Technology Internal Auditing is sometimes frustrating and not always understood by non-technology executives. For technology auditing to be meaningful, it must be focused on the business objectives that matter to your organization's executives and board. Cost savings. Efficiencies. Improved quality and effectiveness. The results from I.T. audits must be delivered in simple and understandable business terms that are actionable for decision makers. At Protiviti, our experienced professionals do just that. We ensure I.T. audits move beyond risk identification and provide management with relevant insight into how to improve their business. We call it “High Value Auditing.”

And it is why our clients understand that the greatest risk in a technology audit is missing the opportunity to drive organizational value from the information.

To learn more about Protiviti's High Value Audits or to speak with a Protiviti team member, please visit protiviti.com/highvalueaudit or call 866.720.7264.

protiviti®
Independent Risk Consulting

Know Risk. Know Reward.®
Information Systems Control
The Magazine for IT Governance Professionals
VOLUME 4, 2008

Columns

5 Guest Editorial: A Rogue Trader Strikes Again!
Deepak Sarup, CISA, FCA

9 IS Security Matters: Managing Information Crises
By Steven J. Ross, CISA, CBCP, CISSP

11 IT Audit Basics: What Every IT Auditor Should Know About Access Controls
Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA

17 IT Value: Five Steps to Introducing Val IT: Applying Val IT to Introduce or Improve Value Management in an Enterprise
By Sarah Harries and Peter Harrison, FCIP

20 Five Questions With...
Ray Slocumb, CISA, CFE

22 IT Governance: New Framework for Enterprise Risk Management in IT
By Urs Fischer, CISA, CIA, CPA Swiss

Features

25 Book Review: Securing Converged IP Networks
Reviewed by Kamal Parmar, CISA, FCCA, CCNA, MCP

26 Book Review: Business Continuity and Disaster Recovery for IT Professionals
Reviewed by Naiden Nedelchev, CISM, CEH, ITIL

Reviewed by Reynaldo J. de la Fuente, CISA, CISM

29 Book Review: Fraud Casebook: Lessons From the Bad Side of Business
Reviewed by Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA

31 A Comprehensive Method for Assessment of Operational Risk in E-banking
By George Tanampasidis, CISA, PMP

38 Risk Management Standards: The Bigger Picture
By David Ramirez, CISA, CISM, CISSP, BS 7799 LA, MCSE, QSA

41 Automating Security Policy and Procedures With Workflow: How to Improve the Effectiveness of Risk Management Solutions
By Michael Godfrey

45 Case Study: Better to Prevent Than Cure—A New Way to Enhance IT and Business Governance Collaboration
By Tuulikki Help

49 Secure Software Development—The Role of IT Audit
By Ozlem Aras, Barbara L. Ciaramitaro, Ph.D., CISSP, and Jeffrey Livermore, Ph.D.

54 IT Governance Roundtable: Boston, November 2007

Plus

16 Standards, Statements, Guidelines
ISACA® Member and Certification Holder Compliance

57 HelpSource Q&A
By Gan Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCSI, BS 7799 LA

59 CPE Quiz #119
Based on Volume 2, 2008
Sally Chan, CMA, ACIS

S1-S8 ISACA Bookstore Price List Supplement

The following articles will be available to ISACA members online on 1 August 2008.

Evaluating Privacy Controls
By Sean M. Price, CISA, CISSP

Information Systems Audit Legislation Passed in Korea
By Ilkoon Cho, Changmin Lee, Daul Shin, Jaque Rim, Sojung Kim, Hyunnok Oh and Kyeonghee Oh

What E-commerce Audit Planners Should Remember: The Top 10 Global CSFs for B2B Audit
By S. Ejaz Ahmad, Ph.D., Abdulkadir A. Hussein, Ph.D., and Jagdish Pathak, Ph.D.

The Information Systems Control 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 governance, control, security and assurance.
Don’t let fraud go undetected.

IDEA
See it right the first time.

The analysis of company data is the single most effective way of detecting fraud. **IDEA** is the most powerful and complete data analysis software available today to assist you in the detection of fraud.

Auditors and fraud investigators in over 90 countries in 13 languages, use **IDEA** to outperform the expectations of clients, employers and regulators. For more information about **IDEA** and to request a free demo version, visit our website at [www.caseware-idea.com/new](http://www.caseware-idea.com/new).

**Streamline your data analysis with IDEA Smart Analyzer.**

**IDEA Smart Analyzer** is an add-on collection of preprogrammed audit tests and reports that can be run by any auditor with a minimum amount of training. To download a 30-day evaluation version go to [www.caseware-idea.com/smartanalyzer](http://www.caseware-idea.com/smartanalyzer).

IDEA is a registered trademark of CaseWare IDEA Inc.

IDEA significantly improves your ability to detect fraud.
Introducing ACL AuditExchange
A Managed Analytics Platform for the Entire Team

ACL AuditExchange provides a secure and centralized environment for the whole audit team to access data, analyze business transactions and report on audit findings and results. Regardless of source and size, you’ll have access to any type of enterprise data you need. With ACL AuditExchange you’ll be able to create a central audit repository to capture and preserve audit knowledge and results. So, even when people leave, the remaining audit team can continue to efficiently produce consistent, high quality audits.

For 20 years, ACL has been the leading provider of audit technology. Visit www.acl.com/ISACAJournal today for more information on how our latest innovation can help your team:

- Access any type of enterprise data
- Increase productivity by automating audit tests and sharing findings and results
- Share an audit repository across your team, wherever they are

» Find out more at www.acl.com/ISACAJournal
On 24 January 2008 the global financial markets were in the midst of an ongoing crisis triggered by the looming woes of a troubled US economy, the ongoing fallout from the subprime crisis and the spiraling increase in commodity prices. On that same day, Société Générale, a widely respected global French bank, made a shocking announcement that it had lost a staggering €4.9 billion (about US $7.2 billion) from the unauthorized trades of a single trader at its Paris Head Office—by far the biggest loss of its kind in the history of banking.

“Unbelievable. Frankly, I can’t explain it,” said Christian Noyer, governor of the Bank of France, on being asked by the French parliamentary finance committee how Société Générale had failed to detect the multibillion euro fraud.1

One can understand the reaction of the governor of the French central bank. The unfolding drama at the giant French bank had come as a huge shock across the world. Société Générale had long been known for its savvy in complex derivative trading, the quality of its people and the capabilities of its risk management systems. Yet, what it had announced was a colossal fraud in the relatively simple business area of trading on European stock indices—supposedly a low-risk venture where traders with small limits place modest bets, with near matching trades in the opposite direction to offset any downside. What had gone wrong? How could this happen?

Although this was by far the largest loss caused by a rogue trader in the history of the financial services industry, it was only one of a few major cases over the last dozen or so years:

• In 2002, a currency trader at US bank Allfirst, based in Baltimore, Maryland, and then a subsidiary of Allied Irish Bank, pleaded guilty to fraud amounting to US $691 million.
• In 1996, Sumitomo Corp., the giant Japanese trading company, reported a loss of US $2.6 billion in unauthorized copper trading by its chief copper trader on the London Metal Exchange.

None of the above cases, however, comes even close to the drama at Barings Bank in 1995—so vividly captured by Hollywood in the 1999 movie “Rogue Trader.” This is a case that is worth revisiting.

The Barings Bank Meltdown

The collapse of Barings Bank in 1995 is a textbook example of the damage a rogue trader can cause. Over a period of three years, Nick Leeson, a Singapore-based British manager of London’s Barings Bank, lost US $1.4 billion, primarily on futures contract speculation and, by manipulating records, hid his actions until February 1995.

Leeson’s initial responsibilities had not included trading, but it appears that he just assumed control over both the trading floor and the back-office settlement functions soon after arriving in Singapore. He then started his ruinous run of speculative trades, hiding mounting losses in a spurious error account. He claimed that the early trades were conducted to hide genuine losses of his junior traders that he was determined not to report. Later losses, it seems, were concealed in the hope that they would be offset, eventually, by future gains, as well as the desire to protect his job and newfound lavish lifestyle.

Unfortunately, he was not a good trader—far from it—and the losses started to mount beyond any sensible loss limit. In the final days of the saga, almost all the players in the market...
appeared to know about his speculative trades and were successfully betting against him. He was, however, an accomplished liar and succeeded in duping his superiors in London on what was really happening.

When the losses were finally disclosed in early 1995, Barings Bank—the oldest merchant bank in the City of London, the Queen’s personal bank, and the financier of the Napoleonic Wars and the Louisiana Purchase—was forced into insolvency and an ignominious end to its proud and long history.

So how was this tragic ending possible? The report of the inquiry into the collapse of Barings makes it abundantly clear that a few fundamental control failures enabled Leeson to both initiate and conceal his unauthorized activities. This preliminary report identified, among others, the following glaring causes of the debacle:

- Failure of the bank’s management to understand the business they were managing
- Lack of clear lines of responsibility
- Inadequate segregation of duties
- Inadequate internal controls, including independent risk management for all business activities
- Failure to ensure the quick resolution of significant weaknesses identified to management by internal audit or others

Clearly, the rogue trader was guilty of unauthorized trading that resulted in massive loss, but the other failures in internal controls, of the most basic kind, it seems, created an environment where such a fraud, was made possible. As was noted in the debate on the report in the House of Lords:

…The collapse was brought about by the three factors...: firstly, unauthorized and concealed trading by Mr. Leeson; secondly, a total management failure at Barings; and, thirdly, a serious regulatory failure by the Bank of England. The collapse would not have occurred without each of those three ingredients to the fatal brew. The report demonstrates that this unbelievable mess was brought about not just...by a rogue trader, but also by a rogue management and a rogue regulatory system. All three were necessary for the collapse; only one of them is still in place.6

Société Générale and the Biggest Trading Loss in History

In 2000, fresh from business school, Jérôme Kervial joined Société Générale, France’s second largest bank. For about five years he toughed it out in the unglamorous back office of the bank, learning, no doubt, of the bank’s many control practices applied to the trading room and, quite possibly, ways around them.

In 2005, he was promoted to the trading floor, albeit in the relatively low-risk and unfashionable area where European stock market indexes are traded. His work as an arbitrager consisted of the parallel management of two portfolios of broadly similar size and composition, each covering the other and allowing for just marginal positions and modest profits.

Like Leeson before him, Kervial almost immediately engaged in irregular trades by taking open positions and covering them with fictitious matching trades. The size of these unauthorized trades was initially small, but by the end of 2007 the fraudulent trading portfolio had reached around €30 billion. In November 2007, these abnormally large positions prompted one of the clearinghouses to ask Société Générale about the trading strategy of Kervial, but the errant trader was able to explain away these anomalies to his superiors with relative ease. Indeed, his trading positions caught the attention of his supervisors several times in 2007, but he was always able to convince them that the underlying trades arose from an error that could be resolved easily. Ultimately, when the alarm was raised belatedly by the bank’s risk management function on 18 January 2008, the size of the unauthorized positions had reached €50 billion—in excess of the market value of the bank itself! Over the next few days, these unauthorized positions were rapidly liquidated but with a staggering loss to the bank of €4.9 billion—about US $7.2 billion.

Kervial was accomplished, quite clearly, in hiding his deception. Indeed, as one of the senior executives of the bank noted, because the real and fake transactions balanced each other out, “we could not see anything.”5

Although not quite as damning as Barings, the Société Générale case, when fully investigated, will no doubt reveal a similar and troubling breakdown in some relatively fundamental internal controls that should have been in place in any bank’s trading room, such as have been identified in a preliminary government report:5

- Failure to set and monitor gross trading limits held by each trader; apparently, Kervial did not even have a defined gross exposure limit
- Inadequate follow-up by management as and when alarms were raised, particularly when the German-Swiss-operated Eurex alerted the bank about the unusual positions in Kervial’s book
- Lack of independent confirmation of both external and (worryingly) internal counterparties to the trades that had been made
- Failure to review all transactions, or at least voided transactions, executed by each trader
- Breaches in the access control mechanisms—It is alleged that Kerviel sometimes used the login and passwords of his colleagues to conduct fictitious trades.

The bank’s own internal investigation into the massive trading loss “highlights a systemic breakdown in the human chain of control.”6

Lessons Still to be Learned

The initial media coverage on the massive Société Générale loss has focused, understandably, on the rogue trader. Yet, over time, a more considered perspective will show that as much of the blame should rest with the bank’s management and, perhaps, other related parties (such as risk managers and auditors), who collectively failed to implement a robust internal control framework or identify glaring weaknesses. Were such a framework in place, it would have mitigated against, if not
precluded, any potential rogue trader from conducting unauthorized and undisclosed trading activities.

The Société Générale fiasco illustrates that the current preoccupation with governance and risk management frameworks may be superfluous, if even basic internal controls are not in place. This is not to say that there will be no rogue traders in the future. Far from it—there will always be misguided and doomed attempts to surreptitiously outperform the markets. What is necessary, however, is the religious implementation of fundamental internal control policies and practices to guard against this type of errant trader.

Perhaps it is time for those in a position of authority to refocus the risk managers and auditors (internal or external) on the less glamorous, but critical, need for a regular assessment of the adequacy of internal controls, particularly in highly vulnerable areas, such as the trading room of a financial institution. If not, I fear it is only a matter of time before history repeats itself somewhere else, as these types of control flaws are by no means unique to the Société Générale. Otherwise, as a noted 20th century Spanish philosopher wrote: “Those who cannot learn from history are condemned to repeat it.”

Endnotes
1 The Rogue Rebuttal, The Economist, 9 February 2008
3 Lord Eatwell, House of Lords, Daily Hansard Text, 21 July 1995
5 Abstract from an unofficial translation of the “Report to the Prime Minister of France” concerning the lessons from the recent events at Société Générale (publishing source not available), February 2008
7 (Common adaptation from) Santayana, George; The Life of Reason, The Project Gutenberg eBook, www.gutenberg.org

© 2008 Deepak Sarup. All rights reserved.
Clear Guidance in IT Controls

ITAF™: A Professional Practices Framework for IT Assurance—New From ISACA

The IT Assurance Framework™ (ITAF™) is the premier resource for IT audit and assurance professionals. The framework:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments
- Defines terms and concepts specific to IT assurance
- Establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct, and reporting requirements

If you provide assurance over components of IT systems, processes, applications and infrastructure, or if you use IT audit and assurance reports, ITAF will be useful to you!

ISACA members—download your complimentary PDF of ITAF today! Visit www.isaca.org/itaf.
Managing Information Crises

By Steven J. Ross, CISA, CBCP, CISSP

Information security is really pretty simple. There are only three things that can go wrong with information: it can be disclosed when it should not be; it can be destroyed or unavailable when it should not be; or it can be changed when it should not be. Simple, right? Actually, no.

Major Crises, Minor Upsets

There are scales and degrees that differentiate minor and major disclosures, losses and integrity breaches. It is better to disclose a record than a file, and not all files are equally sensitive. It is preferable to lose a file than a data center, and it is better to breach the integrity of a data entry than a database. However, the fact that a single record can be disclosed is indicative of a security vulnerability. If one record can be disclosed when it should not be, there is a failure—technical, procedural or managerial—somewhere in the system of control that might be exploited the next time to much more devastating effect. Of course, the same point can be made about loss of information or a violation of its integrity.

There are hoary tales in which an intrepid investigator follows the trail of a small discrepancy back to a major ring of hackers and, often enough, they are true.1

At the other extreme, there are large, impossible-to-miss security incidents. If proprietary personal information shows up in the newspapers, that is serious. It is serious when a data center burns down and all data are lost. It is a matter of great concern if bank records are hacked and balances changed. The ideal of security is to make sure that these things never happen. The reality is that sometimes they do; a certain part of security deals with what to do when bad things happen to good information.

The response to these incidents falls under the rubric of crisis management. There is an indistinct point at which an incident becomes a crisis. A fair way of describing that point is when the effects of an incident go beyond the ability of an organization to contain it. If civil authorities are notified or regulators are alerted, then it is a crisis.

If one record can be disclosed when it should not be, there is a failure—either technical, procedural or managerial.

Similarities and Differences Between Logical and Physical Crises

In many ways, crises involving information are no different from those concerning buildings or people or materials. Management must take action to protect a company’s reputation, revenue and customer interests in either case. The organization must mobilize, communicate, analyze, communicate, repair and communicate. In one way, information crises are less serious than the physical sort; it is unlikely that anyone would die. Research has shown that companies face their greatest challenge in responding to crises when there are fatalities, and, if management is not nimble, caring and responsive, the effects on the organization can be severe.2

On the other hand, the loss, disclosure or misuse of information strikes at a core value of every commercial enterprise: trust. Thus, companies must take these sorts of crises just as seriously as physical events. The phases of managing any crisis do not begin with an incident nor are they finished when the incident is over. But information crises, I submit, must be handled differently.

An organization should accept the fact that, at some time, a negative event involving its information may occur. When a building burns down, the fact is evident. When information is misused or disclosed, it may not be so clear and the first course of action is to determine the extent of the damage. This may require extensive investigation, albeit at a time when time is at a premium. The security skills needed to evaluate the amount, nature, sensitivity, criticality and value of the affected information are different from those needed to implement an access control system or monitor logs. Personnel need to be prepared in advance and perhaps providers of specialist services need to be identified and kept on retainer. Preparation is not everything, but it is a lot.

In that same vein, there ought to be a documented plan for how an organization will respond if an information crisis occurs. It is much like a disaster recovery plan, except the disaster is logical instead of physical. I have written in the past that the interests of business continuity and information security are convergent.3 In no case is this more evident than in preparation for the business response to an incident involving information. A hack, a virus or a denial-of-service attack may have the effect of halting business operations. A senior-level crisis management team that is not versed in the demands of dealing with a technical incident is likely to either panic or abdicate control. Developing a plan that can be tested and improved over time will result in a smoother, more coordinated response.

Roles and Responsibilities

The focus of responsibility falls on the chief information officer (CIO) and the information security professionals, rather than the facilities manager and the guard staff. The
The scope of preparation incorporates the range of information security measures—authorization, identification, authentication, access control, encryption, accountability—and includes specialized activities in forensics, restoration, and even law and labor relations.

Technical personnel have the responsibility to diagnose the problem and determine the appropriate solution. All the while they must communicate with senior and business function management and often, through them, with customers and the public. A crisis involving information surely has business effects and many constituencies need to be informed and reassured. However, the technical skills needed to resolve an incident generally do not include crisis communications—a specialized skill in itself. Assuming that a business continuity plan exists and includes communications preparations, the IT personnel dealing with the sort of event discussed here should have designated spokespeople to deal with internal and external audiences, rather than putting the CIO, for example, in front of the media. No slur intended on CIOs, but they would have more pressing priorities at that time. Communications specialists should do the communicating.

**Crisis Aftermath**

Eventually, all crises end. However, they do not always end with positive results. The aftermath of an information crisis is trickier than a physical one. If a factory burns down, it is possible to valuate the property and its revenue-producing potential. It is not nearly as clear what the direct and indirect costs might be of a loss or disclosure of information. Without a reckoning, it is difficult to place insurance claims or defend litigation. These follow-up activities are just as much a part of crisis management as putting out the flames, literally and figuratively. One of the smartest ploys is to make certain that an organization has the necessary insurance for negative events involving information, with appropriate limits and retentions. Crisis management both precedes and follows events; companies should anticipate with insurance and follow up with detailed records supporting claims according to previously agreed-upon formulae.

Crises happen. That is life, and that is business as well. The important point is to accept and anticipate that fact. Information crises should not happen, but they do, and management, in particular IT management, should take as much preventive action as practical. Alas, they must also recognize that in time these measures too will fail. What is necessary is a crisis management program when there is no crisis…and then when there is. Information crises call for skills that must be developed; an information security professional with innate talent in this area is rare.

But there is a payback even when there is no critical incident. It is my contention that the skills needed to manage big crises have applicability to small ones. And, organizations that can deal with day-to-day tribulations will prove to be more successful. That is a subject best explored in another column.

---

**Endnotes**

1. For example, see Stoll, Cliff; *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Doubleday & Co., 1989. (Nearly 20 years old counts as hoary in our accelerated age.)
2. Knight, Rory; Deborah Pretty; *Protecting Value in the Face of Mass Fatality Events*, Oxford Metrica, 2005
4. Government agencies rarely buy insurance. The idea is they self-insure and only spend public monies when they have a need. The issues of crisis management in the public sector, therefore, take on a different coloration, beyond the scope of this column.

*Steven J. Ross, CISA, CBCP, CISSP* is a director at Deloitte. He welcomes comments at stross@deloitte.com.
Tommie W. Singleton, Ph.D., CISA, CITP, CMA, CPA
is an associate professor of
information systems 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 information
systems (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
southeast 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
publications on fraud, IT/IS,
IT auditing and IT
governance have appeared in
numerous publications,
including the Information
Systems Control Journal.

**What Every IT Auditor Should Know About Access Controls**

One of the more pervasive concerns of IT audits, whether associated with financial audits or not, is the risk associated with IT general controls, such as access control. The increased usage of databases, the growth of access points on networks (especially remote connectivity) and wireless technologies have increased dramatically the risk associated with networks and access control. Once a person has gained access to a system, that person could potentially access data, financial reporting data, applications (e.g., journal entry software) and other high-risk functions. While each entity must be analyzed according to its individual characteristics, virtually all entities subject to audits have some risk associated with access control.

