk-aware culture is like being all dressed up with nowhere to go. Especially in this tough economy, risk managers must focus on creative and thoughtful approaches to investment and value, not just fixing the most visible risks.

Second, maturity must be assessed and improved across the disciplines. Risk managers can assess their organizations against maturity models in Risk IT or other frameworks.[14] Then, they should identify gaps in each discipline and work to bring all up to appropriate maturity. For example, if an enterprise is a strong CobiT shop, it likely has several mechanisms to improve areas such as networks or storage, but may struggle to build business cases around them. In this situation, it is probably wise to increase maturity in risk governance to improve alignment and gain stakeholder support for their investments. The governance process may be more mature in companies that focus on compliance or audit, but risk managers may struggle to "get beyond reporting" and show real business impact. Still others may be protecting an overly complex foundation without identifying opportunities to reduce operations risk by reducing complexity.

Third, IT risk management concepts must be integrated more tightly into other IT and business management processes. Managers who link IT risk to business objectives and outcomes can make the case for moving the IT foundation in the right direction—getting less complex, not just better managed. They also improve the risk-aware culture by helping everyone understand what drives operational IT risks and by making the risk implications of key IT decisions more apparent. By creating risk-based cost scenarios, they can help IT and business executives better align their expectations.

Also, by influencing decisions rather than trying to protect the results of risk-blind decisions, risk governance can pay off twice. It reduces negative incidents and increases business benefit by maturing the foundation. For example, operational risk managers at a major credit card company and at a Canadian bank both reported that, when examining risks in their business processes, they discovered useful ways to reengineer the processes. Their initial investments in risk management largely paid for themselves through improved business efficiency and service quality.

Finally, to improve outcomes from their activities, IT risk leaders can join forces with others who have shared objectives. Managers in IT governance, enterprise architecture, business continuity, compliance, security and project portfolio management all have reasons to emphasize risk as well as return, less complexity over more, and a more risk-conscious culture over one that is less so. Potential allies often have more influence over investment prioritization and project execution than risk managers do. Conversely, risk managers can sometimes help these allies justify their initiatives through risk considerations. For example, many enterprise architects found that focusing on the risks of Sarbanes-Oxley compliance helped them provide rationales for initiatives they had difficulty justifying before.

CONCLUSION

Companies that are mature in all three disciplines—risk governance process, IT foundation and risk-aware culture—have statistically significantly fewer incidents, higher IT efficiency, better alignment and higher business agility. But maturity means more than just doing the basics. It is more than identifying risks, protecting existing assets and increasing awareness of threats. Companies with mature risk management capability use risk governance to reduce complexity in the foundation. They go beyond awareness to build a culture in which safe discussion of risk (from availability through agility) is the norm. These companies not only prevent risk, but also can take new risks safely. They not only reduce incidents, but also improve efficiency. Then, the company's investments in risk management pay off not only in better risk management, but also in better IT management and business results.

AUTHORS' NOTE

The authors continue their research into IT and enterprise risk management. If you are interested in being a case study or survey participant, please contact George Westerman at *georgew@mit.edu* or Brian Barnier at *brian@valuebridgeadvisors.com.*

ENDNOTES

[1] Westerman, George; Richard Hunter; *IT Risk: Turning Business Threats Into Competitive Advantage*, Harvard Business School Press, 2007

[2] This article is the third paper based on this research. Previous papers are: Westerman, G.; B. Barnier; "How Mature Is Your IT Risk Management?," MIT Sloan CISR Research Briefing, vol. VIII, no. 3C, December 2008. Westerman, G.; B. Barnier; "IT Risk Management: Balanced Maturity Can Yield Big Results," IBM white paper, February 2009.