The most basic principle in assessing the sufficiency of access control is to verify the alignment of the level of protection (sophistication) of access controls with the level of risk; that is, the more risk, the stronger the controls should be. It is becoming increasingly necessary to test more IT controls due to Sarbanes-Oxley requirements, the American Institute of Certified Public Accountants (AICPA)’s Risk Suite requirements and increased reliance on IT controls. This article demonstrates one methodology to assess the appropriateness of access controls using risk assessment, assess controls evaluation, and assess access control tests.

**Authorization vs. Authentication**

The first area of understanding regarding access controls is the difference between authorization controls and authentication controls. Authorization controls basically provide the functionality to verify that a certain combination of ID and password has been granted authorization to access the network. Hopefully, that ID/password also has been granted access to a limited number of files, applications, or data and appropriate access rights (read/write permission) via some network technology. Authorization is the cornerstone of access controls, and absolutely necessary, but it should not be the only access control, except in the most basic of systems and circumstances (e.g., small companies, simple systems or low-risk situations). The key to the authorization aspect of access control is whether or not the entity employs best practices for password policy.

Authentication becomes the second aspect, and more powerful in terms of mitigating risk. Authentication verifies that the login (ID/password) belongs to the person who is attempting to gain the access, i.e., users are who they say they are. Some examples include swipe cards, smart cards, USB devices, temporary PINs, specific and private information, and biometrics. There are various ways to implement a control with this objective, but there are times that the IT auditor would want to verify that some control for authentication exists (e.g., higher risk).

**Measuring the Level of Risk**

Most of the auditing profession today, regardless of the type of audit, uses a risk-based or top-down approach to the audit. The IT auditor will want to assess the level of risk associated with access controls, and the IT auditor working on a financial audit will probably limit the evaluation to risks associated with material misstatements, financial reporting, and financial data associated with risks of unauthorized access. That level of risk is escalated by a variety of circumstances.

One of the issues is the size of the system(s) under review. Size is measured by the sheer number of workstations, servers and network components. Typically, smaller systems are found in smaller entities. Smaller entities have fewer resources for segregation of duties and IT staff. Usually this inherent constraint has a negative impact on the strength of the system of internal controls, especially automated or IT-dependent controls. Therefore, the smaller the size, the
more likely the IT auditor would assess access control risk at a higher level. That is not to say that large, complex systems, such as enterprise resource planning (ERP), do not have inherent risks as well—some most certainly do. But the risk associated with large ERP systems is more a function of complexity than size (number of users).

Complexity, or sophistication, of the systems under review is correlated to risk—the more complex, the more risk, generally speaking. If all of the systems are the same platform, the risk is lower than if there are multiple systems, especially those affecting financial reporting and data, and different platforms. For instance, in frauds of the past, it is a common factor that fraudsters who have the authority will deliberately use different systems for different aspects of the accounting functions and financial reporting, including pulling data off the various systems into a spreadsheet and producing financial reports from offline spreadsheets in a smoke-filled back room. Thus, generally speaking, the more systems in use, and the more disparate platforms being used, the greater the risk assessed by the IT auditor. Access control across disparate systems is usually difficult to administer.

If the entity has access to the source code, modifies code or generates code, then the access control risk is probably higher. Anytime people can affect the code being generated, there is a relatively high risk of error (which can be mitigated), and usually a moderate risk of fraudulent or malicious code. Therefore, if an entity has its own in-house programmers, the risk is generally higher than one that uses strictly commercial off-the-shelf (COTS) software. Access controls can be thwarted by malicious code.

Other issues relate to specific types of technologies or system architectures that inherently have higher risks. Some of them include wireless technologies, access to the Internet (i.e., the number of access points), shared files and databases, remote access, outsourcing of critical applications or system functions, and changes to infrastructure. These technologies or situations generally complicate the ability of the entity to adequately manage access control.

The outcome of this evaluation process is some level of risk associated with the access controls. Generally speaking, IT auditors like to simplify the assessed risk level as low, medium or high.

### Measuring the Strength of Controls

The IT auditor needs to assess the ability of access controls to mitigate any risk above a certain level. The controls should be based on the level of risk/sophistication of the system. That is, the greater the risk, the stronger the controls should be. The IT auditor needs to be careful to not oversimplify audit procedures, i.e., simply verify that authorization controls exist for logins and network access without regard to overall risk.

One common way of developing an effective IT audit procedure is to compare best practices of the object being audited against the practices being employed. For example, what are the best practices of access control and passwords? The IT auditor could use those best practices to evaluate the effectiveness of access controls at the level of login, and passwords in particular. **Figure 1** provides some of the generally accepted best practices for password policy, and the metric is generally considered to be the best way to structure that aspect of passwords (however, these are not absolutes). This list of best practices and metrics provides the IT auditor with a road map toward assessing the level or strength of password-policy practices.

![Figure 1—Best Practices for Password Policy](image)

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Automatic change of password time frame</td>
<td>Every 90 days, or some regular period</td>
</tr>
<tr>
<td>2. Ease to crack—strong password</td>
<td>• 8 characters or more</td>
</tr>
<tr>
<td></td>
<td>• Mix of upper case, lower case, numbers and special characters (usually three of these)</td>
</tr>
<tr>
<td>3. Protection, security of the password</td>
<td>• No notes with the login/password on the monitor or under the keyboard</td>
</tr>
<tr>
<td></td>
<td>• Never respond to an unsolicited request for login information</td>
</tr>
<tr>
<td></td>
<td>• Accounts lock after three unsuccessful attempts</td>
</tr>
<tr>
<td>4. Need to know</td>
<td>Access and rights (read/write) limited to user’s view</td>
</tr>
<tr>
<td>5. Limited admin access</td>
<td>Limited number of administrators and strong login (no default logins)</td>
</tr>
<tr>
<td>6. Password termination</td>
<td>Effective immediately upon an employee’s termination/departure</td>
</tr>
<tr>
<td>7. Matching levels of risk to controls</td>
<td>Above low-level, multifaceted access control</td>
</tr>
</tbody>
</table>

If the risk is low, the IT auditor probably has a limited scope and small number of audit procedures used to evaluate the effectiveness of the controls. For instance, the IT auditor could attempt a login of some critical application or the network server and verify that the authorization process is at least working. The access control itself would need to “fit” the circumstances of low risk. That is, a strong password and employment of relevant password policies (see **Figure 1**, numbers 1 and 6) would probably be enough to mitigate a low level of risk.

If the risk is medium, however, the strong password alone would not be sufficient to mitigate the risk. For instance, if the entity is a financial institution with online access to financial accounts, the level of access control risk is probably medium or high because of threats such as identity theft. If an entity allows remote access for its employees, the same result is likely to occur—medium or high risk for access control. At levels above low, the entity should employ multifaceted controls, i.e., combine another access control with the password policy and controls shown in numbers 1-6 in **Figure 1** (a simple authorization process).

One way to accomplish that objective is to have a second login control with a different ID and password for the more sensitive access (e.g., network access is the first level of access, but a second ID and password are required to gain access to the payroll application software). Another way to accomplish that objective is to add something other than a login, e.g., a smart card, temporary PIN or biometric fingerprint.

The common framework for multifaceted access controls is something you know (e.g., ID and password, mother’s maiden name, personal facts), something you have (e.g., smart card, temporary PIN) or something you are (i.e., biometric). Obviously, these controls are listed in order of strength or design effectiveness.
Thus, a bank that is assessed with high level of risk associated with access control, because of online banking risks, and that requires a login (ID and password) and mother’s maiden name for secure login does not employ a level of effectiveness sufficient for a high level of risk associated with online banking; that is, the fit is not appropriate. That level of effectiveness is most likely low to medium at best. But the bank that requires two questions on personal information not easily attained from Internet search engines or other sources has stronger access control, even though the bank uses only the first level of multifaceted controls.

The stronger, more effective, approach is to add a second level of access control associated with the second level of multifaceted controls (e.g., temporary PIN sent via preestablished e-mail account), or even the third level: a biometric control.

The same would be true for a high level of risk associated with remote access and/or wireless access. A temporary PIN provided via a pager device or a smart card would strengthen the access controls to more appropriately fit the level of risk. For a high level of risk, the most effective multifaceted control is a biometric. For example, using a virtual private network for remote access is an effective control for the communications during the online session. But, how does the entity know users are who they say they are? How does the entity authenticate the user?

Therefore, using multifaceted password controls is not the same as having a sufficient authentication control. Many entities will use the private information of a user (college roommate, favorite “fill in the blank,” etc.) as a substitute for authentication, and it may serve adequately as authentication. Likewise, the something the user has may be a surrogate for authentication, but it could be lost or stolen. A biometric is clearly the most effective way to authenticate the user, but not the only way.

Thus, IT auditors use these steps and information to seek alignment between the level of risk and the level of effectiveness of access control in their evaluation and audit procedures.

**Test of Controls**

The IT auditor should be able to develop appropriate audit objectives based on the assessed level of risk, best practices and the principle of alignment. For example, does the entity sufficiently control unauthorized access of high-risk (sensitive) information, data and/or systems?

Next is the matter of how to execute, but execution is more complicated than it sounds. Often access controls and password policy are so spread out in the network system and software that there is no easy way to gather the appropriate information. However, sometimes it is possible to gather it fairly efficiently.

One way to illustrate the step of developing audit procedures is to use the access control information from risk assessments and best practices and assume the entity is using Microsoft Server and Active Directory. The IT auditor can access the network server and conduct some quick and effective tests against the evaluation process and results. Using a utility tool known as Dumpsec, the IT auditor can print out access users and access rights—something more cumbersome without Dumpsec. The Dumpsec tool gathers the users and permissions and creates a table of access from which the auditor can assess the effectiveness associated with such areas as “need to know,” admin access and terminated employees (see numbers 4-6 in figure 1).

For this platform, the IT auditor would also want to dump permissions for shared folders. For instance, if the entity compiles data into a spreadsheet and manipulates them to generate financial reports, the folder containing those files should be restricted to a limited number of authorized employees and certainly not accessible by anyone in the entity. Sharing permissions would allow the IT auditor to evaluate quickly the effectiveness of existing access controls over those sensitive (i.e., high-risk) files.

Also associated with this platform is the ability to review password policies that were established by IT staff. That information can be compared to the best practices in figure 1 to evaluate the number of best practices being employed. That information can be accessed through the “admin” utility and “Permissions for Shares” function.

Perhaps one additional test would be to see if the IT auditor can log onto the network server using one of the default logins, such as (ID) admin and (password) blank. This login is normally considered a high-risk access control because of the global access to permissions and the network. The IT auditor wants to gain some assurance that this login is strong and certainly not a default ID/password, which hackers and crackers know and use to carry out malicious activities.

The results of these tests are fairly easy to gather and evaluate and should enable the IT auditor to do a valid assessment of the effectiveness of access controls.

**Conclusion**

Like most of the audit procedures of today’s audit world, IT audit procedures are risk-based, and IT auditors are assessing the appropriate level and scope of controls associated with the residual risks. Access control is one of the more common areas of IT audit concern. This article shows the basics of assessing the level of risk, assessing the effectiveness of controls, and verifying the level and scope of controls and their effectiveness as to whether they are adequate for the risks associated with access control (fit or alignment).

There are some simple tests of controls that an IT auditor can conduct to gain a reasonable and basic understanding of the nature of an entity’s access controls and password policies. While there are many more issues and concerns with IT audits, these are meant to illustrate some of the common concerns and how to test them at a basic level. Most assuredly, this methodology could be effective for small to midsized businesses, but might be woefully weak for larger entities. However, these represent a good start for any size business.

**Endnotes**

1 One can find these defaults by searching “default logins” in search engines, such as Google. They include admin/administrator/<blank> and admin/administrator/password/<blank>, among others.
Do you know which one of your team accessed your key financials last night?

With Cyber-Ark® you will.

With Cyber-Ark's Digital Vault Solutions, you will know who is doing what with your highly sensitive information, processes and systems and you will be able to prove it.

Does your enterprise’s approach to risk management fully address the challenges around all of your privileged users and most highly sensitive data? Are you sure? Can you prove it?

For instance – do you know who accessed your key financial systems anonymously as the System Administrator last night? Do you know who has the rights to both create and approve a purchase order? Or a speculative financial trade? Are you willing to risk your brand on the integrity of faceless insiders with privileged access to highly sensitive systems, information and processes?

With Cyber-Ark's suite of Digital Vault Solutions, you will always know that your most sensitive systems and information are secure, controlled, and completely managed in a provable, auditable manner.

Cyber-Ark's Enterprise Password Vault® today enables over 300 global enterprises to address their Privileged Identity Management challenges. With the FPV as a core part of their infrastructure, enterprises can now:

- Automate manual processes and reduce IT's workload while serving the overall security and compliance goals.
- Coupled with the powerful Inter-Business Vault® and Sensitive Document Vault™ that create Communities of Trust for securely storing and sharing highly sensitive information within your organization and with your business partners, Cyber-Ark's suite of integrated Digital Vault solutions provides a solid, sustainable and robust solution to address any concerns around Privileged users and Highly sensitive information raised in SOX, PCI, Basel II, HIPAA and other regulations and IT frameworks.

So if your organization needs to know the who, what, where and when, then come and talk to us. After all the last thing your business needs is “15 minutes of fame”.

For further information on Cyber-Ark's Digital Vault solutions visit
www.cyber-ark.com/ISACA108
or call Cyber-Ark Software on
888 808 9005

Cyber-Ark®
The Leader in Privileged Identity Management Solutions
Celebrating 30 YEARS
The Nation's Premier Recruiting Firm for the Audit Profession

LANDER INTERNATIONAL, LLC

Honesty Integrity Ethics

The strongest audit departments around the world depend on Lander International to find the talent they need.
The best auditors trust Lander International to find them premier career opportunities.

(800) 548-5318 in USA and Canada
(510) 232-4264 International
www.landerint.com
The titles of issued documents follow.

IS Auditing 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

IS Auditing Guidelines
G1 Using the Work of Other Auditors and Experts Effective 1 March 2008
G2 Audit Evidence Requirement Effective 1 May 2005
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 2007
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 March 2000
G10 Audit Sampling Effective 1 March 2000
G11 Effect of Pervasive IS Controls Effective 1 March 2000
G12 Organisational Relationship and Independence Effective 1 September 2000
G13 Use of Risk Assessment in Audit Planning Effective 1 September 2000
G14 Application Systems Review Effective 1 November 2001
G15 Planning Revised 1 March 2002
G16 Effect of Third Parties on an Organisation’s IS Controls Effective 1 March 2002
G17 Effect of Non-audit Role on the IS Auditor’s Independence Effective 1 July 2002
G18 IT Governance Effective 1 July 2002
G19 Irregularities and Illegal Acts Effective 1 July 2002
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 August 2003
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 Reengineering (BPR) Projects 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

IS Auditing Procedures
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 2006
P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

Standards for Information System Control Professionals Effective 1 September 1999
S10 Statement of Scope
S10.010 Responsibility, Authority and Accountability
S10.100 Professional Independence
S10.200 Organisational Relationship
S30 Professional Ethics and Standards
S30.010 Code of Professional Ethics
S30.020 Due Professional Care
S40 Competence
S40.010 Skills and Knowledge
S40.020 Continuing Professional Education
S50 Planning
S50.010 Control Planning
S56 Performance of Work
S56.010 Supervision
S56.020 Evidence
S56.030 Effectiveness
S570 Reporting
S570.010 Periodic Reporting
S580 Follow-up Activities

Code of Professional Ethics Revised May 2003

ISACA 2007-2008 Standards Board
Chair, Ravi Muthukrishna, CISA, CISM, FCA, ISCA, Capco IT Services
India Pte. Ltd., India
Brad David Chin, CISA, CPA, Google Inc., USA
Sergio Flegensky, CISA, AKZO Nobel, Uruguay
Maria Gonzalez, CISA, CISM, Department of Defence, Spain
John Ho Chi, CISA, CISW, CBIP, CFE, Ernst & Young, Singapore
Andrew J. MacLeod, CISA, CIA, FCPA, MACS, PCP, Brisbane City Council, Australia
John G. Olt, CISA, CPA, AmtersourceBergen, USA
Jason Thompson, CISA, CIA, KPMG, USA
Meera Venkatasesh, CISA, CISI, ACS, CISSP, CWA, Microsoft Corp., USA
Five Steps to Introducing Val IT:
Applying Val IT to Introduce or Improve Value Management in an Enterprise.

By Sarah Harries and Peter Harrison, FCPA

This is the second of six articles to be published in this column on the practicalities of introducing and establishing Val IT. The first was published in volume 3, 2008. These articles draw from the authors’ many years of experience working with enterprises to introduce value management.

The remainder of the series will cover:
• Practical Guidance on Establishing Value Governance
• The Challenges of Implementing Portfolio Management
• Benefits Realisation and Programme Management—Beyond the Business Case
• Critical Success Factors for Introducing Val IT

Introducing or improving value management practices in an enterprise is not an easy task, and will take time. It may require significant change in terms of executive thinking and action around decision making, value and accountability. However, this should not deter enterprises from taking action—action that must balance achieving the longer-term vision with realising near-term value by taking an incremental approach within the context of an overall vision and plan.

This article describes five basic steps needed to introduce value management successfully using the Val IT framework. Identification of these five steps comes from experience working with many different enterprises over more than a decade. Key to success is to take a measured and structured approach with a focus on incremental change.

The five steps are defined in the following sections and in figure 1.

Looking at each of these steps and focusing concentrated effort on the first two steps will draw out the activities required for the remaining steps.

Step 1—Define the Journey

The first step is to work out and get agreement as to the journey or plan to introduce value management and Val IT thinking and practices into the organisation—articulate what must be achieved and what needs to be done to get there.

This includes the following:
• Create the vision. Establish a clear picture of what will be achieved with value management. What is the ideal future state? How should things look in one year? In three years? What are the consequences of not doing things in the new way?

• Assess the current governance around IT value management. How do enterprise and IT governance relate? Assess the organisation’s capability and readiness for the acceptance of business governance of IT-enabled investments.

• Enlist the support of the most senior executive possible. Determine who ‘owns’ value in the organisation, or who owns the ‘problem’ of value delivery and leakage from IT-enabled investments. Get them to own the goal and vision of value management. Start informing other senior executives about value management and what effect improving it would have on their roles in the organisation. Focus on how the pain points they are suffering will be improved.

• Document the change programme the enterprise needs to undertake to achieve the desired level of value management maturity. Quantify and justify the financial investment needed to establish and sustain value management—essentially developing a business case. Identify how any adverse change impacts and inhibitors will be addressed, e.g., overcoming subjective or defensive views on organisational decision making.

• If necessary, seek help for the journey. A recent international survey of organisations introducing frameworks concluded: ‘Implementing process frameworks straight “out of the box” isn’t going to work very well for you…. Getting help from people who have been there before is likely the best advice that I can give you’.

Step 2—Select a Starting Point to Assess Appetite and See What Will Work

Getting practical and demonstrated value from the application of Val IT and the Val IT management practices is the next step. People may accept the theory but ask: ‘So how would that improve things for us, specifically? We are unique’.

The new Getting Started With Value Management guide from the Val IT series Enterprise Value: Governance of IT Investments identifies a number of common pain points or ‘trigger’ points (such as questioning the value of IT, a major investment failure or a change in funding) that can indicate the most logical starting scenarios in introducing
value management using Val IT. These starting scenarios include:
• Building awareness and understanding of value management
• Clarifying the value of individual investments
• Implementing or improving governance
• Undertaking an inventory of investments

The starting point has to be one where success will bring visible value to the organisation. It makes sense to start with the point that is giving the executives the most pain, as demonstrating a quick win here will help greatly in engaging senior stakeholder support for more widespread changes. Success will be achieved when senior executives are comfortable that the organisational changes arising from the introduction of value management will bring enterprise value. Those sitting on the fence or doubtful of the benefits will feel more comfortable throwing their hat into the ring once benefits of the approach have been proven.

**Step 3—Define and Grow Internal Capabilities**

Investment will probably be required to introduce or extend current internal capabilities for value management. This requires an investment of at least time in the areas of executive, management and staff training and awareness. It is possible that expertise may need to be brought in to support changes in governance structures and processes, information needs, templates, and possibly tools—all the things needed for the change programme to succeed.

**Step 4—Operationalise the Governance Capability**

Once the starting scenario(s) outlined in step 2 has been introduced, it needs to be operationalised within the organisation. Again, this is best done on an incremental basis. The change programme for introducing value management needs to identify and drive the adoption into the most valuable areas for the enterprise first. This will smooth the way for the lower-level, behind-the-scenes changes needed to operationalise the improvements. This may include revising templates such as business cases and board remits.

**Step 5—Continuously Improve Capabilities**

The introduction of value management is a journey of possibly a year or more. Lessons from the previous steps need to be reflected in a continuous improvement process for value management. The framework must have an accountable owner, and regular reviews of its suitability must be conducted, at least annually, preferably at least every six months.

Further, the sustainment of value management requires investment in the maintenance of capability, e.g., the inevitable staff turnover and the loss of knowledge. This applies to stakeholder turnover as well as turnover amongst the owners of the value management approach.

**Conclusion**

In summary, introducing value management using the Val IT framework thinking, principles and management practices can be illustrated in the steps and actions described in figure 1.

---

**Figure 1—Steps to Introducing Value Management**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Key Actions</th>
</tr>
</thead>
</table>
| Step 1: Define the journey. | • Enlist senior executive support.  
• Understand current and target maturity.  
• Develop a change programme. |
| Step 2: Select a starting point to assess appetite and see what will work. | • Adopt starting scenarios where value can be maximised and delivered quickly.  
• Ensure that senior executives see the value. |
| Step 3: Define and grow internal capabilities. | • Invest in awareness and education, governance structures and processes, information needs and tools, etc. |
| Step 4: Operationalise the governance capability. | • Adopt an incremental approach. Make use of regular cycles. |
| Step 5: Continuously improve capabilities. | • Adopt lessons learned from steps 1 through 4. |

Readers are encouraged to review Val IT, as described in Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0 and Enterprise Value: Governance of IT Investments, Getting Started With Value Management, and share them with key governance stakeholders within their enterprises.

Sarah Harries was with Fujitsu Services (UK) until 2008, specialising in value management (VM). She also chaired Fujitsu’s global VM community of interest. She is now benefits realisation manager at Openreach, a BT Group business.

Peter Harrison, FCPA is a principal and member of the Enterprise Value Management leadership team within Fujitsu Consulting Australia and New Zealand, and is a member of the Val IT Steering Committee.

**Editor’s Note:**

The publications of the Val IT project can be downloaded free from the ITGI web site, www.itgi.org, and include: Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0; Enterprise Value: Governance of IT Investments, Getting Started With Value Management; Enterprise Value: Governance of IT Investments, The Business Case; and Enterprise Value: Governance of IT Investments, The ING Case Study. Please visit www.isaca.org/valit or contact Brian Selby at bselby@isaca.org for further information regarding Val IT.

**Endnotes**

Streamline the audit process
Improve audit visibility
Increase audit efficiency & productivity
Leverage assessments by other GRC groups

SAVE TIME, CONDUCT BETTER AUDITS

INTERNAL AUDIT SOFTWARE • THINK PAISLEY

Internal audit software from Paisley includes features for risk assessment, planning, scheduling, workpapers, reporting, issue tracking, time and expenses, quality assurance and personnel records. It is part of a comprehensive governance, risk and compliance solution that also includes functionality for financial controls management, compliance, risk management and IT governance.

Join over 1,300 leading organizations that utilize software from Paisley to increase efficiencies, reduce costs and improve the overall quality of financial, IT and operational audits.
Ray Slocumb is the US leader of the systems and process and assurance (SPA) practice of PricewaterhouseCoopers (PwC), managing more than 1,600 professionals in the areas of IT control, IT internal audit, risk management, enterprise resource planning (ERP) controls, business process, security and technology.

With more than 22 years of experience in the profession, he has led various IT internal audit, systems technology and business process projects on all technical platforms, including mainframe, client-server, network and web-enabled environments. He has performed work on US Sarbanes-Oxley Act section 404 projects, as well as system applications such as SAP, Peoplesoft, Lawson and Oracle. He also serves as engagement partner for various clients in the Houston, Texas, USA, market.

In addition, Slocumb frequently speaks at professional organizations around the country on a variety of topics, including Sarbanes-Oxley legislation, security, business continuity planning and leadership. In his spare time he enjoys going to the beach, playing golf, fishing and playing the piano.

**Question**

You have experience in IT audit and information security. What bridges do you see between IT auditors and security professionals?

**Answer**

I see much common ground between the two professions. IT auditors must know and understand what security controls should be in place to have a well-controlled systems environment. They have to know what to review and what to look for when assessing security controls. Similarly, security professionals must know what sort of controls should be in place to protect their organization, and they must have a solid understanding of what the auditors will be looking for in an audit.

In my mind, the most well-controlled organizations have IT auditors and security professionals working together to understand the security risks that exist and the security controls that should be in place based on those risks. Having said that, IT auditors need to remain independent in their approach to assessing security controls and not have ownership in implementing security.

Looking ahead, I see IT auditors and security professionals continuing to be linked, for example, obtaining common certifications such as Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), etc. In fact, I have seen several instances now where security professionals have become IT auditors and vice versa, and are adapting well to the new field because of their strong IT controls experience.

As a partner in a Big 4 firm, I can tell you that we have had much success in recruiting security professionals, not only to execute security diagnostic reviews for our clients, but also to become well-versed IT auditors. So I definitely see a strong linkage continuing to evolve over time between IT auditors and security professionals.

**Question**

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

**Answer**

Sarbanes-Oxley, the Public Company Accounting Oversight Board’s Auditing Standard (AS) No. 2 and No. 5, and other regulatory standards have had a very significant impact on the IT auditor in the US. This stems from both the sheer scope of work that is now required, with regard to reviewing controls, and the level of technical knowledge needed regarding IT systems.

We are also seeing a greater demand for IT auditors because of these regulatory changes. In fact, there seems to be a shortage of them throughout the country. This has spawned a real increase in the number of individuals wanting to enter the profession and take the CISA exam, as well as the number of regular auditors or IT professionals converting to the IT auditor role.

However, while there has been a steep increase over the past five years, there is a leveling off right now related to financial reporting internal controls due to AS No. 5.

As I look ahead, I see continued regulatory involvement spelling more work for the IT auditor. Aside from Sarbanes-Oxley, new standards, regulations and/or regulatory bodies are increasingly centering on specific industries—such as the North American Electric Reliability Corporation (NERC) cybersecurity standards for utilities, and the Payment Card Industry (PCI) security standard for the retail consumer industry—and there will be more coming our way.
Question
What trends in IT audit and controls are you seeing that will be impacting business in the near term?

Answer
There are several key trends shaping the market right now. Certainly, the impact of new Extensible Business Reporting Language (XBRL) reporting requirements necessitates that the IT auditor understand the controls in place around XBRL reporting.

Also, as I mentioned earlier, I do see an increase in regulatory bodies requiring more compliance in specialized industries and sectors. Of course, companies will find it imperative to win the confidence of their consumers/clients, business partners, regulators and/or other interested parties with which they interact, and will need to work to meet those mandates.

Companies are continuing to go global, and business models increasingly incorporate shared services, offshoring and outsourcing solutions. So the controls around data exchange, across country borders and within companies alike, are critical. Organizations will need to make sure controls are in place, even though they are outsourcing to another entity across the ocean, so they can continue to provide consistent, high-quality services. They will also need to manage and mature their controls model overall, while justifying their investment in IT controls systems.

What all of this says to me is that the IT audit profession is alive and well. And it will continue to grow and present many opportunities for those interested in engaging in it.

Question
How do you believe the certifications you have attained have advanced or enhanced your career? What certifications do you look for when hiring new members of your team?

Answer
I believe that certifications say a lot about a person’s ability. All things being equal, a prospective employer will be more interested in a person with a certification (or more than one) than one without. It is certainly something I take into consideration when looking at résumés or considering a person for an interview. Having said that, certifications alone do not make you well versed; certifications combined with solid experience are a great differentiator.

I continue to encourage all of the professionals in my practice and in PwC to sit for their exams. Even if they do not realize it at the time, certification will help them for years to come in their career.

The certifications I look for relating to the audit profession are: Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Public Accountant (CPA), Certified Internal Auditor (CIA) and Certified Fraud Examiner (CFE).

Certifications say a lot about a person’s ability.

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

Answer
I faced a great challenge three years ago when I moved into the US lead position at PwC for systems and process controls. I went from leading 300 professionals in my regional post to 1,600 professionals nationwide.

It was a very different dynamic from what I was used to, in many ways. From the market perspective, I needed to work to understand the demand for controls services in the various US markets. From the people perspective, I had to learn how to work effectively with the styles and abilities of my own leadership team in order to move us forward toward success.

The key challenge for me as a leader has been making decisions that have huge impacts, as they trickle down through the organization. I am very mindful that every decision I make has a real effect on real people and their families. Regardless of whether you are leading through good times or bad, you have to put the face of leadership on every day and lead through it.

So the way I have worked to overcome this challenge has been to learn to ask for advice from the leaders around me; seek to understand all the facts before making a decision; and learn how to listen, as opposed to delegating decision making or thinking that I have all the answers.

I have also made it a point to learn from my mistakes. This has been a key part of my personal growth in this role, and I believe it to be an important part of the journey for everyone.

Additionally, I have worked hard to get to know as many people in the practice as I possibly can. I try to understand their concerns and address their questions. I try to find out what is enjoyable to them in their career path, and what it is they want to do so that, together, we can develop a very strong team.

I want people to grow and stay here, and to love their job. If someone is not happy, I take it personally and work to see what I can do to address the situation.

My goal is to take the systems and process controls team from where we were when I started as leader three years ago, and continue to move them up to the next level, which is a real challenge to do when you have a high-performing team.

At the end of the day, I really love what I do. The greatest enjoyment I get is working with great people, especially when I know I have played a small part in their development.
New Framework for Enterprise Risk Management in IT

By Urs Fischer, CISA, CIA, CPA Swiss

As enterprises increasingly rely on IT to succeed, effective management of business risk has become an essential component of IT governance. Leading the drive to help organisations mitigate risks, the IT Governance Institute® (ITGI™) is developing the IT Risk Management Framework. The intended audiences for the benefits related to the adoption of the framework include risk managers, IT management, IT security and service managers, chief financial officers (CFOs), business management in general, internal/external and IT auditors, and regulators.

Why Is It Important?

ITGI has identified a gap in the current array of risk management frameworks for IT: there is no known framework that includes both a holistic look at risk management and, at the same time, provides adequate depth and detail when covering IT.

Therefore, the new risk-oriented framework, expected to be available by the end of 2008, will round out ITGI’s full coverage of IT governance by covering the risk management component. The other four focus areas of IT governance—strategic alignment, value delivery, resource management and performance measurement—are addressed by ITGI’s other two internationally tested and globally adopted frameworks: Control Objectives for Information and related Technology (COBIT®) and Val IT™.

“Recent research published in the IT Governance Global Status Report—2008 found a 6 percent increase from 2005 in the importance of IT to business strategy,” said Lynn Lawton, CISA, FBCS CITP, FCA, FIHA, PIJA, international president of ITGI and ISACA. “This clearly shows that management of IT-related risks is increasingly vital for enterprises around the world. ITGI’s risk framework will provide clear guidance that business and IT managers can use to help protect their organizations.”

The IT-ERM Task Force oversees the development planning and progress of ITGI’s IT Risk Management Framework initiative. The task force is made up of highly professional people who are representing the intended audience and are experts in the relevant subject matter (i.e., IT-related risks). The members are also familiar with ITGI’s other major product offerings.

What Will It Cover?

The framework aims to fill the gap between generic risk management frameworks such as the Committee of Sponsoring Organisations of the Treadway Commission (COSO)’s Enterprise Risk Management (ERM) and Australia/New Zealand AS/NZ 4360, and detailed (mostly security-related) IT risk management frameworks. Indeed, the goal of this framework is to allow organisations to understand and manage all IT-related risks (beyond security) and to address all aspects (beyond operational management of IT) when managing risk.

The current ITGI frameworks’ material and concepts are leveraged to the maximum possible extent. Indeed, ITGI wants to create a coherent set of frameworks aimed at providing the user with best possible guidance on IT governance. The IT-ERM Task Force has analysed a large number of already established and existing standards and frameworks for concepts and components that could be reused, knowing that it would not make sense to reinvent already existing and good material. The use and benefit of ITGI’s new framework lies in the fact that it will not be cast in stone, but will evolve over time, taking into account new ideas, evolving technologies and organisational theories.

It will be complemented with additional guidance to help the risk management practitioner to the maximum extent possible. Many of the existing frameworks have a focused view on risk, e.g., addressing security risk. This framework is meant to address all IT-related risks at each level throughout the enterprise, i.e., starting from strategic risk down to operational risk.

Like COBIT and Val IT, the new risk framework will be vendor-, application- and platform-neutral. It is not focused on any particular legislation or regulation, but will instead consist of internationally accepted good practices for the identification, assessment and mitigation of IT risk across an enterprise.

Benefits and Outcomes

The IT Risk Management Framework will cover the following requirements of the intended audiences:

1. A need to have an accurate view on current and near-future IT-related risks throughout the extended enterprise and to determine how well the enterprise is addressing these risks
2. A need for end-to-end guidance on how to manage IT-related risks, beyond the purely technical control measures and beyond security
3. Understanding of how to capitalise on investment made in an IT internal control system already in place, to manage IT-related risk
4. A need, when assessing and managing IT risk, to integrate with the overall risk and compliance structures within the enterprise
5. A need for a common framework/language to help manage the relationship between the chief information officer and enterprise risk management

The IT Risk Management Framework initiative includes:
• A risk management framework that provides the missing link between ERM and IT management and control, fitting in the overall IT governance framework of ITGI and building upon all existing risk-related components within the current frameworks, i.e. COBIT and Val IT
• A number of related services and products (including practical guides, reference data, interfaces/mappings with other standards, etc.)

Urs Fischer, CISA, CIA, CPA Swiss
is the chairman of ITGI’s IT-ERM Task Force. Fischer is head of IT governance and risk management within the SwissLife Group. Previously, he worked as head of IT audit for SwissLife’s audit department based in Zurich, Switzerland. Since 1989, he has worked in the IT audit and security areas and has extensive audit and information systems security experience, especially in the finance and insurance area. He is on the board of the ISACA Switzerland Chapter and has volunteered on the Programme Committee for six EuroCACs conferences. He is a member of ISACA’s Assurance Committee and ITGI’s COBIT Steering Committee.

Editor’s Note:
More information on the IT Risk Management Framework will be posted at www.itgi.org as it becomes available.
CISA Review Manual 2008

ISACA

The CISA® Review Manual 2008 has been completely revised and updated with new content to reflect changing industry principles and practices, and is organized according to the current CISA job practice areas. The manual features detailed descriptions of the tasks performed by IS auditors and the knowledge required to plan, manage and perform IS audits. The new edition also features new case studies to assist a candidate’s understanding of current practices. Also included are definitions of terms most commonly found on the exam, practice questions similar in content to what has previously appeared on the exam and references to additional study materials on specific topics. 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 2008 edition has been developed and is organized to help prepare the CISA candidate in studying the following job practice areas:
- The 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


ISACA

The CISA® Review Questions, Answers & Explanations Manual 2008 consists of 600 multiple-choice study questions that have previously appeared in the CISA® Review Questions, Answers & Explanations Manual 2006 and the 2007 Supplement. 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 to provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, but are intended to provide the CISA candidate 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 2008.

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

CISA Practice Question Database v8

ISACA

The CISA® Practice Question Database v8 combines the CISA Review Questions, Answers & Explanations Manual 2008 with the CISA Review Questions, Answers & Explanations Manual 2008 Supplement into one comprehensive 700-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 the user’s previous scoring history, allowing CISA candidates to easily and quickly identify their strengths and weaknesses, and focus their study efforts accordingly. Other features allow the user to select sample exams by specific job practice areas, view questions that were previously answered incorrectly and vary the length of their study sessions. Also included are Information Systems Control Journal articles referenced in the CISA Review Manual 2008. The database is available in CD-ROM format or as a web site download.

PLEASE NOTE the following system requirements:
- Intel Pentium 3 or higher (Pentium 4 recommended)
- Windows 98SE or higher
- 256 MB RAM (512 MB recommended)
- Hard drive with 225 MB of available space
- CD-ROM drive
- Display with recommended resolution of 1024 x 768

The CISA Practice Question Database v8 is licensed for installation on one computer only for personal, noncommercial use.

To order CISA review material for the December 2008 exam, see the order form on page S-8 in this Journal or visit www.isaca.org/cisabooks.
There is a plethora of information and literature available on the security of IT networks, specifically data-only networks. To a lesser extent, there is also guidance available on new communications technology, such as Voice-over Internet Protocol (VoIP). However, thought leadership on the risks associated with the fusion between the two—that is, information and communications technology (ICT)—is relatively scarce. 

Securing Converged IP Networks attempts to address exactly that: security risks and treatment concepts peculiar to technologies that are converging through the Internet Protocol (IP).

Convergence obviously began with the emergence of the Transport Control Protocol/Internet Protocol (TCP/IP), which, over time, virtually dominated legacy protocol suites such as Novell’s SPX/IPX, Banyan and X.25. Encapsulation of voice data into IP packets led to VoIP. As the benefits of convergence on a single platform have arisen, there has been increasing pressure to converge due to cost, functionality and efficiency.

This book should attract a wide range of audiences, including risk managers, auditors, legislators, regulators, equipment manufacturers and C-level executives. Unlike many other publications, this book goes beyond simply citing potential audiences and identifies which portions are relevant to each audience and to what extent (“need to know,” “important,” “useful” or “not core”).

This book is timely for those in industries that are experiencing or driving convergence, such as telecommunications, utilities, manufacturing, media and entertainment. It is designed for people who want to understand what has changed security-wise under convergence and is not intended to be an ICT security primer. It is assumed that the reader is familiar with the basic concepts of firewalls, security policies and IP.

The book argues that the same tools and techniques used to manage the security of data-only networks also apply to converged networks, but a different philosophy is required in managing the security risks associated with converged networks.

Its argument is based on the premise that the sensitivity of a converged network to security risks is higher than the sum of sensitivities of individual assets on the converged network. This is different from the portfolio view of risks, which holds that, due to the possible correlation between risk events, combined sensitivity is equal to or less than the sum of the sensitivities of the individual assets. It is an interesting proposition and one would need to read the book to appreciate it.

The book starts with an explanation of the drivers behind IP convergence and the concept of converged sensitivity. A discussion of threats and vulnerabilities peculiar to converged IP networks follows. Some threats mentioned in this section are novel and insightful in the context of converged networks.

A discussion of controls and safeguards for converged network security follows and looks at the delta between data-only and converged networks. Although the discussion draws on tools and techniques already in use in data-only networks, such as secure network design and encryption, this chapter focuses on how these controls can be implemented to mitigate risks in a converged environment.

The book tackles the process of managing assurance for converged networks and references the use of quantitative and qualitative metrics for measuring security and maturity models such as Control Objectives for Information and related Technology (COBIT) from the IT Governance Institute (ITGI), Security Engineering Institute’s Capability Maturity Model (SEI CMM), and US National Institute of Standards and Technology (NIST) SP800-55.

It concludes with a chapter on new considerations related to the security of converged networks. Alternative concepts, such as overlay networks and multihoming for redundancy, are discussed.

Overall, this book is a useful read for anyone with an interest in the topics described here, and it will become relevant to even more people as IP convergence continues to grow.

Kamal Parmar, CISA, FCCA, CCNA, MCP is a manager in Deloitte’s Enterprise Risk Services practice in Melbourne, Victoria, Australia. Over a seven-year period, Parmar has performed and managed numerous attack and penetration, web application security, profiling, data analysis, and forensic engagements. He is a member of ISACA’s Publications Committee and has presented sessions at ISACA conferences.

Editor’s Note:

Securing Converged IP Networks 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.
While the reader may not have been involved in a complete business continuity/disaster recovery (BC/DR) project yet (as is the case with this reviewer), Susan Snedaker makes the reader feel as if he/she has been living it for years. In this book, the process of BC/DR is presented by a veteran in IT management and consulting who provides practical advice, not only for the main subject, but also for other supporting processes, such as project management, change management and related public relations.

Investments in BC and DR are often seen by management as costly and useless. There are also situations where IT managers are in doubt about their ability to handle such an effort because of its complexity or magnitude. For these reasons, the book is very valuable; it enables the reader to observe things that were not recognized previously and gives the reader confidence to handle a true enterprise initiative and deliver notable results.

Organizations are increasingly dependent on advanced computer-based technologies. The loss of these resources, for even a short time, can result in major adverse effects such as damage to credibility, loss of critical controls, inability to carry on operations, financial losses or breach of regulatory compliance. BC/DR planning is an effort that helps reduce operational risk associated with natural, human or technology-originating hazards.

Business Continuity and Disaster Recovery for IT Professionals provides equally well the big picture of the corporate environment, constraints and requirements, together with the details of a business impact analysis (BIA) and specifics of a risk assessment concerning IT and operational resources. In fact, more than half of the book is dedicated to the preliminary efforts of BC/DR planning; this involves an introduction to the process environment, the various legal obligations, project management, BIA and risk assessment. This pays off later when the steps for mitigation strategy, BC/DR plan development, crisis management, emergency response and testing of the developed solutions are described.

To properly plan and prioritize the necessary work for such an effort, it is important to have all of the necessary details and information at hand, and this book provides that; it serves as a one-stop resource.

One of the highlights of the book is the risk assessment chapter that presents in reasonable depth the different perspectives of a practical evaluation methodology. From an IT-centric perspective, there are many components to a risk assessment, such as hardware, software, processes, people and their dependencies, which the book breaks down.

There is a great deal of information within the book that is beneficial for various roles in the field of IT governance, including managers, security experts and auditors. Furthermore, the book is in some way practical for all IT specialists—from business analysts to service managers.

The process management and technical information prevail, as the overall goal of the book is to be an effective guide to BC best practices that might be directly used by security or business contingency managers. Sufficient information for monitoring, testing and auditing is provided at the end to facilitate the work of an IT auditor—from the beginner to the senior member of the team. The book is written in a comprehensive manner, which addresses the security management and day-to-day operational duties that contribute to an information security officer in charge of the planning, development and maintenance of business resilience.

Naiden Nedelchev, CISM, CEH, ITIL is technology security officer at Mobilitel EAD, specializing in information assurance and security governance for telecommunications. He is a professor of information assurance foundations at the Technical University of Sofia, Bulgaria. Nedelchev is a member of the ISACA Publications Committee and the Management Board of CIO Club Bulgaria.