[3] *Op cit*, Westerman and Hunter

[4] CobiT (IT Governance Institute, 1996-2007) is an IT governance framework and supporting tool set that allows managers to bridge the gaps among control requirements, technical issues and business risks. CobiT enables clear policy development and good practice for IT control throughout organizations. More information is available at *www.isaca.org/cobit.*

[5] As defined in Risk IT (ISACA, 2009, *www.isaca.org/riskit*), "Any metric showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk tolerance is a KRI." KRIs are described in more detail in section 7, "Essentials of Risk Response," of Risk IT.

[6] Westerman, G.; R. Walpole; "PFPC: Building an IT Risk Management Competency," MIT Sloan CISR Working Paper #348

[7] *Op cit*, Westerman and Hunter

[8] The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) and ALARM (The Public Risk Management Association), *A Risk Management Standard* (ARMS), UK, 2002, *www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf*

[9] Standards Australia and Standards New Zealand, AS/NZS 4360:2004, *Australian/New Zealand Standard for Risk Management*, 2004

[10] Committee of Sponsoring Organizations (COSO) of the Treadway Commission, *Enterprise Risk Management—Integrated Framework* (COSO ERM), 2004. This should not be confused with the COSO Control Framework that is familiar to many CobiT practitioners. A summary of COSO ERM is available at *www.coso.org.*

[11] Office of Government Commerce, IT Infrastructure Library V3, UK, 2008, *www.ogc.gov.uk/guidance_itil.asp*

[12] Val IT (ISACA, 2008, *www.isaca.org/valit*) is an ISACA framework and supporting publications addressing the governance of IT-enabled business investments.

[13] To cover this, ISACA provides a 281-page mapping from CobiT to The Open Group Architecture Framework (TOGAF). See ISACA, *CobiT® Mapping: Mapping of TOGAF 8.1 With CobiT® 4.0*, 2007, *www.isaca.org/cobitmapping.*

[14] Readers are welcome to contact the authors for the short set of assessment questions used in their research.

Prepare for the 2010 CISM Exams

ORDER NOW—2010 CISM Review Materials for Exam Preparation and Professional Development

To pass the Certified Information Security Manager® (CISM®) exam, candidates should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA® offers several study aids and review courses to exam candidates.

www.isaca.org/cismreview

To order CISM review material for the June/December 2010 exams, visit the ISACA web site at *www.isaca.org/cismbooks* or see pages S1-S4 in this *Journal*.

CISM Review Manual 2010

ISACA

The *CISM® Review Manual 2010* is a comprehensive reference guide designed to assist individuals in preparing for the CISM exam and individuals who wish to understand the roles and responsibilities of an information security manager. The manual has evolved over the past six editions and now represents the most current, comprehensive, globally peer-reviewed information security management resource available.

The *CISM Review Manual 2010* features a new format. Each of the five chapters has been divided into two sections for focused study. The first section contains the definitions and objectives for the five areas, with the corresponding tasks and knowledge statements that are tested on the exam.

Section 1 is an overview that provides:

- Definitions for the five areas
- Objectives for each area
- Descriptions of the tasks
- A map of the relationship of each task to the knowledge statements
- A reference guide for the knowledge statements, including the relevant concepts and explanations
- References to specific content in section 2 for each knowledge statement
- Sample practice questions and explanations of the answers
- Suggested resources for further study

Section 2 consists of reference material and content that supports the knowledge statements. Material included is pertinent for CISM candidates' knowledge and/or understanding when preparing for the CISM certification exam. Also included are definitions of terms most commonly found on the exam.

This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses. It is a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.

The 2010 edition has been developed and is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- Information security governance
- Information risk management
- Information security program development
- Information security program management
- Incident management and response

CM-10	English Edition
CM-10J	Japanese Edition
CM-10S	Spanish Edition

CISM Review Questions, Answers & Explanations Manual 2009

ISACA

The *CISM® Review Questions, Answers & Explanations Manual 2009* consists of 450 multiple-choice study questions that have previously appeared in the *CISM® Review Questions, Answers & Explanations Manual 2008* and the *2008 Supplement*. These questions are not actual exam items, but are intended to provide CISM candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam. This publication is ideal to use in conjunction with the *CISM Review Manual 2010*.