Editor’s Note:
Business Continuity and Disaster Recovery for IT Professionals 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.
Announcing the **CISA® Online Review Course From ISACA**—Exceptional Training From a Trusted Source

Discounted pricing available exclusively to ISACA® members!

This new, **web-based** review course is **completely self-paced** and leverages the **latest materials and guidance** from ISACA’s own subject matter experts and certified Certified Information Systems Auditor™ (CISA®) holders.

If you are a **candidate preparing for the CISA exam**, or a **CISA-certified professional seeking certified professional education (CPE) credit**, this course is for you!

Choose from **six course modules** and earn up to **26 CPE credits**:
- Module 1–The IS Audit Process
- Module 2–CISA’s Role in IT Governance
- Module 3–CISA’s Role in Systems and Infrastructure Life Cycle Management
- Module 4–CISA’s Role in IT Service Delivery and Support
- Module 5–CISA’s Role in Protection of Information Assets
- Module 6–CISA’s Role in Business Continuity and Disaster Recovery

Visit [www.isaca.org/elearningcampus](http://www.isaca.org/elearningcampus) to register today!
The balanced scorecard (BSC) is a masterful tool for guiding companies through transformation. It is considered in the IT Governance Institute (ITGI)’s model for IT governance implementation regarding performance measurement and is used practically in Control Objectives for Information and related Technology (COBIT).

Whether a chief executive officer, chief financial officer, chief information officer, vice president, division or department manager, or business consultant, Balanced Scorecard Step-by-Step, 2nd Edition, allows readers to efficiently execute their organization’s strategy and successfully compete in today’s business environment.

The book provides a practical road map to plan, execute and sustain a winning scorecard campaign. The book is easy to read and tells a powerful story with lessons learned and best practices from global customer implementations.

This second edition includes steps on determining a guiding rationale for using the scorecard, testing the mission, building a strategy map, developing measures and targets, placing the scorecard at the center of the management system, and sustaining success.

Updated and enhanced with the latest BSC topics, this influential book looks to empower organizations to turn strategy into performance at every organizational level and translate their intangible resources, such as innovation, customer relationships and intellectual capital, into real value. It includes updated case studies as well as new and expanded coverage on:

• Strategy maps, the powerful communication tools that convey to the entire workforce (and beyond) what is most critical in executing the organization’s strategy
• The linkage between the balanced scorecard and corporate governance
• The critical importance of strategy-centered management meetings
• The emerging trend of the office of strategy management
• The latest trends in balanced scorecard implementation methodology
• Postimplementation guidance

In addition to tackling the use of the balanced scorecard for an incentive compensation system, chapter nine refers to something familiar for the readers of this Journal: the BSC and corporate governance. It first presents a board of director’s strategy map and then goes over corporate governance implications in the financial, stakeholder, internal and employee learning and growth processes of the scorecard.

Chapter 10 is initially devoted to advising on balanced scorecard automation aspects:

• Choosing balanced scorecard software
• Design issues; configuration of the software
• Reporting and analysis
• Technical considerations
• Maintenance and security
• Evaluating the vendor

Chapter 10 emphasizes the importance of meetings for strategy-centered management.

The author is a management consultant and noted speaker on the subjects of performance management and the BSC. As both a practitioner and consultant, he has developed successful performance management systems for organizations large and small around the globe. This book can be used as an excellent guide for the efforts of professionals and practitioners involved in IT governance implementations and preparing to plunge into the BSC methodology.

Reynaldo J. de la Fuente, CISA, CISM is project manager and chief executive officer of DataSec (www.datasec-soft.com), an IT governance, security and software tools development firm in Uruguay. 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 regional and international positions since 1993.

Editor’s Note:

Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 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.
Fraud Casebook: Lessons From the Bad Side of Business
Edited by Joseph T. Wells

Reviewed by Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA

Fraud Casebook, the 13th publication from Joseph Wells, a well-known figure among fraud examiners, pulls together the experiences of antifraud professionals across the world, detailing a case they have investigated. The book is divided into four parts: the four basic types of fraud. Part one deals with asset misappropriation and has 41 cases. Part two covers corruption schemes and presents nine cases. Part three includes six cases on financial statement fraud schemes. The last section covers, in six cases, other fraud schemes. An index of all 62 cases is included and enables cross-referencing topics.

The editor begins with a very telling comment about fraud: “Fraud is not committed by accounting systems or computers. It is carried out by living, breathing human beings who outwardly seem no different from you and me.”

Each of the fraud cases is based on the experiences of an individual author, and the literary styles differ from one to the next. However, all these cases essentially delineate four areas:

- **Why the fraud was committed**—An important part of the human angle in the case
- **How the fraud was committed**—Gives accounting and other technical details
- **Lessons learned**—Offers advice on what went wrong that contributed to the fraud taking place and being perpetrated undiscovered
- **Prevention of future occurrences**—Shows how such frauds can be prevented in the future

Information systems (IS) auditors and professionals dealing with confidentiality, integrity and availability of information look at efficiency, effectiveness, legal compliance, responsiveness and resilience. They are as much concerned with governance as with operational assurance, functionality and accountability. Fraud, of both the external variety and insider abuse, from management to employees, subverts governance and adversely affects compliance and accountability. By unfairly benefiting a few at the cost of stakeholders, it affects the smooth functioning of corporations, exposing them to severe consequences and losses—financial and otherwise. Understanding frauds and knowing how to deal with them are becoming significant issues for IS audit and security professionals.

In fact, the combined lessons of the 62 fraud cases bring home the universal truth that most people who commit frauds do so without a grand plan and actually end up making bad decisions, one after the other. Fraud, like water, follows the path of least resistance. Many frauds are perfectly simple, as they are never more complicated than necessary for achieving the objective. Occupational frauds follow a definite pattern and the cases are classified in these categories.

The book is very well presented and can be used by academics wishing to expose their students to the realities of fraud. It can be a good accompaniment to several fraud texts. Practitioners, managers and business owners, especially those who are audit professionals, will learn a lot from this compilation of cases.

Fraud is a serious problem that goes beyond monetary losses. It ruins lives and reputations, and it destroys careers and companies. Above all, it shakes the foundations of society by striking at the root of governance and an orderly ethical society.

The growing menace of frauds, as is evident from their increasing number, size and ramifications, is something that all professionals have to deal with in today’s times.

Fraud Casebook: Lessons From the Bad Side of Business sheds light on the murky side of business, industry and governance, on the dark world of fraud. The lessons learned and advice to prevent future occurrence, if used judiciously, will go a long way in preventing frauds and mitigating the impact of those that still manage to occur. The publication is well edited and compiled. Much can be drawn from the combined knowledge and wisdom of the 62 authors who have shared their experiences with the readers and presented the world of fraud very lucidly and in a captivating manner.

Vishnu Kanhere, Ph.D., CISA, CISM, AICWA, CFE, FCA is 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, academic relations, standards and research coordinator of the ISACA Mumbai Chapter; member of the ISACA Publications Committee; honorary secretary of the Computer Society of India, Mumbai Chapter; convener of the 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.

**Editor’s Note:**

Fraud Casebook: Lessons From the Bad Side of Business 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.
Information Security Training
From knowledge to practice

ISO 27001 Training

ISO 27001 Lead Auditor
The ISO 27001 Lead Auditor course provides you with the necessary knowledge to perform an audit or be in charge of ISMS (Information Security Management System) audit.

The five-day intensive course is based on the ISO 19011:2002 standard and other international audit standards and guidelines, and is conceived specifically for those who wish to carry out external or internal audits according to the ISO 27001:2005 standard's criterion.

ISO 27001 Lead Implementer
The ISO 27001 Information Security Management System (ISMS) Implementation course teaches students the necessary steps of ISMS implementation as specified in ISO 27001.

The training is also aligned with project management best practices regarding the Project Management Institute (PMI) and the International Project Management Association (IPMA) as well as the ISO 10006 standard, “Guidelines for quality management in project”.

Certified by the RABQSA

United States of America

<table>
<thead>
<tr>
<th>City</th>
<th>City</th>
<th>City</th>
<th>City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anaheim</td>
<td>Las Vegas</td>
<td>Alger</td>
<td>Mexico</td>
</tr>
<tr>
<td>Atlanta</td>
<td>Los Angeles</td>
<td>Beijing</td>
<td>Montreal</td>
</tr>
<tr>
<td>Boston</td>
<td>New York</td>
<td>Brussels</td>
<td>Paris</td>
</tr>
<tr>
<td>Buffalo</td>
<td>San Diego</td>
<td>Bucharest</td>
<td>Prague</td>
</tr>
<tr>
<td>Chicago</td>
<td>San Francisco</td>
<td>Casablanca</td>
<td>Sydney</td>
</tr>
<tr>
<td>Dallas</td>
<td>Seattle</td>
<td>Geneva</td>
<td>Tokyo</td>
</tr>
<tr>
<td>Detroit</td>
<td>Tampa</td>
<td>Hong Kong</td>
<td>Toronto</td>
</tr>
<tr>
<td>Houston</td>
<td>Washington</td>
<td>Madrid</td>
<td>Vancouver</td>
</tr>
</tbody>
</table>

International

For more information, contact us at training@veridion.net

www.veridion.net
A Comprehensive Method for Assessment of Operational Risk in E-banking

By George Tanampasidis, CISA, PMP

The deregulation of the international banking system and the fierce competition among banks have motivated them to develop new channels for attracting and retaining customers. The evolution in telecommunications technology and the Internet has boosted a revolution in the development of electronic networks, through which customers have access to banking products and services (electronic banking). In these channels, the degree of automation is usually high, the human intervention low. This new situation raises new legal and ethical dilemmas and challenges to both the customer and the bank in such areas as:

- Impersonal communication between the bank and the customer
- A high degree of automation
- Sensitive data interchange through public networks
- 100 percent system availability
- Technology
- Competition
- Regulatory framework

On the other hand, the issue of operational risk has become more important in recent years. The Basel II Capital Accord requires management and evaluation/measurement of operational risk in all banking activities. Regulators have issued various sets of rules and principles for managing operational risk. Nevertheless, these directives usually focus on a passive approach, since they do not try to actively measure operational risk but rather describe the tools that can be used to minimize it—perhaps because of regulators’ worldwide focus on the measurement of Value at Risk (VaR). The VaR methodology translates the level of risk into monetary units while it requires extensive historical data to calculate variability and probabilities (loss data). These requirements make this methodology very difficult to be applied in the case of e-banking, as it is a new area and there are few available loss data. Additionally, operational risk in e-banking is related to a number of qualitative factors that are very difficult to quantify.

Methodologies for managing and evaluating operational risk in information systems that bypass the constraints of VaR have been developed. These methods are a mix of expert opinion and self-assessment methodologies, with the use of risk factors as an index for the level of risk. The most important constraint of these methods is that the results among surveys are not comparable, since they depend on the environment. Nevertheless, the combination of the expertise of a risk analyst with that of the system users can quantify, at a high level of confidence, the operational risk that the bank is exposed to and indicate critical areas for further investigation.

This paper presents a comprehensive methodology that helps the auditor to overcome the numerous qualitative parameters of the operational risk in e-banking. The methodology integrates three separate tools that can be used extensively by the information systems (IS) auditors in operational risk management:

- Self-assessment by the users
- Expert opinion by the IS auditor
- Key risk factors

In the suggested methodology, the auditors perform a survey on e-banking’s operations and define critical areas of risk exposure. Then, they set the framework for the survey and prepare questionnaires for the business users to self-assess the level of risk exposure. The business users assess the level of risk by answering a structured questionnaire, which is previously set by the auditors. Afterwards, the auditors’ responsibility is to collect the answers and put them into spreadsheets to calculate the risk exposure by area.

The rationale of the whole process is based on the following principles:

- The auditor has enough expertise to review the e-banking processes and identify key risk areas and factors.
- The business users have enough knowledge of the daily operations and are capable of assessing the level of risk exposure for each area/risk factor.

The reliability of the results depends on the degree to which both the risk analyst and the business users actively participate in the process. Thus, the methodology cannot be applied by only the auditor or the business users. Each of these parties has different perspectives and contributions to the whole process. The auditor can identify key risk areas but does not know in detail the daily operations, while the business users know the daily operations but not the total picture. Additionally, the business users may have an interest to hide certain risks from the auditor to make their job easier.

The advantages of this methodology include the following:

- The auditor focuses on the qualitative parameters of risk exposure.
- It is relatively easy for an auditor with average expertise to identify key risk areas and factors.
- It is easy for business users to assess risk exposure by assigning a grade from zero to three for each key risk factor, according to their own subjective criteria. Despite its subjectivity, the methodology can give unbiased results if enough business users are involved in the process.
The information systems control journal, volume 4, 2008

• It integrates the knowledge and objectivity of an external auditor with the knowledge and expertise of the business users.
• All business users contribute to the survey, which, on average, makes the final result unbiased.
• The results of the survey can be understood easily by top management since they can be presented graphically from various perspectives. Therefore, management can focus on specific areas for appropriate action.

The restrictions of this methodology include the following:
• It is completely subjective (both at the auditor’s and the business user’s level). Nevertheless, if the auditor asks all the business users of e-banking to assess the risk exposure, the final result, on average, is unbiased and reveals the real level of risk exposure.
• The results are not comparable to other similar surveys, since they depend on the external and internal environment of the organization under survey.
• The results are not comparable even to previous surveys in the same organization as they cannot take into account process changes and system upgrades that have taken place in the meantime.

Methodology
The suggested methodology includes the following stages:
1. Strategy analysis and evaluation
2. Risk identification
3. Identification of points of risk mitigation and control
4. Risk evaluation
5. Risk measurement:
   • Business unit activity
   • Application/subsystem functionality and constraints
   • Identification of key risk factors
   • Self-assessment
   • Data processing
6. Reports

Strategy Analysis and Evaluation
The risk analysts have to prepare a report in which they describe the bank’s strategic goals in the context of e-banking. The analysts have to interview key bank executives who are responsible for banking operations and have a decisive role in the e-banking services. The analysts must focus on three major areas as described in figure 1.

Risk Identification
The deliverable of this stage is a two-column table (figure 2). In the first column, analysts list the key e-banking functions and in the second column they list, for each function, all of the risks that have been identified without taking into account any controls or points of risk mitigation that may have been applied to reduce risk exposure (inherent risks). To fill in the data in this table, analysts should first determine:
• The services/functions provided in e-banking
• The operational risk types identified and associated to each function
• The business units (BUs) that are involved in the daily processes

The analyst should conduct a SWOT analysis to assess the strengths and weaknesses of the internal and external environment and identify opportunities and threats that may arise in the near future. The SWOT analysis will be used to identify the level of operational risk to which the bank is exposed.

Points of Risk Mitigation and Controls
The deliverable of this step is a two-column table (figure 3). The first column contains all risks identified in the previous stage. The second column includes all points of mitigation and control mechanisms that have been applied to reduce every one of the risks identified previously.

Auditors must review all mitigation controls that are used to reduce risk exposure. For each of the control mechanisms, analysts must assess the quality of the allocated resources and their costs.

At the end of this stage, the auditor should have a list of all of the key risks to which e-banking is exposed, accompanied by the major control mechanisms/points of risk mitigation that are used to decrease the risk exposure.
**Risk Evaluation**

Risk evaluation is a process where analysts must determine the following:

- The level of residual risk after all control mechanisms are in place
- Control effectiveness
- The “sensitive” risk areas
- Who is in charge of applying the control mechanisms and how effective they are

At the end of this stage, the auditor must be in a position to identify for further investigation the residual risk and assess the areas where the risk is eliminated or is insignificant, as well as the areas where the risk is relatively high.

The overall assessment of risk exposure is a process based on expert opinion. Analysts use their professional expertise to evaluate the findings of the review process to identify key risk factors and sensitive areas for further investigation.

**Objectives Achieved in Stages**

In the first four stages of the methodology, analysts have identified and documented the major strategic goals of the bank in e-banking, the operations/functions, the risks per function and the control mechanisms applied in each case to reduce risk exposure. Moreover, analysts conduct a first assessment of the level of risk exposure and identify sensitive areas for further investigation. During this process, analysts have the opportunity to identify and record:

- The number and the type of information systems involved in e-banking
- The BUs involved in the e-banking business processes
- The functionality and duties of each BU in the context of e-banking

Analysts now use their professional experience to assess the importance of each BU and information system in relation to e-banking. They make a sort list of all BUs and systems, according to their importance, and decide on which to focus.

**Risk Measurement**

Risk analysts must directly contact the business users who are involved in the e-banking business processes. The meeting can be arranged with the head of each BU, but it would be more productive if there were separate meetings with a couple of key executives within each BU. The call for the interview should take the form of a letter, from the auditor to the head of the department, asking for a meeting to discuss the functionality and duties of the business unit in relation to e-banking.

The information gathered in these sessions can be summarized in two forms:

- Business unit activity form
- Application description form

**Business Unit Activity**

The BU activity form is used to record the major business processes in which the BU is involved. For each BU the risk analysts should record:

- BU name
- Head of the BU
- Operations and procedures
- Hardware and other technical infrastructures
- Software and information systems used
- Major users
- Major risks identified
- Future plans

The BU activity form enables risk analysts to identify the major applications/information systems in relation to e-banking. The next step enables risk analysts to learn more about these systems.

**Application/Subsystem Functionality and Constraints**

The application description form is used to record the characteristics of each application/subsystem of e-banking. The major characteristics that should be recorded in this form are:

- Application/subsystem name
- Application/subsystem supervisor

---

**Figure 4—Risk Assessment Form Example**

<table>
<thead>
<tr>
<th>Number of system users</th>
<th>Account Data and Transactions</th>
<th>Fund Transfers Within Bank</th>
<th>Fund Transfers</th>
<th>Payments</th>
<th>Direct Debits</th>
<th>Checkbooks</th>
<th>Transaction Authorization</th>
<th>User Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-One user group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-A few user groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-Many internal departments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-Internal departments plus customers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System's importance</th>
<th>Number of system users</th>
<th>Account Data and Transactions</th>
<th>Fund Transfers Within Bank</th>
<th>Fund Transfers</th>
<th>Payments</th>
<th>Direct Debits</th>
<th>Checkbooks</th>
<th>Transaction Authorization</th>
<th>User Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-No impact from nonavailability</td>
<td>0-One user group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-Useful but not necessary for bank operations</td>
<td>1-A few user groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2-Important for bank operations</td>
<td>2-Many internal departments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3-Critical for bank operations</td>
<td>3-Internal departments plus customers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please fill in each cell 0, 1, 2 or 3
Identifying Key Risk Factors

After the interviews with the BUs, auditors must be in a position to know:
• Which BUs are involved in the e-banking business processes and their operations
• How the BUs interact with each other
• Daily operations, procedures and processes
• Deficiencies and risks of business processes
• The applications/subsystems of which the e-banking systems are composed
• The BUs that use or interact with each application/subsystem
• Data volumes
• Interconnection to other systems

Risk analysts collect the BU activity forms and the application description forms. They analyze the data gathered, so that eventually they are in a position to understand in detail the e-banking functionality.

Analysts aggregate the information, and use their judgment and expertise to determine the key risk factors (KRFs) that are considered to be critical for the determination of the bank’s operational risk exposure. It is obvious that risk analysts will end up with a set of KRFs that depend on both the environment and their own experience. Different analysts may end up with different sets of KRFs—the major disadvantage of this methodology. Nevertheless, daily practice has shown that auditors with average experience will end up with similar sets of KRFs.

Self-assessment

The next step in the process is to allow users to self-assess the level of risk exposure. The tool for this process is the risk assessment form (RAF), a questionnaire prepared by the auditor and shipped to each business user of e-banking (figure 4).

The RAF has the format of a double-entry matrix. It is usually developed in an Excel spreadsheet. The rows of the matrix include the KRFs that have been defined in the previous step. For each KRF, the risk analyst has assigned four answers rated from zero to three. Each rating indicates different levels of risk exposure, with zero as the minimum and three as the maximum. For presentation and visualization purposes, it can be better to assign a color to each rate (0=White, 1=Yellow, 2=Orange, 3=Red); however, this is not included in these examples. In the columns, the major functions/subsystems of the e-banking system are placed. The RAF is sent to the key users of all BUs. The users must fill in the cells with their rating of each KRF for each subsystems/application of e-banking.

Data Processing

After receiving all the RAFs from the users, the analysts must copy the rates of each user in the application risk assessment form (ARAF). This form has the format of a double-entry matrix similar to the RAF, where rows and columns are transposed. The rates given by each user are copied to the ARAF and grouped by business unit. Finally, the analyst calculates the average rates per KRF and per application/subsystem, both by BU and the total. The results of the analysis are shown in figures 5, 6 and 7.

The final step of data processing is the measurement of risk that is related to the technical infrastructure. The tool for this kind of measurement is the technical infrastructure risk assessment form (TIRAF). The format of a TIRAF is shown in figure 8.

The key functions of e-banking are placed in the rows, and the main pieces of technical infrastructure (PTI) that are used by the e-banking system are placed in the columns. In the column next to functions, the average risk per function, as it has been calculated in the ARAF, is placed. For each row (function), its average risk rate is moved to the right, under those pieces of technical infrastructure used by the specific function. At the bottom of the spreadsheet, the average risk rate per PTI is calculated, as are the number of functions that use each PTI.

After completing all the steps, the analysts have to quantify and visualize the following:
• Average risk per KRF
• Average risk per function
• Average risk per piece of technical infrastructure

Reports

Eventually, after the risk analysis has been completed, the analysts will be in a position to understand the risk structure of the e-banking service and identify those areas with high risk exposure. At the final step of the risk analysis process, they prepare a report for the project sponsors (in this case, the top management) where the findings are summarized.

The final report should include the following sections:
• Overview—There will be an overview of the functionality of the e-banking service and a generic assessment of the risk exposure.
• Key risk factors—The major KRFs should be presented in detail. Analysts must report the impact of each KRF on the level of risk exposure.
• Risks per function—There must be a short description of the most risky areas of e-banking according to the findings from the analysis. For each area, the analysts must list the causes and the KRFs that yield to high risk exposure, and make proposals for actions or business process reengineering that will moderate the risk exposure.
• Technical infrastructure risks—A summary of the technical infrastructure used and its risk exposure are presented. The analyst must present how the KRFs affect the risk exposure of the technical infrastructure and propose control mechanisms and actions that should be taken to reduce risk exposure.
Conclusions

As e-banking is a relatively new banking service, there are few historical loss data available worldwide. In e-banking, the system’s structure, its functionality and complexity are attributes that are very difficult to quantify. Thus, the use of an advanced measurement approach (AMA) for the calculation of operational risk exposure is either difficult or impossible.

On the other hand, IS auditors have developed tools that enable them to assess and visualize operational risk. The disadvantage of these methods is their subjectivity and the fact that the results depend entirely on the system being audited. However, the advantage is their simplicity: they require neither loss data nor complex mathematics. The main tools for the application of these methods are the interview with key business users and the professional experience of the auditor.
### Figure 6—Average Rate per Risk Factor

<table>
<thead>
<tr>
<th>Key Risk Factors</th>
<th>Rating</th>
<th>Key Risk Factors</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Number of system users</td>
<td>2.1</td>
<td>16 Support</td>
<td>1.3</td>
</tr>
<tr>
<td>2 System’s importance</td>
<td>1.9</td>
<td>17 Interconnection with other systems</td>
<td>1.8</td>
</tr>
<tr>
<td>3 Funds’ throughput</td>
<td>0.8</td>
<td>18 Documentation</td>
<td>0.9</td>
</tr>
<tr>
<td>4 System’s availability</td>
<td>1.1</td>
<td>19 Data sensitivity</td>
<td>2.4</td>
</tr>
<tr>
<td>5 Management’s interest</td>
<td>1.2</td>
<td>20 Changes</td>
<td>1.3</td>
</tr>
<tr>
<td>6 Time elapsed since last audit</td>
<td>0.5</td>
<td>21 System’s age</td>
<td>1.1</td>
</tr>
<tr>
<td>7 How the internal controls are applied</td>
<td>1.0</td>
<td>22 Complexity</td>
<td>2.3</td>
</tr>
<tr>
<td>8 Impact on bank’s operations</td>
<td>1.4</td>
<td>23 Cost-efficiency</td>
<td>1.1</td>
</tr>
<tr>
<td>9 Results of last audit</td>
<td>1.3</td>
<td>24 Impact on profitability</td>
<td>1.2</td>
</tr>
<tr>
<td>10 Compliance</td>
<td>1.0</td>
<td>25 Automation</td>
<td>1.9</td>
</tr>
<tr>
<td>11 Transaction volume</td>
<td>1.3</td>
<td>26 Sensitivity to mishandling</td>
<td>0.6</td>
</tr>
<tr>
<td>12 Number of customers</td>
<td>0.7</td>
<td>27 Generic risk assessment</td>
<td>0.8</td>
</tr>
<tr>
<td>13 Number of internal users</td>
<td>1.4</td>
<td>28 Unavailability</td>
<td>2.6</td>
</tr>
<tr>
<td>14 External security</td>
<td>0.5</td>
<td>29 Average risk rate</td>
<td>1.3</td>
</tr>
<tr>
<td>15 Internal security</td>
<td>0.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16 Support</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 Interconnection with other systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18 Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19 Data sensitivity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 Changes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21 System’s age</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22 Complexity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23 Cost-efficiency</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24 Impact on profitability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25 Automation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26 Sensitivity to mishandling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27 Generic risk assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28 Unavailability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 Average risk rate</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Figure 7—Average Risk Rate per Function and Business Unit

<table>
<thead>
<tr>
<th>Applications/Functions</th>
<th>Average Risk Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account data and transactions</td>
<td>1.2</td>
</tr>
<tr>
<td>Funds transfers within bank</td>
<td>1.4</td>
</tr>
<tr>
<td>Funds transfers</td>
<td>1.5</td>
</tr>
<tr>
<td>Payments</td>
<td>1.5</td>
</tr>
<tr>
<td>Direct debits</td>
<td>1.5</td>
</tr>
<tr>
<td>Checkbooks</td>
<td>1.5</td>
</tr>
<tr>
<td>Transaction authorization</td>
<td>1.5</td>
</tr>
<tr>
<td>User management</td>
<td>1.5</td>
</tr>
</tbody>
</table>

### Figure 8—Technical Infrastructure Risk Assessment Form

<table>
<thead>
<tr>
<th>Pieces of Technical Infrastructure (PTI)</th>
<th>Core Banking System</th>
<th>DIASDEBIT</th>
<th>SWIFT</th>
<th>DIASTRANSFER</th>
<th>Credit Cards</th>
<th>Checkbooks</th>
<th>Direct Debits I</th>
<th>Direct Debits II</th>
<th>Payments</th>
<th>User Authentication</th>
<th>Security and Access Control</th>
<th>Avg. Risk Rate</th>
<th>Depended Applications per PTI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Banking System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIASDEBIT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWIFT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIASTRANSFER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Credit Cards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checkbooks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Debits I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Debits II</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security and Access Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avg. Risk Rate</td>
<td>1.3</td>
<td>1.4</td>
<td>1.5</td>
<td>1.4</td>
<td>1.5</td>
<td>1.2</td>
<td>1.2</td>
<td>1.2</td>
<td>1.4</td>
<td>1.5</td>
<td>1.3</td>
<td>1.3</td>
<td></td>
</tr>
<tr>
<td>Depended Applications per PTI</td>
<td>8</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>8</td>
<td>8</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>
The methodology, and its rationale, which can be easily understood by any risk professional and/or top management, can be applied by an average-to-experienced auditor and yield a pretty good understanding of the risk exposure.

References
Bank of Greece, “Core Principles for Operational Risk Management in Information Systems,” 2005

Endnotes
1 The rows of figure 5 are filled with the answers of each business user in each business unit. In our example there are one user in the funds transfer department, two users in the business analysis dept., one user from the technical infrastructure dept., etc. The auditor must calculate the average risk exposure by KRF (by department and overall).
2 Figure 6 presents the overall average rate for each KRF (last line in figure 5).
3 Figure 7 aggregates the results of figure 5. The rows stand for functions/processes of e-banking (rows in figure 5), while the columns stand for the BUs. In the cells, the auditors fill in the values of the column “Average Risk Per Function” in figure 5.

George Tanampasidis, CISA, PMP is a senior IT professional working in the banking sector in Athens, Greece. He has more than 10 years of IT and banking experience, specifically in project management, business analysis and IS design. He has been actively involved in projects regarding Basel II, AML and regulatory compliance reporting.
“Risk” is one of those words that everyone understands and is used across many different fields and professions; this allows for a large number of interpretations linked to specific situations. Depending on the profession, there are very particular models, methods and actions used to understand and manage risk. Examples in the financial world include Value at Risk (VaR), Montecarlo Simulations and complex models; in IT security, models such as Simple to Apply Risk Analysis (SARA), Simplified Process for Risk Identification (SPRINT), and Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) have been applied for some time to support risk assessments. Other professions have mechanisms to measure and manage risk as well.

For information security auditors and other information security professionals, there is an opportunity to use a number of models for risk management, rather than limiting the scope to risk assessment tools only. Risk management models contribute to the bottom line of the organization by ensuring a more comprehensive framework and increasing visibility of the balance between opportunities and risks. This is a complex issue as it involves interacting with individuals at all levels in the organization and establishing a common language and approach to manage risk, without trying to bring all risks under the same umbrella.

There are different standards in use, and others currently in development, aimed at providing a risk management model that could be deployed by organizations across different industries; these standards are supported by at least three well-established risk management models that have the benefit of time to reach maturity. The risk management models are also supported by the increased adoption of the ISO/IEC 27001 standard from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The standard has increased the number of organizations using an information security management system (ISMS) supported by a risk assessment working as a cornerstone.

Examples of Risk Management Standards and Frameworks

Over the past two decades, a number of risk management standards have been developed as a result of demands from different industries, increased maturity of the profession, and higher expectations from regulators regarding the understanding and management of risk. Each one of the standards has aspects that could benefit particular deployments; some include more detailed recommendations, while others prefer to use a more general approach. The selection of the appropriate risk management standard for an organization should be the result of a formal comparison and subject to the specific needs and expectations defined by senior management.

As with any standard, the risk management standards described in this article are intended to provide a general description of the elements, processes and activities required for risk management; they do not provide a comprehensive view or a one-size-fits-all solution.

The following is a brief reference to some of the most widely used risk management standards, including some references to the topics covered.

AAIRM

The AIRMIC, ALARM, IRM (AAIRM) standard includes references to areas such as:
• Terminology definition for risk
• Risk management
• Risk assessment
• Risk analysis
• Risk evaluation
• Risk reporting
• Risk treatment
• Risk monitoring and the review of the risk management process
• The structure and administration of risk management

Figure 1 shows the process flow to be followed during the operation of the risk management function, maintaining a cycle that covers the organization’s strategic objectives to monitoring of the risk management model. The process flow is supported by formal audits.

Figure 1—AIRMIC/ALARM/FIRM Risk Management Process
The standard also includes an appendix with a useful list of risk identification techniques as well as risk analysis methods and techniques that could be used to learn more about available developments that could support the execution of the risk management functions. The standard provides a good overview of the stages and activities required for risk management; however, more details would be required to implement a real-life process.

AS/NZ 4360

The well-known Australia and New Zealand Standard 4360, Risk Management Systems Standard (AS/NZ 4360), includes slightly more detail than the AAIRM standard. AS/NZ 4360 is the result of a long-term evolution and maturity starting in 1995, with a second edition in 1999 and the current version published in August 2004.

AS/NZ 4360:2004 follows a similar baseline as the model recommended by the AAIRM. Although it does add some references to the task of communicating and consulting the results, AS/NZ 4360:2004 lacks the specific references to roles and responsibilities available in AAIRM. A representation of the standard is included in figure 2.

![Figure 2—AS/NZ 4360:2004 Risk Management Standard](image)

The AS/NZ risk management process and the AAIRM standard follow a similar framework and allow risk managers to follow an end-to-end process to ascertain the risk levels applicable to the specific context, analyzing and evaluating the risk, and then treating the specific risk levels and reducing exposure. There is a particular focus in the AS/NZ standard to the context of the process, starting with a phase dedicated to establishing the contextual information for the risk management framework.

M_o_R

The UK Office of Government Commerce (OGC) has issued a risk management model titled “Management of Risk: Guidelines for Practitioners (M_o_R).” This guide, originally written in 2002, with a new version released in 2007, includes more detailed guidance than AAIRM and AS/NZ 4360.

M_o_R covers four main areas:
- **Principles**—Critical for the development of good risk management practice. Based on corporate governance, principles are supported in the concept that risk management is a key internal control.
- **Approach**—Specific elements required to ensure the successful implementation of the risk management model. This would include the definition of elements within the risk management policy and other key documents.
- **Processes**—Critical processes required for risk management, including activities involved in ensuring that risks are identified, assessed and controlled
- **Embedding and reviewing**—Effective mechanisms that ensure the consistent implementation of principles and procedures within the organization; critical to successful implementation of the risk framework.

COSO ERM

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework provides very useful information to deploy and operate the risk management function. Originally formed in 1985, COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls and corporate governance. In 2004, COSO published an updated document, Enterprise Risk Management—Integrated Framework.

The COSO model includes areas recommended by other risk management models as well as a three-dimensional matrix matching four objectives categories, eight components and an entity’s units. This visualization of risk components provides significant value, as it can help risk professionals to break the problem into smaller elements, simplifying the analysis and review of solutions. As a result, automated tools could be developed to provide a representation of the risk profile of an organization.

The areas included in COSO in the first dimension are internal environment, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. These are referenced to the second dimension, which includes entity level, division, business unit and subsidiary. Both are then mapped with the third dimension, which covers areas including strategic, operations, reporting and compliance.

This multidimensional view allows risk professionals to slice the areas and concentrate on smaller domains—all while maintaining the global scope.

Interaction

These examples of risk management models have supported the maturity of the knowledge and approach to the topic. Currently ISO is working on the development of a standard, Risk Management—Guidelines on Principles and Implementation of Risk Management, which is being reviewed and is planned for publication by the second half of 2009.

The importance of the proposed ISO 31000 (figure 3) is that it provides a common language and model to be used by organizations to implement a risk management model that would be consistent, replicable and accurate.
Conclusion

What is the impact for auditors and information security professionals?

Having a standardized methodology for risk management would allow auditors to simplify their approach by using the output of the risk management framework. Once the organization has implemented a risk management model, many information security audit and information security functions would be greatly simplified. Instead of requiring the deployment of ad hoc risk assessment methods and duplicating some risk management functions, auditors and security professionals would be able to interact with the risk management framework directly.

This has the added advantage of senior management being aware of the risk-related decisions, and the board of directors being able to officially establish the risk appetite and monitor the impact of risk management decisions across the organization.

The increased maturity and exposure of risk management methodologies and similar evolution in information security methodologies are creating the basis of risk convergence between the two professions. Risk management has been managed in silos within companies as a core management responsibility; each business area tends to create personalized views and models on risk management. With the inception of formal risk management models supported by information security standards, companies can deploy a corporate model for risk management using a common language that would cover physical, digital, legal, operational and financial risk, among others.

In the future, more institutions may be able to articulate risk and information security standards and provide a single console to senior management representing a comprehensive view of risk—allowing auditors to concentrate on critical risks to the business instead of individual interpretations of risk exposure by each unit.

References

Ward, Stephen; Risk Management: Organisation and Context, Witherbys, 2005
Gregg, Michael; CISA Exam Prep; Exam Cram, 2007

Endnotes

1 Association of Insurance and Risk Managers (AIRMIC), ALARM (National Forum for Risk Management in the Public Sector) and Institute of Risk Management (IRM), A Risk Management Standard, 2002, London
4 Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management—Integrated Framework, 2004

David Ramirez, CISA, CISM, CISSP, BS 7799 LA, MCSE, QSA is a senior manager for the global security consulting practice at Alcatel-Lucent. He has more than 13 years’ experience within information security and IT audit, leading successful engagements worldwide. Ramirez has specific experience working on behalf of the major insurance companies, auditing banks and financial institutions around the world; this includes a number of central banks and dozens of retail banks. He has published a number of articles and white papers, and his second book on security was published by Wiley in January 2008.

Editor’s Note:

ISACA and the IT Governance Institute (ITGI) are undertaking an initiative to develop the IT Risk Management Framework that will allow business managers to assess IT controls for deficiencies and business risks. For more information, please read the article “New Framework for Enterprise Risk Management in IT” in this issue.
Automating Security Policy and Procedures With Workflow: How to Improve the Effectiveness of Risk Management Solutions

By Michael Godfrey

A security policy, be it network, information or physical, is designed such that the system, organization, people or other entity in question remains in a highly safe and secure state. The inherent challenge in creating a security policy is to first define what it means to be secure. Generally speaking, to be secure refers to the absence of harm. For a network, that may mean the absence of viruses; for an information system, it may mean the absence of a privacy breach of protected information. A secure physical security system generally refers to the absence of threats that may cause damage, injury or death to facilities and people.

With the definition in place of what it means to be secure, the challenge then becomes enforcement. Enforcing a security policy requires a detailed set of procedures designed not only to proactively prevent and detect threats, but also to respond quickly and effectively when security breaches do occur so as to efficiently mitigate risk.

As today’s security risks become increasingly complex, interrelated and global, the growing convergence of physical and IT security is aiding the goal of developing approaches for holistic enterprise security risk management.

Security Convergence

The Open Security Exchange (OSE) defines convergence as the migration of physical and IT security toward common objectives, processes and architectures. This trend is resulting in increased systems interoperability and centralized security management to unite the many disparate security subsystems (e.g., access control, surveillance cameras, CCTV, intercom, perimeter detection, fire alarm) under one common management platform.

While the benefits of security convergence are many, the integration and interoperability of multiple systems and functional groups do pose challenges. Of particular significance is how to train operators to comprehensively manage and swiftly respond to the vast amounts of available data that converged security solutions produce.

Traditional security operators are trained extensively in procedures that are documented in printed binders (i.e., “big, black binder”). Effective response to security-related events depends on the security operator not only remembering the appropriate procedure, but also correctly following that procedure. Should the operator successfully recall and execute the procedure, without systems integration and interoperability, response times may be slow and difficult to audit after the fact.

Integration Intelligence

Using Internet Protocol (IP) network architecture as a backbone, converged security solutions can add a layer of “integration intelligence” that goes a long way toward ensuring that security procedures are being followed as they were intended to be, to mitigate risk as effectively and efficiently as possible. This integration intelligence, incorporated through sophisticated rules-based engines, can automate a chain of actions or walk an operator through the appropriate manual response procedure for a particular security event.

Figure 1 depicts a sample flow of action an operator would have to follow in the event of a security alarm (in this case, a fire alarm). The procedure works on a step-by-step basis, thus ensuring that all the necessary procedures are met and reducing any human decision-making errors that might occur during a high-pressure event.

When chief security officers (CSOs), or the persons in charge of security policy and procedures, can transfer their knowledge and experience to security operators by incorporating best practices and predefined response procedures directly into the system, complexities associated with the “big, black binder” and human error are reduced. This leads to more rapid event response and increased security.

Workflows are essential to turn the knowledge and experience of the CSO (or equivalent security policy director) into integration intelligence that can be accessed by any security operator when responding to security threats. Workflows create a series of manual and/or automatic actionable steps based on operator responses to “if/then” statements.

Consider a system that incorporates video surveillance, fire detection, access control, incident reporting and building automation systems, such as lighting, ventilation and temperature control. In a converged security system, a workflow application establishes an integration intelligence layer that will provide the true interoperability among these disparate systems and reduce verification and response times to effectively mitigate risk.

A notification from the fire detection system could initiate a workflow that would automatically present the operator with the most appropriately positioned camera for alarm verification and prompt the operator to indicate whether the alarm is valid (e.g., Are there signs of smoke and fire? Yes or No)—see figure 2. The operator response will initiate the appropriate follow-up action, e.g., if yes, the system will trigger the emergency lighting and ventilation system, lock down doors in unsafe areas, and notify emergency services.
Workflows add a layer of intelligence to integrated security solutions, thus reducing reliance upon manual decision making in high-pressure situations. Workflows reduce human error by automating emergency event management for rapid, intelligent response.

**Procedure Analysis**

Workflows also provide a measurable status quo. In a converged system that records each step in the workflow event response, postevent analysis can help to continually improve procedures to ensure that security policy is maintained adequately. Analysis and tracking are also important for policy compliance auditing for management of internal security and for external investigations, be they legislative or judicial.

**Return on Investment**

Measuring the return on investment (ROI) from security installations has traditionally been a difficult task. While the need for security is generally recognized, calculating the probability and consequences of a potential event is by no means an exact science.

In addition to the standard return on security investment, converged and intelligent rules-based security solutions can provide measurable return in terms of system operation. Using a workflow application significantly reduces training costs for security operators, a significant expenditure in this high-turnover industry. Additionally, workflows aid in the reduction of costs associated with the mishandling of a security-related event.

The convergence of systems, together with an enhanced ability to track and record alarms and responses, provides for ROI in terms of successful investigation and prosecution. Litigation claims, a costly expense for many municipalities, airports, transit authorities, etc., can be avoided with readily available and admissible evidence.

**The Future of Risk Mitigation Technology**

By providing a means for comprehensive, centralized information exchange, the convergence of IT and physical security is the first step toward effective risk mitigation. However, by itself, it does not represent a total risk management solution, as it does not address the need to harness, understand and make decisions based on the data provided through this information exchange. Intelligence sharing and collaborative decision making are critical to creating truly holistic security risk mitigation.

With regard to security risk, intelligence capabilities can be measured through compliance processes, risk identification, risk assessment, risk response and continuous process...
improvement. Workflow application software, embedded into the security management process, will play an important role in driving the adoption of security convergence and holistic risk mitigation. Workflow provides the layer of intelligent integration to security convergence solutions that will be critical in realizing ROI and measurable improvements to enterprisewide risk management.

**Michael Godfrey**

is the chief technology officer at Visual Defence, where he oversees research and new industry developments. Previously, he was president of ViaLight Canada, where he was responsible for the development and delivery of fiber solutions to the home. Godfrey has a highly respected and diversified background within the IT field, with certification in advanced communication systems and engineering management.

**Editors Note:**

The Alliance for Enterprise Security Risk Management™ (AESRM™), a partnership of two leading international security organizations—ISACA and ASIS International, addresses issues surrounding the convergence of traditional and logical security. To learn more, please visit [www.aesrm.org](http://www.aesrm.org).
Prepare for the 2008 CISM Exams

ALL NEW—COMPLETELY REVISED—2008 Certified Information Security Manager (CISM) Review Materials for Exam Preparation and Professional Development

To pass the CISM exam, a candidate should have an organized plan of study. To assist individuals with the development of a successful study plan, ISACA offers study aids and review courses to exam candidates (see www.isaca.org/cismexam for more details).