To assist candidates in maximizing study efforts, questions are presented in the following two ways:

- Sorted by job practice area
- Scrambled as a sample 200-question exam

CQA-9	English Edition
CQA-9J	Japanese Edition
CQA-9S	Spanish Edition

CISM Review Questions, Answers & Explanations Manual 2009 and 2010 Supplements

ISACA

Developed each year, the *CISM® Review Questions, Answers & Explanations Manual 2009 Supplement* and *2010 Supplement* are recommended for use when preparing for the 2010 CISM exam. Each supplement consists of 100 different sample questions, answers and explanations based on the current CISM job practice areas, using a process for item development similar to the process used for developing actual exam items. The questions are intended to provide CISM candidates with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISM exam.

2010 Editions

CQA-10ES	English Edition
CQA-10JS	Japanese Edition
CQA-10SS	Spanish Edition

2009 Editions

CQA-9ES	English Edition
CQA-9JS	Japanese Edition
CQA-9SS	Spanish Edition

CISM Practice Question Database v10

ISACA

The CISM® Practice Question Database v10 combines the *CISM Review Questions, Answers & Explanations Manual 2009* with the *CISM Review Questions, Answers & Explanations Manual 2009 Supplement* and *2010 Supplement* into one comprehensive 650-question study guide. Sample exams with randomly selected questions can be taken and the results viewed by job practice, allowing for concentrated study one area at a time. Additionally, questions generated during a study session are sorted based upon previous scoring history, allowing CISM candidates to easily and quickly identify their strengths and weaknesses and focus their study efforts accordingly. Other features provide the ability to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of study sessions. The database software is available in CD-ROM format or as a download.

PLEASE NOTE the following system requirements:

- 400 MHz Pentium processor or equivalent (minimum); 1 GHz Pentium processor or equivalent (recommended)
- Supported operating systems: Windows Server 2003, Windows Server 2008, Windows Vista, Windows XP
- 512 MB RAM or higher
- One hard drive with 250 MB of available space (flash/thumb drives not supported)
- Mouse
- CD-ROM drive

MDB-10	English Edition—CD-ROM
MDB-10W	English Edition—Download

HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Gan Subramaniam, CISA, CISM, CIA, CISSP, SSCP, CCNA, CCSA, ISO 27001 LA, is the global IT security lead for a management consulting, technology services and outsourcing company's global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big Four professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam's previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK; Thomas Cook (India); and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.

Q I believe that deployment and usage of 'collaboration tools' is the order of the day. With the wide and rampant use of e-mails, voice and normal conversations combined with blogs and social networking sites, what kind of policies should an organisation have in place?

You may also wish to share your thoughts on archival of e-mails by corporate entities. Is there a minimum, rather ideal, period until which archives must be kept?

A It is a very tricky scenario. On one hand, companies may restrict access to social networking and blogs as part of their Internet browsing policy; yet, the company makes a presence on such sites as well.

Corporate entities must have clear policies defining what their employees must do and must not do in no uncertain terms—whether it is blogging, cell phone, e-mail or Internet use. I am sure you can write your own policies on what to do and what not to do. However, I believe that it is essential that we understand the criticality of the matter given the litigious environment. There are many instances where companies have been held liable for the inappropriate acts of employees.

Let me illustrate this with some real-life examples. An Atlanta, Georgia, USA-based company in the construction business was ordered to pay US $4.75 million as compensation to settle a lawsuit involving one of its employees. The employee involved had caused a car crash resulting in serious injuries, while making business calls on a company provided mobile phone.

This is not a unique case. I can quote many more similar cases:

- A multinational banking giant paid US $500,000 as compensation to the family of a motorcyclist who was fatally injured when one of its brokers caused an accident while making sales calls on his personal mobile phone.
- A state government was made to pay US $1.5 million dollars as compensation to a pedestrian who was hit by a teacher, an employee of the state, who was driving the car and simultaneously speaking on the phone, leading to the accident.