CISM Review Manual 2008
ISACA

The CISM® Review Manual 2008 has been completely revised and updated with new content to improve consistency and clarity and to remain current in a dynamic field. The updated manual reflects the fact that the information security management profession is rapidly evolving, with increasing responsibilities, scope and authority. Topics covered include governance and management, strategy and policy, security architecture and metrics, and the alignment of security activities with, and in support of, overall business objectives. The new edition also features definitions of terms most commonly found on the exam, practice questions similar in content to what has previously appeared on the exam and references to additional study materials on specific topics. The CISM Review Manual 2008 is designed to assist candidates in preparing for the CISM exam, and for individuals wanting to learn more about the roles and responsibilities of an information security manager. The 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 2008 edition is organized to help prepare the CISM candidate in studying the following job practice areas:
• Information security governance
• Information risk management
• Information security program development
• Information security program management
• Incident management and response

ISACA

The CISM® Review Questions, Answers & Explanations Manual 2008 consists of 350 multiple-choice study questions that have previously appeared in the CISM Review Questions, Answers & Explanations Manual 2007 and the 2007 Supplement. Many questions have been revised or completely rewritten to recognize a change in job practice, be more representative of the current CISM exam question format, and/or to provide further clarity or explanation of the suggested correct answer. These questions are not actual exam items, but are intended to provide the CISM candidate 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 2008.

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

Please Note the following system requirements:
• Intel Pentium 3 or higher (Pentium 4 recommended)
• Windows 98SE or higher
• 256 MB RAM (512 MB recommended)
• Hard drive with 225 MB of available space
• CD-ROM drive
• Display with recommended resolution of 1024 x 768

Preparation and Professional Development

Whether one is considering IT or non-IT audit, it is important to understand that there are no requirements solely reserved for audit, when evaluating internal controls, risk management, information, security or continuity. There are only business objectives and related information requirements.

The focus of an (IT) audit should be to create value for the organisation. To accomplish this, an assessment model for internal control and risk management, in which IT objectives are stated clearly and aligned to the company’s overall objectives, should be adopted.

Enabling the organisation to realise its business objectives entails important requirements for information. These requirements are related to the effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability criteria of information. Business and IT should be seen as partners working together to achieve convergent objectives. In the same way that internal audit is to be holistic, traditional auditing and IT auditing should integrate seamlessly.

**Self-assessment As a Method to Enhance Control Awareness**

Internal auditors’ scope of action has extended over the years, and the trend is moving towards issuing assessment, assurance and high-level consulting services, related to internal control, risk management and process management business activities.

In addition, an emphasis is placed on doing more and more proactive auditing—better to prevent than to cure. The only good incident is the one that did not hit the company. This applies to both IT and non-IT auditing.

Using self-assessment is a very effective way to give IT and business entities the tools to evaluate and enhance internal controls and, at the same time, increase insight and co-responsibility. The usage of self-assessment allows for broadening the audit universe, not reducing it, because facilitating self-assessment does not conflict with traditional audit approaches.

**Internal Control Frameworks for Auditing and Control Self-assessment**

The most common international frameworks and standards for evaluating internal controls and risk management related to information, as required by business activities, are shown in figure 1.

The control frameworks with the highest level of abstraction are at the top in figure 1; these include the Committee of Sponsoring Organisations of the Treadway Commission’s *Enterprise Risk Management Framework* (COSO ERM) and the IT Governance Institute’s *Control Objectives for Information and related Technology* (COBIT) and Val IT frameworks. These frameworks provide information on what is needed to achieve internal controls—controls that are more on the strategic, managerial level. The British Office of Government Commerce’s *IT Infrastructure Library* (ITIL) and Carnegie Mellon University’s Software Engineering Institute’s *Capability Maturity Modeling Integration* (CMMI), for example, provide detail on how to realise better controls on the more tactical and operational level in the organisation.

**Business Governance Assessment Using COSO ERM**

A couple of years ago, Pension-Fennia began organising internal control self-assessments inside its business entities by using the COSO ERM model. Evaluations were facilitated by internal audit and the subjects were discussed with the responsible managers and executives following the COSO ERM model’s different layers: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. The discussions and the resulting agreed-upon improvement actions were documented and integrated into the continuous planning process of the organisation.
IT Governance Assessment Using the COBIT Framework and Maturity Models

More than a year ago, Pension-Fennia’s chief information officer (CIO) and the chief audit executive (CAE) had a discussion concerning the IT function’s aim to gain an even better understanding of the needs of business to achieve better quality IT services. To this end, the CIO and CAE realised the need to gain better insight into the controls used in IT and they decided to start an evaluation process using COBIT’s maturity models.

COBIT’s maturity model proved to be a very useful tool for the IT professionals. The maturity model enables IT to define the actual level of controls and set the maturity ambition level to deliver the required service to the business. After all, the key objective of IT is to ensure reliable, effective and efficient services that are aligned with the business’s objectives.

The COBIT model groups all information and IT activities into four domains, which are articulated into 34 processes (see figure 2).

Within every individual process of COBIT, it is possible to evaluate the current maturity of its control using the maturity evaluation grid tailored for each process (figure 3).

Pension-Fennia’s IT function started the self-assessment process by attending a two-day training to gain a better knowledge of IT governance and the COBIT framework. Subsequently, IT management evaluated 24 processes in the course of a few months. During the training and the self-assessment, IT collaborated closely with an external expert. The IT managers evaluated the present maturity levels of controls over each process and the level of ambition to which they aspire. To bridge the gap between present and future levels, they prioritised the improvement actions. These actions were integrated in an IT governance improvement plan. This plan included not only the actions to be performed internally in the IT entity, but also the improvement actions to be accomplished within all business entities and outside service providers.

The relationships, roles and responsibilities amongst IT, business entities and outside service providers are described in figure 4. The abbreviations mentioned in the figure refer to different COBIT processes presented in figure 2.

As visualised in figure 4, the COBIT framework covers the relationships of IT with the business entities, the outside service providers and the organisation’s executive management.
Combining Business and IT Governance Issues

The COSO ERM framework does not cover maturity aspects, but Pension-Fennia wondered if it was possible to use COBIT’s maturity approach and extend it into COSO ERM. Even further, is it possible to combine the two frameworks? Pension-Fennia’s staff found that it was.

They did so by continuing to mould the discussion model based on COSO ERM, described previously. They attached to it several areas related to the development projects of the organisation’s COBIT self-assessment. Furthermore, they combined the two risk management layers inside COSO ERM into one layer in their approach. Last, in COSO ERM, the internal environment is the first layer, but in Pension-Fennia’s model, it was the result of the evaluation of the first six layers. That meant the internal control culture changed from the starting point to the outcome of the project.

To better facilitate the discussions amongst the company managers and executives in a structured manner, a questionnaire was created that contained the following six layers as in figure 5:

1. Planning of activities
2. Risk management process (evaluation, assessment, response and monitoring)
3. Daily operations (including segregation of duties)
4. Information, security and continuity
5. Reporting and information
6. Monitoring

Every layer in the questionnaire is divided into three parts. The first part consists of questions related to that layer. For example, layer four (information, security and continuity) includes questions related to sensitivity and criticality of information, segregation of duties, roles and responsibilities, management of data, information security, business continuity planning, and resource management.

The second part in every layer consists of a list of supporting documents requested, such as the entity’s strategy, process descriptions, control instructions and documents, productivity objectives, job descriptions, and minutes of the entity’s meetings.

In the third part, the maturity of controls is evaluated with the help of different criteria, such as systematicness, regularity, level of documentation, conformity to enterprise risk management (ERM) and business planning, quantity, and quality and validity of reports. To situate this maturity, Pension-Fennia used the generic maturity model for internal controls, as published in appendix III of COBIT.
Conclusions From the Project

While carrying out discussions with managers and executives and when evaluating the results of the discussions, Pension-Fennia came to the conclusion that all parties—business units, IT and internal audit—benefitted greatly from the project. The business managers and executives received a useful and down-to-earth tool, with which they are able to evaluate the pertinence of their internal control activities and determine the need for further control development activities. This tool also deepened the synergy and mutual understanding between business units and IT, as well as between IT and its service providers.

By using this combined approach, together with the results of the COBIT project, the organisation was able to clarify the mutual goals and roles and responsibilities of its business units. Furthermore, the COBIT self-assessment has been credited with deepening the managerial skills of the organisation’s IT managers and their insight into control issues.

For internal audit, the two combined projects represented an opportunity to introduce authoritative, comprehensive control frameworks into the organisation and also to develop synergies, as well as an improved understanding between IT and non-IT auditing.

The methodology described in this article for defining the status of overall controls at Pension-Fennia is now used regularly in the organisation. The first ‘round’ created the basis for a common understanding of controls. The aim for the following rounds is to continue to strengthen collaboration between the business and IT.

Tuulikki Help

is the CAE of the mutual insurance company Pension-Fennia, Finland. Previously, she served as chief financial officer (CFO) in several Finnish financial and construction companies. Help was a board member of the Institute of Internal Auditors (IIA) Finland and the chair of the IIA Finland Seminar Committee during 2003-2005. She has spoken at many seminars and has written articles on internal audit, business and IT governance, and risk management.
Hidden within innumerable software applications in use every day by countless companies and organizations is one of the greatest security risks and challenges. As security threats shift away from attacks on the network perimeter protected by firewalls and intrusion detection devices, security attacks have become more focused on software applications and their links to data repositories. The Gartner Group reports that more than 70 percent of current business security vulnerabilities are found within software applications rather than the network boundaries. The financial risk to companies resulting from these attacks is not benign; it has been documented that businesses spend billions of US dollars each year recovering from these security breaches.

Although the risks to companies from insecure software code are increasing in number and cost, this area has been largely ignored by most software engineers, security professionals and IT auditors. Oftentimes software developers consider security “that other department” that organizes penetration tests immediately prior to software’s release. Rarely are the results of these penetration tests fed back into software development as lessons learned. In discussions with members of development and security teams, the authors have found that developers often believe that the security team knows nothing about software development. Conversely, the security team believes that security issues and their resolution belong to them alone. Unfortunately, it appears that there is no acknowledgment on the part of either group that software construction itself may be the cause of multiple security vulnerabilities and threats.

It is quite disconcerting that there is no current standard in the domain of IT auditing to assess compliance with secure software development best practices. This absence of a standard contributes significantly to the state of confusion as businesses try to address this absence on their own. Consequently, much of the current software, both in development and production, continues to be rife with security vulnerabilities, errors and flaws.

The lack of knowledge and standards in secure software development became quite evident to the authors when they examined the certification training and practice of security professionals. The result—little to no mention of the topic—is in stark contrast to the role of the IT auditor who has “always been responsible for consulting with management to help ensure that sufficient and adequate internal controls exist within organizations to mitigate major risks…” Although the insecurity of existing software and its associated risks have been documented clearly, the auditing profession has not yet developed criteria to assist management in the identification and mitigation of these risks.

The software engineering, security and IT audit professions cannot be blamed exclusively for this void of guidance. Educational institutions must accept a part of the blame. Software development companies have stated that higher educational institutions have failed to educate software developers and security professionals on the issues surrounding software security. “New college and university graduates in computer science and related disciplines generally lack the training necessary to join the workforce ready and able to design, develop or test secure software.”

In view of this absence of guidance for assessing secure software development practices and the compelling need to better manage these vulnerabilities, the authors have engaged in this research effort to establish an IT audit protocol, questionnaire and supporting documentation for secure software development guidance and assessment. The authors believe that these tools will provide both the software development and security functions with knowledge and guidance on how to establish practices that lead to secure software applications.

Before a guidance document can be developed, an understanding and acceptance of best practices must be established—a distinct challenge in a new, developing area like secure software development. The authors have accepted this challenge as the validity of their research effort depends on a strong foundation. Therefore, the authors began their research effort with an exploration and extraction of secure software development best practices from both the software development and security domains.

### Secure Software Development Best Practices

According to the American Society for Quality Control, best practices are determined through “the process of improving performance by continuously identifying, understanding, and adapting outstanding practices and processes found inside and outside the organizations.” In the domain of software development, the establishment of best practices follows this process. Companies such as Microsoft Corp. that have reduced their application security risks
Developers must begin to see their software in the same light as attackers do.

significantly have been identified and their underlying practices examined. Notably, research has found that companies that implement these secure software development practices can recoup a 21 percent return on their investment when the costs of security breaches are taken into account.6

It is an underlying premise in the information security domain that the most important factor in establishing secure practices is the institution of a security policy with strong management support.7 Without an industry-accepted guide on how to secure software development best practices, organizations remain unable to determine how to institute these policies and practices beyond a general statement of support.

One common sentiment across the current practice and research on secure software development is the need to focus on security in every phase of the software development life cycle (SDLC).8 The need to establish a common framework for software development activities is detailed in Control Objectives for Information and related Technology (COBIT), which is globally accepted and provides “a comprehensive framework for managing risk and control of information technology.”9 Specifically, COBIT control objectives P08.2 and P08.3, from the Plan and Organize domain, delineate the need to identify, adopt and maintain quality-focused standards, procedures and practices for application throughout the SDLC that include the need for secure development methods.10

Therefore, based on current practices and adopted standards, the application of secure software development practices in each phase of the SDLC was found by the authors to be a best practice that establishes a solid foundation on which to build audit tools. The SDLC consists of a series of phases that occur during the creation of a software application. Requirement gathering is the first phase, where stakeholders identify functional and nonfunctional requirements against which the software is developed.

The next phase is design and analysis, during which the requirements are translated into logical models to clarify functional and nonfunctional requirements against which the software is developed. Testing is the SDLC phase where the verification and validation of the functionality of the software against the requirements is assured. Last, deployment and maintenance is the phase where the software is implemented in a real-world environment and modified or enhanced as needed.

“Because security is not a feature, it can’t be bolted on after other software features are codified, nor can it be patched in after an attack has occurred...it must be built in from the ground up.”11 For a development team to create secure software, it must be able to anticipate abnormal and threatening behavior at the start of the development effort. The emphasis on requirement gathering has always been on identifying desired and normative behavior through “use case” scenarios and diagrams that visually depict the desired action of the software to user and system requests. To develop secure software, however, developers must begin to see their software in the same light as attackers do, and, for many, this is a difficult concept to grasp. As a result, identification of security requirements has been ignored largely during the requirement gathering phase. Even when organizations try to include security issues during the requirements phase, they often use inadequate techniques. “In many cases these methods are not oriented towards security requirements and do not result in a consistent and complete set of security requirements.”12

To accurately identify security requirements, different elicitation methods are required, the most common of which is the use of “misuse cases.” While a use case describes desired behavior for systems to perform, misuse cases describe undesired situations and behavior that may occur and must be prevented or mitigated. However, there is an important caveat to the effectiveness of misuse cases. To be used successfully, developers must be familiar with common attack patterns used to exploit software systems, such as injection vector attacks, where an attacker attempts to perform an input-driven attack such as a buffer overflow.13

One advantage to using misuse cases is the familiarity most developers have with using the tool. Misuse diagrams reuse the familiar concept of actors and actions with a different focus: security attacks. Misuse diagrams generally focus on the identification of several common elements, including the identification of internal and external attackers who may use the system in unexpected and malicious ways. Misuse cases can also identify the objective of the threat from the attacker’s viewpoint in terms of data breaches or other malicious activity. As a result of their effectiveness in identifying potential vulnerabilities, the authors consider misuse cases to be a best practice in the requirement gathering phase of secure software development.14

The design and analysis phase of the SDLC translates the requirements into models that specify the information flow, data structure and architectural design of the planned software. Many standard modeling techniques are used by software developers during this phase, including data flow and entity relationship diagrams. None of these traditional models focus on identifying and modeling security risks and vulnerabilities.

Threat modeling is a technique specifically focused on identifying and documenting software application-level security risks. It examines each entry and exit point in the software as well as the paths where data pass from a trusted to an untrusted environment. Threat models also include a reference to the value of the information assets the application contains. It examines a software application from an adversary’s perspective to anticipate attack goals.15 Threat modeling also seeks to understand the value of data from the business perspective and how an attacker could benefit from accessing that data.16 Through the use of threat models, vulnerabilities and potential threats can be identified along with the design of mitigating constraints to prevent the attacks from being successful. The authors have identified threat
Many security vulnerabilities are introduced in the coding phase of the SDLC. “Most software vulnerabilities are the result of small but reoccurring programming errors that could be easily avoided….”24 Software developers need to understand that the impact of certain programming decisions can lead to software vulnerabilities. Through the use of techniques such as misuse cases and threat modeling, the software development team becomes aware of the security risks against which its code needs to guard. However, because most software developers have had no formal training in secure software development, even with the best intention they may not have the knowledge or experience to mitigate the potential security issues.18

Therefore, in the research for this article, two security-focused processes were considered to be best practices for use within the code construction phase. These are the use of secure software checklists and software inspections. The use of secure software checklists has been recommended by several researchers.19 These checklists provide detailed guidance to software developers on common coding errors that can result in significant security vulnerabilities. Software code inspections can net substantial improvements in secure software development during which time the code is reviewed by senior developers familiar with security issues. Based on the positive results these processes bring to the coding phase, the authors consider them to be best practices for secure software development.

Unfortunately, code checklists and inspections do not reveal all potential security vulnerabilities, particularly as they relate to concepts of data classification and integrity. For example, if the organization requires the classification or encryption of information, software developers must understand how to ensure the classification, confidentiality and integrity of stored information when it is collected by these software programs.20 The requirements of data storage and transmission must also be addressed during the development of the software. For example, encryption requirements cannot be bolted on at the end: they must be built into the software application from the start.21 Closely related to data integrity are data access and authentication requirements. Proper access controls and authentication must be designed and developed into the software applications as well as the logging of auditable information related to these controls.22

The testing phase of the SDLC is critical, as at this point the software is verified and validated to be secure to the desired level of acceptability. Each set of security strategies employed during the development of the software must be validated through testing. Several of the design and coding tools previously described can provide feedback into the testing phase and assist in the creation of test scripts. For example, misuse cases can become the basis for test cases, threat models can become the basis for penetration tests, and encryption requirements can become the basis for encryption testing.

Security testing requires a paradigm shift on the part of the traditional tester or testing team. The traditional software tester is focused on verifying that the software fulfills all the functional and operational requirements. However, in security testing, the tester has to think like an attacker and develop test scenarios to uncover potential vulnerabilities.23 Tests must be designed that specifically input problematic data or attempt to access a back-end database. The first step in security testing, therefore, is to identify the application’s attack surface, which identifies all the potential avenues of input possible to maliciously manipulate the application. Penetration tests have been used historically to identify security vulnerabilities. However, the timing and use penetration testing needs to be adapted to better assist in identifying threat and vulnerability software applications. “Perhaps the most egregious mistake made in penetration testing processes, from the standpoint of their applicability to software development, is that they’re almost always applied far too late in the life cycle.”24 Penetration testing should be used early in the SDLC, as a form of stress testing a software system, to determine signs of vulnerability or breakability.

Adding these security elements to the testing phase requires a significant investment. However, the investment is worthwhile, as it is uniformly accepted in the world of software engineering that preventing errors early in the software life cycle is significantly more cost-effective than correcting errors after deployment. As a rule of thumb, every hour an organization spends on defect prevention will reduce repair time, from three to 10 hours, of reworking a software problem. Once the software is in operation, such repairs typically cost 50 to 200 times what it would take to rework the problem in the requirements stage.25 Additionally, waiting until after deployment to address security issues can cause damage to a company beyond the costs of correcting the error, such as damage to reputation and credibility, customer perception, liability, and other legal issues.26

Although testing is often viewed as the last phase of software development, the activities related to deployment and maintenance also need to be addressed. The security landscape is changing daily, and it is often the case that a new security threat emerges between the time that requirements were first gathered and the application’s deployment. The authors believe that Microsoft’s practice of a security deployment review27 constitutes a best practice in the domain of secure software development. Prior to the final release of a product, Microsoft requires a final security review by an expert team of security professionals. Microsoft’s best practice extends beyond the mere review of the application. If the application does not pass this final security review, corporate policy mandates that the application returns to development and its release schedule is placed on hold.

Once a software application is deployed, it is considered to be in the maintenance phase. Software maintenance is considered the longest phase of the software life cycle, often calculated to be 70 percent of a software product’s life, during which defect repairs and enhancements normally occur. The authors consider it a best practice for organizations to extend their security practices to this phase. As new threats and vulnerabilities are identified, they must be addressed in...
software patches or new versions and incorporated into current and future development projects.28

**The Need for Secure Software Development Audits**

As noted previously, IT auditors are responsible for “consulting with management to help ensure that sufficient and adequate internal controls exist within organizations to mitigate major risks to a reasonable level.”29 With significant amounts of money at stake, a risk assessment suggests that the potential costs associated with security breaches in terms of actual revenue loss, down time and reputation far outweigh the costs of instituting a secure development methodology. Certainly, in terms of secure software development, the evidence indicates the need for “sufficient and adequate internal controls”30 to prevent and mitigate the potential risks associated with a lack of compliance with secure software development best practices.

Security audit guidelines’ standards have been a valuable tool historically to assist auditors in the evaluation of systems and controls. These standards are designed to provide guidance for the evaluation of information systems. Although the coverage of existing standards is quite broad, none of them include a reference to secure software development. This is a void in guidance. The focus of this article, and the research on which it is based, is to address this deficiency and provide guidance for the evaluation of information systems. Although the costs of instituting a secure development methodology.

**Conclusion**

Developing accurate information security audit criteria depends upon identifying best practices. This requirement is no different when security is applied to software development. Through this research effort, a comprehensive examination of software development processes and practices was performed to identify secure software development best practices and strategies. These findings have been synthesized into a proposed audit questionnaire with which companies can assess how well their internal secure development practices comply with those recommended by researchers and companies.

**Endnotes**

10 IT Governance Institute, COBIT 4.1, 2007
12 Op cit, Mead
13 Op cit, McGraw 2004
15 Swiderski, F.; W. Snyder; Threat Modeling, Microsoft Press, 2004
16 Ibid.
18 Op cit, Lipner and Howard
20 Op cit, Harris 2005, Tipton and Henry 2007
22 Ibid.
23 Wysopal, C.; D. Zovi; The Art of Software Security Testing, Addison-Wesley, 2007, p. 8
Oezlem Aras
has worked for several years in the manufacturing environment with small and large Fortune 100 clients. She has experience in internal auditing and training including the specific areas of quality and safety. She is currently preparing for CISA and CISSP certification, pursuing professional opportunities in the field of IT security and information assurance, as well as continuing research in the area of secure software development audit and IT controls. She can be reached at lalia_mia@hotmail.com.

Barbara L. Ciaramitaro, Ph.D., CISSP
has many years of academic and professional experience in a variety of IT areas, including software development, quality assurance, networking and security. Prior to joining the academic world, she assisted Fortune 50 clients in establishing secure software development and implementation practices as well as business process redesign. She is currently pursuing research focused on integrating secure software development practices into traditional software engineering methodologies. She can be reached at bciaramitaro@walshcollege.edu.

Jeffrey Livermore, Ph.D.
has experience in both the academic and professional worlds of IT. Prior to joining the academic world as department chair, he acted as chief information officer for both an academic institution and major medical research facility and was responsible for all aspects of technology deployment, including security and information assurance. He is a frequent speaker at conferences and has published several articles on software development methodologies. Livermore is currently conducting research in several areas of information assurance. He can be reached at jlivermore@walshcollege.edu.

Val IT™ 2.0
An Entirely New Framework Addressing the Governance of IT-enabled Business Investments

Val IT™ is the most complete collection of proven management practices and techniques for investment in business change and innovation. It helps companies to make better decisions on where to invest—ensuring that they are doing things the right way, doing them well and reaping the benefits.

- Includes IT services, assets and other resources
- Aligns terminology with Control Objectives for Information and related Technology (CoBIT®)
- Adds management guidelines with detail about Val IT processes and key management practices, as well as maturity models for each Val IT domain

Start fostering the partnership between IT and the rest of your business today—download your free copy of The Val IT™ Framework 2.0 at www.itgi.org/valit.
IT Governance Roundtable:  
Boston, November 2007

Thank you to the IT Governance Institute (ITGI) for providing this content for reprint. The original publication, of which this is a summary, IT Governance Roundtable—November 2007, is available for download at www.itgi.org. This content is the result of the discussions that took place in November 2007, in Boston, Massachusetts, USA. This and planned future roundtables are intended as opportunities to learn more about the real-life situations professionals are facing in regard to IT governance.

The participants at the November event included:
• Paul Williams, Principal, Paul Williams Consulting, UK
• The Honorable Robert T. Howard, Assistant Secretary for Information and Technology, US Department of Veterans Affairs, USA
• Pauline Jorgensen, Head of IT Security and Business Control, British Airways, UK
• Halina Tabacek, Senior Director of IT Business Planning and Management, Sun Microsystems, Inc., USA
• A vice president, risk management, for a financial services firm, USA, who wishes to remain anonymous

What does IT governance mean to your organization?

Halina Tabacek (HT): We have been working to define IT governance for a number of years. The definition has changed over time. Its origins were in control and measurement but it has moved and progressed into more front-end planning, putting the processes in place. It is more preventive, rather than taking action afterwards. It is the framework to do business, make decisions and monitor progress.

Robert Howard (RH): I completely agree; that really is what governance is. It also provides the framework, mechanisms and methodology for involving the people, from those you support to those who provide support, and the boards that meet and deliberate so that people feel they have a say. When someone says “governance,” a lot of people think about how they will fit into the process. Governance is about controlling things, better management of what is going on, and a more responsible look at where we are putting our efforts.

Vice President (VP): I tend to think about it from our point of view and that is: alignment with business needs, delivering consistency, sustainability and accountability for all our IT processes.

Paul Williams (PW): One of the things within ITGI that we have tried to do recently is change the emphasis from IT governance to enterprise governance of IT because we found that, within a lot of organizations, it can often mean the governance of the information technology itself rather than IT’s ability to provide support to and enable the business. That is one of the reasons that our certification is called Certified in the Governance of Enterprise IT™ (CGEIT™), to bring out the enterprise emphasis.

How did your organization embark on the IT governance journey? What was the catalyst?

HT: The catalyst was an inquiry from the board of directors about what methods IT was using for governance. The inquiry contained a reference to Control Objectives for Information and related Technology (COBIT) and no one within the organization at this time was familiar with COBIT. An external board member, who was on the audit committee, was well-versed in the COBIT framework. The CIO embarked on COBIT research to understand what COBIT is and subsequently created a mandate to incorporate its use. It took some time for us to understand what it means to follow COBIT.

RH: For us it was a US Congressional committee—what they saw going on within the US Department of Veterans Affairs (VA), the inability to explain where money was going within the IT arena, and visits to VA hospitals that had a wide variety of ways of operating. A lot of the pressure to reorganize came from Capitol Hill, from the oversight committees, primarily from the House of Representatives side. The House Veterans Affairs Committee has a subcommittee for oversight. Initially, a lot was centered on money and what was going on because of an inability to explain what was going on with the projects and why they never seemed to come to closure. A lot of employees, though, were familiar with COBIT and IT Infrastructure Library (ITIL).

Pauline Jorgensen (PJ): Governance needs to be widened to cover the whole organization, not just IT. There can be a tendency to focus on IT and forget about the governance of the rest because it’s easier to focus on IT.

PW: It is good to see the drive being initiated and sponsored at the board level. Ideally, the initiative should not start within IT. It needs to be properly sponsored by the business and be accountable to the business.
VP: The need for governance comes from the way the company is organized. We are a hybrid organization—we are both centralized and decentralized. Our technical platforms are running as almost separate entities, but report up to a central technology group, so there is a need to make sure everyone is speaking the common language, especially to all our technology groups providing centralized oversight. We have a need to deal with all the internal and external audits, as well as our lines of business, and having all the technology groups looking at things differently created significant problems.

Did you find the COBIT framework helpful? What are your impressions of COBIT as your framework for governance?

PJ: It is particularly useful that COBIT provides a common language that everyone can understand. The stimulus to use COBIT within our organization came from various places, not just in IT. The current version of COBIT is considerably better than the previous one. It has helped us benchmark and assisted with common understanding, and it has been useful in explaining issues to people who do not work in IT all the time.

PW: Have you found that your audit people use it as well?

PJ: Yes, external and internal audit.

PW: So, again, it provides a common language right across the board.

VP: With the newest release of COBIT, there is a higher level of awareness; we are going through, trying to look at it as putting it into the whole central governance model. There is more consistency around everyone speaking the same language. With COBIT 4.1, there is more significant work that we can more easily adopt. We have had someone who has given us some education on it, but it needs to be a regular, more consistent awareness, from our point of view.

RH: It does help explain things to senior officials with a sensible framework; it just seems to make sense. Checklists are enormously helpful. We did not need to put into place or explain the whole methodology, the whole business or controls—just the use of checklists in some of our compliance activities that draw on COBIT to some degree.

PW: What specifically kicked off the use of COBIT? Where did the initiative to use it come from? Was it internal or external?

RH: External and internal heat. When a decision was made to go forward with the reorganization (this took a year or so), it was because of pressure from Congress, some analysis conducted by Gartner that pointed out the benefits that would come from centralization, and security issues. The decision to reorganize (that is, centralize) was coupled with hiring a company to come in and help—in our case, IBM. IBM brought the knowledge of COBIT, but we had a few who were already knowledgeable and had a good understanding of COBIT’s processes and methodologies. Most of the expertise came from IBM; they brought in specialists in this area. We tried to immerse ourselves as much as we could. We use a mixture of ITIL and COBIT.

PW: One of the questions I am often asked by people who probably don’t quite understand is “Should I use COBIT or ITIL?” My response is that you should use a combination of these things. Does that apply to you as well?

Group: Yes.

PW: Have you found that they integrate pretty well?

RH: ITIL is the library of best practices and it changes all the time. COBIT is not necessarily that way; it is focused on a list of controls used to tighten things down, as in “these are the things you need to worry about.” They are different.

PJ: They do not conflict.

Are COBIT’s maturity models useful for the rest of you?

PJ: We do use the generic COBIT maturity models. We set a target according to what the risk is, work out where we are and work on what we need to do to bridge the gaps. The only thing I would say is that sometimes the definitions make it a bit difficult to differentiate between two levels. Sometimes for one area you find you meet certain elements of multiple levels of maturity, but not others. You have some of this one and some of that one, so where do you put yourself?

PW: One of the key things for people to recognize is that they do not need to be on level five on everything. A lot of organizations, when they start off, think that COBIT is too prescriptive and they have to do everything that goes along with it, and you just can’t do that. It is a matter of recognizing the processes, of looking at where you are currently and where you want to be. An organization can be anywhere on the individual scales, depending on its risk and the type of business it is in.

VP: The framework has been helpful, from our point of view, because it guides self-assessment. It helps provide consistency when you have to self-assess because it gives you certain criteria.

PW: I think ‘COBIT evangelist’ is a great term. I think that every organization could benefit from actually having one. One of the concerns that is raised within large organizations is that it is difficult to find people who have real in-depth knowledge of COBIT. Although there is a fairly low-level certification program for learning COBIT—the COBIT Foundation Course—increasingly there are people who are setting themselves up as COBIT consultants. But true COBIT
expertise is still relatively immature in many places, so there can be difficulties in actually getting people who really do understand it. In your organization, for instance, did you use external consultants or was that something that you developed from the inside out?

PJ: We had a COBIT evangelist already in place in our security department—one of the IT people.

PW: That’s good, because we tend to find that evangelists usually come from the audit side because that’s where COBIT started 15 years ago.

When you endeavored to engage the business in IT governance, what were the challenges and how did you overcome them?

RH: People were upset that we were taking their localized IT people away. That’s the struggle we went through. There was great resistance to doing that until finally the Secretary said, ‘Sorry, this is the way we are going to do business’.

What have you done to address the value side of IT governance?

RH: We spent great effort on tightening controls. Now we must figure out a way to provide better service. That’s going to be hard. Staffing problems were discovered and, in some cases, we clearly do not have the people we should have, so we have to figure that out from a contract side. …We’ve tightened our controls with COBIT, now how do we actually do it and enhance delivery?

Has ITGI’s Val IT framework been helpful?

HT: There are elements of Val IT that we were already doing, even without the framework, which represents the entire value chain. The framework helps put it in perspective. Another key is a distinction that was made earlier: the fact that it is enterprise governance of IT, not IT governance. There is currently a very large initiative to perform a major upgrade to our enterprise resource planning (ERP) system. It is very much a business-driven initiative, which is very fortunate and the right way to do it. All of the savings and return on investment are focused on the entire enterprise. It isn’t strictly what we are going to save in IT by doing this because there is a tremendous investment being made in IT, but it’s really how the business organization is going to benefit from the deployment of this IT infrastructure. Once the project is completed, it is going to be such a big component of our IT infrastructure that I think it is the tide turning for the foundation for us to look at it enterprisewide.

PW: I think the key thing with Val IT is to start off with its 10 principles, including measuring benefits across the life cycle, taking the full scope of activities including the business change cost, and so on. I think that is the logical place to start. Val IT is relatively new; it has been available only for about a year. It is very much aimed at covering the more subtle angle within governance, which is the value rather than just compliance and control, although they are all interlinked.

What hints and tips can you provide to organizations beginning on the IT governance journey?

PJ: Make sure you base it on risk. Do not try to be perfect at everything. Also, do not look just at your own risk, but at everyone else’s as well.

HT: Leverage external organizations, whether it’s something like ITGI or research firms like Gartner or Forrester. They can do benchmarking for you and bring those best practices in to give you a running start.

RH: In hindsight, based on what we went through, we should have gotten a very thorough assessment of existing conditions throughout the VA. You had better know what you are going to inherit. We didn’t do that to the degree we should have. Now we are discovering what we have inherited and there are a lot of problems that have to be cleaned up.

VP: Having the right management support has been important. You have to know that the process can work and is going to help, but do not expect overnight results. You have to look further down the road and recognize this is going to be a challenge. It’s really having the right support and the right mindset to get the undertaking going.

PJ: Build the change into the life cycle, but do not do it in isolation. Make sure you don’t make things worse while you are busy fixing things to make them better!

Editor’s Note:
Additional responses to these questions as well as more questions and answers can be found in the full IT Governance Roundtable—November 2007, available for download at www.itgi.org.
Gan Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCSA, BS 7799 LA is the global IT security lead for a global 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 4 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 As a preventive measure, should an organization go for anti-virus solutions from multiple vendors? My organisation uses different vendors for both servers and workstations and it is more due to accident/historical reasons, than by design. My question is about using products from two different vendors for the same workstations/servers to make sure that there is redundancy in terms of controls.

A Without exactly knowing the details of your current organisation, I am afraid that I cannot give a straight answer. Unless your organisation handles certain mission-critical information, which is very key and fundamental to the business, and, at the same time, has exposures to potential virus attacks, I do not see any reason why you should opt for a dual-vendor solution.

It is fashionable sometimes to claim that there are extra controls to make the place look more secure, but, in effect, the second solution adds extra costs, but very little value.

Q As a regular reader of your columns, I feel that you dislike security certifications. Why so?

A Let me make it very clear that I am not anti-certification; I do believe that there is a value in obtaining certifications.

My concerns are as to how certain organisations go about it. In India, for example, the ISO 9000:2000 certification is so common and widely used; airports, educational institutions, hair dressing salons and barbershops have been certified. My worry is whether ISO 27001:2005 will go the same way.

There was a debate at a recent seminar at which I spoke: someone asked the speaker from a certification body whether they have ever revoked a given certificate. The answer was a clear no! It is a plain business opportunity to both the giver and the receiver. Today, there are multiple certification bodies of different sizes and profile, and it really depends on the kind of auditor who comes and does the audit. On many occasions, I have seen auditors who have no clue about IT performing a 27001 audit; equally, I have seen some true experts.

In my personal opinion, achieving security certification and security excellence can be two different parallel objectives. Just because the entity has achieved security certification, it does not mean that it has achieved security excellence. Achieving security excellence is a long and a continuous journey. It is never a destination, but, equally, certification is a starting point.

Q I would like to do an audit of business continuity planning (BCP) testing processes. Can you please help?

A In one of my earlier columns, I have answered a question as to how much testing is enough. I would like to draw your attention to that particular column as well.

The following should provide a quick checklist, but please note that it is not exhaustive:

• Obtain the test results, if any, available for review.
• Determine the extent to which the business areas deemed or categorised as critical have tested their ability to recover from an unplanned loss of information services.
• Determine whether the entity’s business continuity plans and the planning structure are subject to a regular and ongoing review and testing program. Also, assess whether they have been fully tested, at least once annually.
• Assess if the recovery plan is maintained in a current state of preparedness and has been audited by an independent group within the entity, all the content and any possible changes have been communicated to the relevant staff, and, where appropriate, training has been provided to create awareness and understanding.
• Ascertain whether the recovery test scenarios have been developed for both announced and unannounced test situations.
• Determine if every area of the recovery capability is included in the test plan and/or review procedures. Assess the inclusion of the same in the audit programme and whether such tests have been carried out in practise.
• Determine if the test results have been communicated to executive management, summarising the successes and failures and the required set of corrective actions.
<table>
<thead>
<tr>
<th>Items to Look For</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A daemon running more than once, when there should only be one occurrence of it running, e.g., the inetd daemon</td>
<td>Unless the second inetd is started manually, for which there is no real need, there is no logical reason for the existence of two inetd processes. This can be a symptom of a typical Trojan. On the other hand, please note that some daemons, such as httpd, do have multiple versions running simultaneously.</td>
</tr>
<tr>
<td>An unusually high level of system utilisation, in particular one or more processes using unusually high levels of system resources</td>
<td>Running crack utilities or bogus IRC servers is always processor-intensive and resource-consuming. Something like cryptanalysis is also very processor-intensive and resource-consuming. It is not practical to mask them because that will make them very slow and useless.</td>
</tr>
<tr>
<td>Higher network utilisation. This scenario gets discovered by network management tools that are external to the host in suspicion.</td>
<td>One or more of the internal systems is used as a zombie.</td>
</tr>
<tr>
<td>Any discrepancy between ps, top and /proc</td>
<td>PIDs that appear clearly in top or /proc but not in ps may have been intentionally/maliciously hidden.</td>
</tr>
</tbody>
</table>

- Determine whether, in the last 12 to 18 months, there have been any surprise, unannounced tests of the business continuity plans.
- Assess whether the standby power generators are tested regularly to ensure that they are in proper working condition.
- Assess whether the primary power supplies are properly equipped.
- Determine if the alternate or backup equipment’s configurations are checked at least quarterly for changes and alterations that can potentially impact the compatibility, in the event of a recovery.
- Assess whether the transportation facilities for disks, tapes and other essential components have been clearly defined and tested for practicality.
- Assess whether the backed-up information is restored on a regular basis and tested for accuracy.

**Figure 1—What to Look for and Why**

<table>
<thead>
<tr>
<th>Items to Look For</th>
<th>Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A daemon running more than once, when there should only be one occurrence of it running, e.g., the inetd daemon</td>
<td>Unless the second inetd is started manually, for which there is no real need, there is no logical reason for the existence of two inetd processes. This can be a symptom of a typical Trojan. On the other hand, please note that some daemons, such as httpd, do have multiple versions running simultaneously.</td>
</tr>
<tr>
<td>An unusually high level of system utilisation, in particular one or more processes using unusually high levels of system resources</td>
<td>Running crack utilities or bogus IRC servers is always processor-intensive and resource-consuming. Something like cryptanalysis is also very processor-intensive and resource-consuming. It is not practical to mask them because that will make them very slow and useless.</td>
</tr>
<tr>
<td>Higher network utilisation. This scenario gets discovered by network management tools that are external to the host in suspicion.</td>
<td>One or more of the internal systems is used as a zombie.</td>
</tr>
<tr>
<td>Any discrepancy between ps, top and /proc</td>
<td>PIDs that appear clearly in top or /proc but not in ps may have been intentionally/maliciously hidden.</td>
</tr>
</tbody>
</table>

**Q** What are the symptoms that a systems auditor or an administrator should look for in a UNIX system where the kernel has been hacked?

**A** Please note that when the kernel has been hacked, even a simple command like ‘ps’ can provide misleading information. Hence, whilst the table in figure 1 is a list of certain things to look for, remember that these are not the only ones.

**Endnotes**


---

**Earn 38 CPE credits.**

Courses include:
- Fundamentals of IT Auditing
- IT Audit Practices
- Information Security Management
- CoBIT: Strategies for Implementing IT Governance

Register online now!

[www.isaca.org/trainingweek](http://www.isaca.org/trainingweek)

---

**15-19 September**
**Edinburgh, Scotland, UK**

**22-26 September**
**Washington DC, USA**

**13-17 October**
**Anaheim, California, USA**

**3-7 November**
**Chicago, Illinois, USA**

**8-12 December**
**New Orleans, Louisiana, USA**
CPE Quiz

Based on Volume 2, 2008—Bridging Gaps Among Auditing, Compliance and Security Worlds
Value—1 Hour of CISA/CISM/CGEIT Continuing Professional Education (CPE) Credit
Prepared by Sally Chan, CMA, ACIS

True or False

Holt Article
1. The key findings of the 2006-08 IT Governance Study Group was that there was no better foundation than the concise and succinct Australian standard for corporate governance of IT (AS 8015:2005).

2. The draft ISO/IEC DIS 29382, based on AS 8015:2005, will cover six principles (responsibility, strategy, acquisition, performance, conformance and human behavior) for boards to use to govern IT as an integral organizational asset.

3. With 17 nations represented on the ISO/IEC SC7 IT Governance Study Group, the group's survey found that IT governance activities happening across the globe are quite similar, and have no links to a country's business culture.

Ross Article
4. Resilient systems rarely fail, but if they do, it is possible to recover them. Resilience = Availability + Replication + Recoverability.

5. A resilience master plan would put forth, at the very least, a business case to substantiate the expenditure and demonstrate the period of time in which that investment could be recouped.

Thorp Article
6. The current interest in value management is not driven by the factor of increased transparency. It is unrelated to regulations such as the Clinger-Cohen and Sarbanes-Oxley acts in the US.

7. In a 2006 survey of 150 senior executives worldwide, the Economist Intelligence Unit, in conjunction with Deloitte, found that more than 50 percent integrated their project/program tracking into their ongoing performance management process.

De Haes and Van Grembergen Article
8. IT governance can be set up using a variety of structures, processes and relational mechanisms. Relational mechanisms are crucial in the IT governance framework and paramount for attaining and sustaining business/IT alignment, even when the appropriate structures and processes are in place.

9. The authors reported that the Control Objectives for Information and related Technology (CoIT) framework is receiving a lot of attention in literature and in the field, yet with regard to ease of implementation, it scores just above average.