Employers can be held liable for actions of the employees while doing any business-related work:

- A multinational oil company was made to pay a compensation of US $2.2 million to a group of its women employees who sued it on grounds of sexual harassment. The allegation was that the company allowed the usage of its internal e-mail systems to some employees who circulated an e-mail amongst them that contained sexually offensive messages.
- A German bank was slapped with a fine of US $87.5 million for not having the appropriate controls in terms of e-mail archival and retention.
- During the peak of the dot-com boom, a staff member at a multinational investment banking firm was canvassing favourably on the prospects of high-tech companies. However, one particular stock analyst and some of his colleagues were warning the company's private investment clients to steer clear of many of the very same companies that the employer was propping up publicly. Unfortunately for his employer, the analyst had used his company's e-mail system to circulate his thoughts. When regulators investigated the investment banking giant and discovered the analyst's e-mails, the investment banking giant agreed to pay US $100 million in penalties.
- A well-known investment bank was ordered to pay US $29.3 million as compensation for failing to produce subpoenaed e-mails. A former employee had sued the bank alleging discrimination and it came to light during the course of the trial that backup tapes were missing and e-mail messages had been deleted.

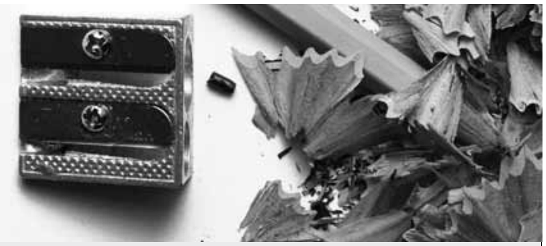
- A UK-based company opted for an out-of-court settlement for alleged defamation by some of its employees using its internal e-mail systems against a competitor. By the time the suit was filed and the trial started the concerned e-mail messages had been deleted. However, the competitor obtained a court order forcing the company to search their backup systems to retrieve the data. The company tendered an apology and paid £450,000 in damages and costs to settle the case with the competitor.

A US blogger coined the term 'dooced,' which means 'to lose your job because of blogging'. She used her blog to rant about a lot of things, including her woes against her employer, without actually disclosing her name. When her employer found out about the blog, she lost her job.

The list of examples is endless.

It is important for companies, in consultation with their own legal function, to determine the ideal period for e-mail archival and retention. I cannot prescribe a set period as the optimal one, as there is no one-size-fits-all approach.

It is equally important for companies to ensure that their employees use the e-mail systems in an appropriate manner as anything otherwise may come back to haunt them as seen in some of the noted examples.



CPE Quiz

Prepared by Sally Chan, CGEIT, CMA, ACIS

Quiz #128

Based on volume 5, 2009, Convergence of Technology, Control and Communication
Value: 1 Hour of CISA/CISM/CGEIT continuing professional education (CPE) credit

TRUE OR FALSE

SINGLETON ARTICLE

1. The Gramm-Leach-Bliley Act of 1999 requires entities that have experienced a security breach of personal private information, where the customers/clients are residents of California (USA), to notify each customer/client of the breach.
2. The privacy principle of "collection limitation" refers to the fact that personal data cannot be disclosed, made available or otherwise used for purposes other than those specified in the "purpose specification" principle.
3. The advantage of using cloud computing is the possible elimination of the risks associated with the storage problems related to laptops, USB drives and drives being transported.

FISCHER ARTICLE

4. Risk governance is one of the three domains of the Risk IT framework. It ensures that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted returns.
5. Risk response is about identification of the important and relevant risks that can possibly occur with IT or in relation to IT, given the pervasive presence of IT and the business's dependence on it.
6. A risk-aware culture begins at the top, with business executives who set direction, communicate risk-aware decision making and reward effective risk management behaviors. Risk awareness also implies that all levels within an enterprise are aware of how and why to respond to adverse IT events.