10. An IT governance practice that was used by the researched organizations, but not promoted by experts and thought leaders as being very important, is having the IT strategy committee at the level of the board of directors.

Leo Article
11. Malware (malicious code) writers have discovered that clients attached to high-speed wireless and wired networks are a powerful means to spread infections. Clients have become the source of distributed network attacks on servers and, more important, applications.

12. The issues of end point security need to be addressed from two different planes: protecting the end point and protecting the enterprise from the end point.

13. Some of the challenges that one must gear up for while implementing end point security products include session and transport security, quarantine and reporting/monitoring.

Sandrino-Arndt Article
14. Situating IT governance in the prevailing enterprise governance context is a key success factor for effective IT governance implementation. In this regard, understanding the relationship between IT governance and enterprise governance is essential.

15. The 3P model proposes a programmatic methodology that eliminates the need to leverage existing enterprise governance when defining IT governance bodies.

Pironti Article
16. Information security defines the areas of an organization’s information infrastructure and identifies what information to protect and the degree of protection needed to align with the organization’s tolerance of risk. Information risk management identifies threats, develops and implements controls, and monitors the effectiveness of these capabilities on a regular basis to ensure alignment.

17. The role of the information security organization in the risk management model is to identify and evaluate threats and vulnerabilities to the information assets and the information infrastructure of the organization.

18. The information risk management organization is a business unit within the enterprise that provides advisory services as well as operational activities to provide value. It is the maturation and evolution of information security within an organization.
Information Systems Control Journal
CPE Quiz
Based on Volume 2, 2008—Bridging Gaps Among Auditing, Compliance and Security Worlds

Quiz #119 Answer Form

(Please print or type)

Name______________________________________________

Address ____________________________________________

__________________________________________________

__________________________________________________

CISA, CISM or CGEIT# ________________________________

Quiz #119

<table>
<thead>
<tr>
<th>True or False</th>
<th>Holt Article</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. _________</td>
</tr>
<tr>
<td></td>
<td>2. _________</td>
</tr>
<tr>
<td></td>
<td>3. _________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sandrino-Arndt Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>14. _________</td>
</tr>
<tr>
<td>15. _________</td>
</tr>
<tr>
<td>16. _________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ross Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>11. _________</td>
</tr>
<tr>
<td>12. _________</td>
</tr>
<tr>
<td>13. _________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pironti Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>17. _________</td>
</tr>
<tr>
<td>18. _________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Thorp Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. _________</td>
</tr>
<tr>
<td>10. _________</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>De Haes and Van Grembergen Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>9. _________</td>
</tr>
<tr>
<td>10. _________</td>
</tr>
</tbody>
</table>

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.

E-mail, fax or mail your answers. 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 the year’s end for CPE credits.

A passing score of 75 percent will earn one hour of CISA, CISM or CGEIT continuing professional education credit.

We Cannot Thank You Enough

ISACA would like to thank our sponsors, Program Committee and ISACA Las Vegas Chapter for their commitment to the North America Computer Audit, Control and Security (CACS™) conference. The support of our sponsors and volunteers has helped make North America CACS the world’s leading conference for IT assurance, security and governance.

North America CACS 2008 Program Committee Members

| Michael A. Berardi Jr., CISA (Chair) | Tara Kissoon, CISA |
| IT Audit Manager, Energizer Inc. | Director, Information Security Services, Visa Inc. |
| Michael Juergens, CISA | Jeff Krull |
| Principal, Deloitte & Touche LLP | Senior Manager, PricewaterhouseCoopers LLP |
| Daniel Daniels, CISA | John Tannahill, CISM |
| IT Audit Supervisor, American International Group Inc. | Management Consultant, Tannahill & Associates |
| Harshul Joshi, CISA, CISM | Madeline Parisi |
| Vice President, Information Technology Services, CBIZ | Staff Liaison, ISACA |
| Susan Kennedy, CISA | |
| Information Security Compliance Manager |  |
| Catholic Health East |  |

Sponsors

Gold Sponsors

Ernst & Young

Jefferson Wells

Oracle

Silver Sponsors

Deloitte

Bronze Sponsor

ACL

Protiviti

Qualys
<table>
<thead>
<tr>
<th>Current field of employment (check one)</th>
<th>Level of education achieved (indicate degree achieved, or number of years of university education if degree not obtained)</th>
<th>Current professional activity (if not your title, please select the BEST match)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Financial/Banking</td>
<td>1 One year or less 7 AS 2 Two years 8 BS/BA 3 Three years 9 MS/MA/Masters 4 Four years 10 PhD 5 Five years 99 Other</td>
<td></td>
</tr>
<tr>
<td>2 Insurance</td>
<td></td>
<td>1 CEO, President, Owner, General/Executive Manager</td>
</tr>
<tr>
<td>3 Public Accounting</td>
<td></td>
<td>2 CAE, General Auditor, Partner, Audit Head/VP/EVP</td>
</tr>
<tr>
<td>4 Transportation</td>
<td></td>
<td>3 CISO/CSO, Security Executive/VP/EVP</td>
</tr>
<tr>
<td>5 Aerospace</td>
<td></td>
<td>4 CIO/CTO, Info Systems/Technology Executive/VP/EVP</td>
</tr>
<tr>
<td>6 Retail/Wholesale/Distribution</td>
<td></td>
<td>5 CFO, Controller, Treasurer, Finance Executive/VP/EVP</td>
</tr>
<tr>
<td>7 Government/Military—National/State/Local</td>
<td></td>
<td>6 Chief Compliance/Risk/Privacy Officer, VP/EVP</td>
</tr>
<tr>
<td>8 Technology Services/Consulting</td>
<td></td>
<td>7 IS/IT Audit Director/Manager/Consultant</td>
</tr>
<tr>
<td>9 Manufacturing/Engineering</td>
<td></td>
<td>8 Security Director/Manager/Consultant</td>
</tr>
<tr>
<td>10 Telecommunications/Communications</td>
<td></td>
<td>9 IS/IT Director/Manager/Consultant</td>
</tr>
<tr>
<td>11 Mining/Construction/Petroleum/Agriculture</td>
<td></td>
<td>10 Compliance/Risk/Privacy Director/Manager/Consultant</td>
</tr>
<tr>
<td>12 Utilities</td>
<td></td>
<td>11 IS/IT Senior Auditor (External/Internal)</td>
</tr>
<tr>
<td>13 Legal/Law/Real Estate</td>
<td></td>
<td>12 IS/IT Auditor (External/Internal Staff)</td>
</tr>
<tr>
<td>14 Health Care/Medical</td>
<td></td>
<td>13 Non-IS/IT Auditor (External/Internal)</td>
</tr>
<tr>
<td>15 Pharmaceutical</td>
<td></td>
<td>14 Security Staff</td>
</tr>
<tr>
<td>16 Advertising/Marketing/Media</td>
<td></td>
<td>15 IS/IT Staff</td>
</tr>
<tr>
<td>17 Education/Student</td>
<td></td>
<td>16 Professor/Teacher</td>
</tr>
<tr>
<td>99 Other</td>
<td></td>
<td>17 Student</td>
</tr>
<tr>
<td>99 Other</td>
<td></td>
<td>17 Student</td>
</tr>
<tr>
<td>99 Other</td>
<td></td>
<td>99 Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certifications obtained (other than CISA, CISM, CGEIT)</th>
<th>Work experience (check the number of years of information systems related work experience)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 CPA 5 CPP</td>
<td>1 No experience 4 8-9 years</td>
</tr>
<tr>
<td>2 CA 6 GIAC</td>
<td>2 1-3 years 5 10-13 years</td>
</tr>
<tr>
<td>3 CIA 7 CFE</td>
<td>3 4-7 years 6 14 years or more</td>
</tr>
<tr>
<td>4 CISSP 99 Other</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment due</th>
<th>Current field of employment (check one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ 65.00 (US)</td>
<td>1 Financial/Banking</td>
</tr>
<tr>
<td><strong>Please PAY THIS TOTAL</strong> $ 30.00 (US)*</td>
<td>2 Insurance</td>
</tr>
<tr>
<td>$ 30.00 (US)</td>
<td>3 Public Accounting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method of payment</th>
<th>Certification Programs (see reverse)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✌ For student membership please visit <a href="http://www.isaca.org/student">www.isaca.org/student</a></td>
<td>1 Certification Programs (see reverse)</td>
</tr>
</tbody>
</table>

By applying for membership in ISACA, members agree to hold the association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees and agents, harmless for all acts or failures to act while carrying out the purposes of the association and the institute as set forth in their respective bylaws, and they certify that they will abide by the association's Code of Professional Ethics (www.isaca.org/ethics). Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2008. No rebate of dues is available upon early resignation of membership. Contributions, dues or gifts to ISACA are not tax deductible as charitable contributions in the United States. However, they may be tax deductible as ordinary and necessary business expenses.

**Make checks payable to: ISACA**

**Mail your application and check to: ISACA**

1055 Paysphere Circle
Chicago, IL 60674 USA

Phone: +1.847.253.1545
Fax: +1.847.253.1443

The dues amounts on this application are valid 1 June 2008 through 6 August 2008.
<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Budapest, Hungary</td>
<td>125</td>
<td>$65</td>
</tr>
<tr>
<td>Ireland</td>
<td>156</td>
<td>$40</td>
</tr>
<tr>
<td>Tel-Aviv, Israel</td>
<td>40</td>
<td>$50</td>
</tr>
<tr>
<td>Milan, Italy</td>
<td>43</td>
<td>$53</td>
</tr>
<tr>
<td>Rome, Italy</td>
<td>178</td>
<td>$26</td>
</tr>
<tr>
<td>Kenya</td>
<td>158</td>
<td>$40</td>
</tr>
<tr>
<td>Latvia</td>
<td>139</td>
<td>$20</td>
</tr>
<tr>
<td>Lithuania</td>
<td>180</td>
<td>$40</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>198</td>
<td>$85</td>
</tr>
<tr>
<td>Malta</td>
<td>186</td>
<td>$25</td>
</tr>
<tr>
<td>Netherlands</td>
<td>97</td>
<td>$50</td>
</tr>
<tr>
<td>Abuja, Nigeria</td>
<td>185</td>
<td>$40</td>
</tr>
<tr>
<td>Lagos, Nigeria</td>
<td>149</td>
<td>$20</td>
</tr>
<tr>
<td>Norway</td>
<td>74</td>
<td>$55</td>
</tr>
<tr>
<td>Warsaw, Poland</td>
<td>151</td>
<td>$30</td>
</tr>
<tr>
<td>Moscow, Russia</td>
<td>167</td>
<td>$10</td>
</tr>
<tr>
<td>Romania</td>
<td>172</td>
<td>$50</td>
</tr>
<tr>
<td>Slovenia</td>
<td>137</td>
<td>$50</td>
</tr>
<tr>
<td>Slovak Republic</td>
<td>160</td>
<td>$65</td>
</tr>
<tr>
<td>South Africa</td>
<td>130</td>
<td>$35</td>
</tr>
<tr>
<td>Barcelona, Spain</td>
<td>171</td>
<td>$110</td>
</tr>
<tr>
<td>Madrid, Spain</td>
<td>183</td>
<td>$85</td>
</tr>
<tr>
<td>Valencia, Spain</td>
<td>182</td>
<td>$75</td>
</tr>
<tr>
<td>Sweden</td>
<td>88</td>
<td>$45</td>
</tr>
<tr>
<td>Switzerland</td>
<td>116</td>
<td>$45</td>
</tr>
<tr>
<td>Tanzania</td>
<td>174</td>
<td>$50</td>
</tr>
<tr>
<td>Kampala, Uganda</td>
<td>199</td>
<td>$0</td>
</tr>
<tr>
<td>London, UK</td>
<td>60</td>
<td>$25</td>
</tr>
<tr>
<td>Central UK</td>
<td>132</td>
<td>$55</td>
</tr>
<tr>
<td>Northern England, UK</td>
<td>111</td>
<td>$75</td>
</tr>
<tr>
<td>Scotland, UK</td>
<td>175</td>
<td>$60</td>
</tr>
</tbody>
</table>

**NORTH AMERICA**

<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calgary, AB</td>
<td>121</td>
<td>$25</td>
</tr>
<tr>
<td>Edmonton, AB</td>
<td>131</td>
<td>$25</td>
</tr>
<tr>
<td>Vancouver, BC</td>
<td>25</td>
<td>$20</td>
</tr>
<tr>
<td>Victoria, BC</td>
<td>100</td>
<td>$0</td>
</tr>
<tr>
<td>Winnipeg, MB</td>
<td>72</td>
<td>$20</td>
</tr>
<tr>
<td>Nova Scotia</td>
<td>105</td>
<td>$0</td>
</tr>
<tr>
<td>Ottawa Valley, ON</td>
<td>32</td>
<td>$10</td>
</tr>
<tr>
<td>Toronto, ON</td>
<td>21</td>
<td>$25</td>
</tr>
<tr>
<td>Montreal, PQ</td>
<td>36</td>
<td>$25</td>
</tr>
<tr>
<td>Quebec City, PQ</td>
<td>91</td>
<td>$45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Islands</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Bermuda</td>
<td>147</td>
<td>$0</td>
</tr>
<tr>
<td>Trinidad &amp; Tobago</td>
<td>106</td>
<td>$25</td>
</tr>
</tbody>
</table>

**Midwestern United States**

<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago, IL</td>
<td>02</td>
<td>$50</td>
</tr>
<tr>
<td>Illini (Springfield, IL)</td>
<td>77</td>
<td>$30</td>
</tr>
<tr>
<td>Central Indiana</td>
<td>56</td>
<td>$30</td>
</tr>
<tr>
<td>Michiana (South Bend, IN)</td>
<td>127</td>
<td>$0</td>
</tr>
<tr>
<td>Iowa (Des Moines)</td>
<td>110</td>
<td>$25</td>
</tr>
<tr>
<td>Kentuckiana (Louisville, KY)</td>
<td>37</td>
<td>$35</td>
</tr>
<tr>
<td>Detroit, MI</td>
<td>08</td>
<td>$40</td>
</tr>
<tr>
<td>Western Michigan</td>
<td>38</td>
<td>$25</td>
</tr>
<tr>
<td>Minnesota</td>
<td>07</td>
<td>$35</td>
</tr>
<tr>
<td>Omaha, NE</td>
<td>23</td>
<td>$30</td>
</tr>
<tr>
<td>Central Ohio (Columbus)</td>
<td>27</td>
<td>$25</td>
</tr>
<tr>
<td>Greater Cincinnati, OH</td>
<td>03</td>
<td>$30</td>
</tr>
<tr>
<td>Northeast Ohio (Cleveland)</td>
<td>26</td>
<td>$30</td>
</tr>
</tbody>
</table>

**Southeastern United States**

<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Carolina</td>
<td>10</td>
<td>$50</td>
</tr>
<tr>
<td>South Carolina</td>
<td>62</td>
<td>$60</td>
</tr>
<tr>
<td>Georgia</td>
<td>82</td>
<td>$60</td>
</tr>
<tr>
<td>Florida</td>
<td>10</td>
<td>$50</td>
</tr>
<tr>
<td>Central Florida (Orlando)</td>
<td>67</td>
<td>$35</td>
</tr>
<tr>
<td>South Florida</td>
<td>33</td>
<td>$40</td>
</tr>
<tr>
<td>West Florida (Tampa)</td>
<td>41</td>
<td>$35</td>
</tr>
<tr>
<td>Atlanta, GA</td>
<td>39</td>
<td>$40</td>
</tr>
<tr>
<td>Charlotte, NC</td>
<td>51</td>
<td>$35</td>
</tr>
<tr>
<td>Research Triangle</td>
<td>59</td>
<td>$25</td>
</tr>
<tr>
<td>Raleigh, NC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South Carolina Midlands</td>
<td>54</td>
<td>$30</td>
</tr>
<tr>
<td>Columbia, SC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memphis, TN</td>
<td>48</td>
<td>$45</td>
</tr>
<tr>
<td>Middle Tennessee</td>
<td>102</td>
<td>$45</td>
</tr>
<tr>
<td>Nashville, TN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virginia</td>
<td>22</td>
<td>$30</td>
</tr>
</tbody>
</table>

**Southwestern United States**

<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Kansas</td>
<td>20</td>
<td>$30</td>
</tr>
<tr>
<td>Kansas City, MO</td>
<td>87</td>
<td>$0</td>
</tr>
<tr>
<td>St. Louis, MO</td>
<td>11</td>
<td>$25</td>
</tr>
<tr>
<td>New Mexico (Albuquerque)</td>
<td>83</td>
<td>$25</td>
</tr>
<tr>
<td>Central Oklahoma (OK City)</td>
<td>49</td>
<td>$30</td>
</tr>
<tr>
<td>Tulsa, OK</td>
<td>34</td>
<td>$25</td>
</tr>
<tr>
<td>Austin, TX</td>
<td>20</td>
<td>$25</td>
</tr>
<tr>
<td>Greater Houston Area, TX</td>
<td>09</td>
<td>$30</td>
</tr>
<tr>
<td>North Texas (Dallas)</td>
<td>12</td>
<td>$30</td>
</tr>
<tr>
<td>San Antonio/South Texas</td>
<td>81</td>
<td>$25</td>
</tr>
</tbody>
</table>

**Western United States**

<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anchorage, AK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denver, CO</td>
<td>16</td>
<td>$40</td>
</tr>
<tr>
<td>Baton Rouge, LA</td>
<td>85</td>
<td>$25</td>
</tr>
<tr>
<td>Greater New Orleans, LA</td>
<td>61</td>
<td>$25</td>
</tr>
<tr>
<td>Greater Kansas City, MO</td>
<td>87</td>
<td>$0</td>
</tr>
<tr>
<td>St. Louis, MO</td>
<td>11</td>
<td>$25</td>
</tr>
<tr>
<td>New Mexico (Albuquerque)</td>
<td>83</td>
<td>$25</td>
</tr>
<tr>
<td>Central Oklahoma (OK City)</td>
<td>49</td>
<td>$30</td>
</tr>
<tr>
<td>Tulsa, OK</td>
<td>34</td>
<td>$25</td>
</tr>
<tr>
<td>Austin, TX</td>
<td>20</td>
<td>$25</td>
</tr>
<tr>
<td>Greater Houston Area, TX</td>
<td>09</td>
<td>$30</td>
</tr>
<tr>
<td>North Texas (Dallas)</td>
<td>12</td>
<td>$30</td>
</tr>
<tr>
<td>San Antonio/South Texas</td>
<td>81</td>
<td>$25</td>
</tr>
</tbody>
</table>

**To receive your copy of the Information Systems Control Journal, please complete the following subscriber information:**

- **Size of ENTIRE organization**
  - Fewer than 50 employees
  - 50 – 149 employees
  - 150 – 499 employees
  - 500 – 1,499 employees
  - 1,500 – 4,999 employees
  - 5,000 – 9,999 employees
  - 10,000 – 14,999 employees
  - 15,000 or more employees

- **Size of IS/IT audit staff (local office)**
  - 0 individuals
  - 1 individual
  - 2-5 individuals
  - 6-10 individuals
  - 11-25 individuals
  - More than 25 individuals

- **Size of information security staff (local office)**
  - 0 individuals
  - 1 individual
  - 2-5 individuals
  - 6-10 individuals
  - 11-25 individuals
  - More than 25 individuals

**Your level of purchasing authority**

- Recommend products/services
- Approve purchase
- Recommend and approve purchase

*Call chapter for information*
ALLIED SEARCH, INC.
Professional and Executive Search
Nationwide - All States
www.alliedsearchinc.com

Corporate Address
Allied Search, Inc.
2030 Union Street, # 206
San Francisco, CA 94123

Contact Information
Tel. 415-921-1971
Fax. 415-921-5309
donmay@alliedsearchinc.com

Mailing Address
Allied Search, Inc.
P.O.Box 472410
San Francisco, CA 94147

OPPORTUNITIES NATIONWIDE

POSITIONS: IT Audit Positions and other positions that require or prefer IT Audit experience.

LEVELS: All levels of responsibility; staff up to Vice President (VP).

CLIENTS: Large Companies In All Industries.

COMPENSATION: Very attractive salaries and bonuses.

BENEFITS: Excellent benefits.

LOCATIONS: U.S. cities nationwide; all fifty (50) states.

RELOCATIONS: Relocation assistance is available.

TRAVEL: Travel varies from company to company (0% to 100%). Some companies have international travel.

EXPERIENCE: Prior experience with a Big 4 Professional Services Firm is preferred, but not required.

COST: Free to applicant candidates; client companies pay our placement fee.

CONFIDENTIALITY: Confidentiality is assured.

APPLICATION: Send your resume on a "confidential" basis by one of the following:

Email: donmay@alliedsearchinc.com
Fax: 415-921-5309 Attn.: Don May
Mail: ALLIED SEARCH, INC.
P.O. Box 472410
San Francisco, CA 94147-2410
Attn: Donald C. May, Managing Director

PROCESS: After your resume is received, the Managing Director will call you on a "confidential" basis to discuss your background, your objectives and our search assignments that match your background and objectives.

INTERVIEW TIPS: Before your first interview, we will discuss with you "How to successfully take the interview and get an offer."

REFERRALS: Referrals are appreciated.

INQUIRIES: If you have any questions, call Don May at 415-921-1971 on a "confidential" basis. If not in, please leave your name, message and phone number, and your call will be returned as soon as possible, on a "confidential" basis.