DE HAES, VAN GREMBERGEN AND VAN BREMPT ARTICLE

7. The CobiT implementation status for the different IT governance processes revealed that the processes in the Plan and Organize and Monitor and Evaluate domains received overall the highest scores compared to those of the Deliver and Support and Acquire and Implement domains.
8. Research confirms a knowing-doing gap regarding the top 10 most important IT governance and business goals for enterprises, implying that enterprises are aware of the importance of these goals but do not manage to realize them in a proper way.

ADOLPHSON AND GREIS ARTICLE

9. Segregation of duties (SoD) dictates that problems such as fraud, material misstatement and financial statement manipulation have the potential to arise when the same individual is allowed to execute two or more conflicting sensitive transactions.
10. The goal of the remediation phase of the SoD road map is the temporary correction of SoD conflicts.

EE ARTICLE

11. The Johari Window provides a means to understand the different levels of communication that take place between auditors and management. The Johari Window is comprised of a window dividing management and auditor awareness. The Blind Spot pane defines the area of information known by the auditors but not management.
12. The Facade pane in the Johari Window represents the highest level of uncertainty and the greatest potential for exploring new ideas and opportunities for improvement.
13. Another information processing paradigm—the Common Ground Congruity (CGC) model—covers underlying motivations and the overlaying perspectives among the official agenda, the client's agenda and the auditor's agenda.

HARE ARTICLE

14. Segregation of duties (SoD) is one of the primary means to prevent fraud yet there is little consensus about best practices related to SoD, even several years since Sarbanes-Oxley was adopted.
15. External auditors will always be focused primarily on whether or not a company's financial statements are materially accurate. They have no exposure or accountability for fraud that is committed below the materiality threshold. It is up to management to design or redesign controls to catch submaterial fraud.
16. If looking at fraud risk holistically, processes and risks outside of the system are just as important as those inside the system. There are considerable risks in manual processes, especially below the materiality threshold, where IT auditors have little training and experience.
17. A comprehensive risk assessment project starts first by identifying the mitigating controls already in place—some may be key controls and some may not be key controls.

ISACA Journal
CPE Quiz
Based on Volume 5, 2009—
Convergence of Technology, Control and Communication

Quiz #128 Answer Form

(Please print or type)

Name ____

____

Address____

____

____

CISA, CISM or CGEIT# ______________________________

Quiz #128

True or False

SINGLETON ARTICLE

1. __________
2. __________
3. __________

FISCHER ARTICLE

4. __________
5. __________
6. __________

DE HAES, VAN GREMBERGEN AND VAN BREMPT ARTICLE

7. __________
8. __________

ADOLPHSON AND GREIS ARTICLE

9. __________
10. _________

EE ARTICLE

11. _________
12. _________
13. _________

HARE ARTICLE

14. _________
15. _________
16. _________
17. _________

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 e-mail, fax or mail your answers for grading. Return your answers and contact information by e-mail 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 or CGEIT CPE credit.

Answers—Crossword by Myles Mellor

See page 52 for the puzzle.

S	C	O	P	I	N	G	■	G	R	C	■	E	D	S
E	■	P	■	P	■	O	■	N	■	A	N	N	■	O
R	I	S	K	■	R	E	T	U	R	N	■	C	I	A
V	■	■	B	■	I	S	■	■	A	■	■	R	■	■
E	V	A	■	■	M	A	T	U	R	I	T	Y	■	P
R	■	G	■	F	■	T	■	R	■	T	■	P	R	O
S	M	E	A	R	S	■	C	L	U	E	■	T	O	W
■	B	■	S	A	T	■	P	■	■	M	A	I	N	E
B	A	C	K	U	P	T	A	P	E	S	■	O	A	R
R	■	H	■	D	■	W	■	K	■	■	■	N	■	L
O	M	I	T	■	P	O	D	I	U	M	S	■	C	O
W	I	■	■	■	A	■	R	■	■	O	■	■	■	S
S	T	A	R	■	T	H	I	N	K	T	A	N	K	S
E	■	■	M	■	H	■	P	N	■	I	■	D	■	■
R	V	■	M	I	S	U	S	E	O	F	D	A	T	A

Standards
Guidelines
Tools and Techniques

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 examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework's concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, *www.isaca.org/cobit*.

Links to current guidance are posted on the standards page, *www.isaca.org/standards.*

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 Application Systems Review Effective 1 October 2008
G15 Planning Revised Effective 1 March 2002
G16 Effect of Third Parties on an Organisation's IT Controls Effective 1 March 2009
G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 15 June 2009
G18 IT Governance Effective 1 July 2002
G19 Irregularities and Illegal Acts Withdrawn 1 September 2008
G20 Reporting Effective 1 January 2003
G21 Enterprise Resource Planning (ERP) Systems Review Effective 1 August 2003
G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
G24 Internet Banking Effective 1 August 2003
G25 Review of Virtual Private Networks Effective 1 July 2004
G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
G27 Mobile Computing Effective 1 September 2004
G28 Computer Forensics Effective 1 September 2004
G29 Post-implementation Review Effective 1 January 2005
G30 Competence Effective 1 June 2005
G31 Privacy Effective 1 June 2005
G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
G33 General Considerations for the Use of the Internet Effective 1 March 2006
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G36 Biometric Controls Effective 1 February 2007
G37 Configuration and Release Management Effective 1 November 2007
G38 Access Controls Effective 1 February 2008
G39 IT Organisation Effective 1 May 2008
G40 Review of Security Management Practices Effective 1 October 2008

IT Audit and Assurance Tools and Techniques
P1 IS Risk Assessment Measurement Effective 1 July 2002
P2 Digital Signatures and Key Management Effective 1 July 2002
P3 Intrusion Detection Systems (IDS) Review Effective 1 August 2003
P4 Malicious Logic Effective 1 August 2003
P5 Control Risk Self-assessment Effective 1 August 2003
P6 Firewalls Effective 1 August 2003
P7 Irregularities and Illegal Acts Effective 1 December 2003
P8 Security Assessment—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
P10 Business Application Change Control Effective 1 October 2005
P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

Standards for Information System Control Professionals Effective 1 September 1999
510 Statement of Scope
.010 Responsibility, Authority and Accountability
520 Independence
.010 Professional Independence
.020 Organisational Relationship
530 Professional Ethics and Standards
.010 Code of Professional Ethics
.020 Due Professional Care
540 Competence
.010 Skills and Knowledge
.020 Continuing Professional Education
550 Planning
.010 Control Planning
560 Performance of Work
.010 Supervision
.020 Evidence
.030 Effectiveness
570 Reporting
.010 Periodic Reporting
580 Follow-up Activities
.010 Follow-up

Code of Professional Ethics Revised May 2003

Advertisers/Web Sites

Audit^2	*www.audit2.com*	Back Cover
CCH Teammate	*www.CCHGroup.com/ISC*	Inside Back Cover
ExamMatrix Learning	*www.ExamMatrix.com/ISJ*	11
IAD Solutions, Inc.	*www.AuditLeverage.com*	31
Lander International LLC*	*www.landerint.com*	9
Modulo	*www.modulo.com*	1
RSH Consulting	*www.rshconsulting.com*	24

* Position openings/recruitment listings

ISACA® Journal, formerly *Information Systems Control Journal*, is published by ISACA, a nonprofit organization created for the public in 1969. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

Subscription Rates:
US: one year (6 issues) $75.00
All international orders: one year (6 issues) $90.00. Remittance must be made in US funds.

ISSN 1944-1967

Leaders and Supporters