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.

PAISLEY | Software for Governance, Risk & Compliance

PAISLEY ENTERPRISE GRC™ AND GRC ON DEMAND™ — Software for integrated audit, operational risk management, financial controls management, IT governance, and compliance. Call 888-268-0283 or visit www.paisley.com
Columns

5
Taking a Look Back: Data Security
Excerpted and reprinted from
The EDP Auditor Journal, Winter 1980

6
Guest Editorial: Business Reform and
Change Enabled by IT—An Alternative
Perspective
Tony Hayes, CGEIT, FCPA, FACS, FIIA (AUS),
CCHSE, CHE

9
IS Security Matters:
Reliable Security, Revisited
Steven Ross, CISA, CBIP, CISSP

12
IT Audit Basics: What Every IT Auditor
Should Know About IT Audits and Data
Tommie W. Singleton, Ph.D., CISA, CITP,
CMA, CPA

15
IT Governance: Driving Value From
Information Security: A Governance
Perspective
Vishnu Kanhere, Ph.D., CISA, CISM, AICWA,
CFE, CFA

22
Five Questions With…
Howard Nicholson, CISA, CGEIT

26
IT Value: Benefits Realisation and
Programme Management: Beyond the
Business Case
Sarah Harries, Peter Harrison, FCPA

29
Crossword Puzzle
Myles Mellor

Features

31
Justifying IT Projects: Connecting the
Dots From Systems to Business Value
Amitava Dutta, Ph.D., CISA

37
Driving Value From Nonrevenue-
generating Activities: Myths and
Misunderstandings of Governance and
Risk Management
Brian Barnier

45
Value of IT: Beyond the Theoretical
Tony UcedaVelez, CISA, CISM, GSEC

52
The Hidden Values of IT Risk Management
Timothy Abram, CISA, CGEIT, CISSP,
MCSE-Security, MCSA, Security+

Plus

25
Standards, Statements, Guidelines ISACA®
Member and Certification
Holder Compliance

57
Help Source Q&A
Gan Subramanian, CISA, CIA, CISSP, SSCP,
CCNA, CCSA, BS 7799 LA

59
CPE Quiz #123
Based on Volume 6, 2008
Prepared by A.Rafeq, FCA, CISA, CGEIT,
CIA, CCSA

S1-S8
ISACA Bookstore
Price List Supplement

Journal Online

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

Online Features
The following articles will be available
to ISACA members online on
1 April 2009.

Auditing Enterprise Resource
Planning Systems
Sean M. Price, CISA, CISSP

Information Technology Legislative Update
A. Abimbola, Ph.D.

Insider Computer Fraud—An In-depth
Framework for Detecting and Defending
Against Insider Attacks
By Kenneth C. Brancik
Reviewed by Vishnu Kanhere, Ph.D., CISA,
CISM, AICWA, CFE, CFA

A Study on Canadian IT Security Practices
Rafael Etges
Walid Hejazi
Alan Lefort
Unhappy with your current audit software? Still using a spreadsheet for audit analysis?

It’s time to take a closer look at IDEA

For over 20 years, IDEA – Data Analysis Software has set the standard for ease-of-use, performance and functionality. Now with the release of IDEA Version Eight, we have once again raised the bar with unique and innovative new features.

For more information about IDEA and to request a Free Demo, visit our website at www.caseware-idea.com.

Auditors in over 90 countries in 16 languages use IDEA to outperform peers and exceed the expectations of clients, employers and regulators.

IDEA is a registered trademark of CaseWare International Inc.
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 EPV as a core part of their infrastructure, enterprises can now:

- Manage, Personalize and Audit the full range of Privileged Users, including Administrative and Application Identities

- 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 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
Data Security
By Belden Menkus

There are really only two ways in which data (including program load module content) can be made secure. This is true whether the data in question are in storage or are being transmitted between various points. Data can be protected only against either unauthorized access to its content and/or modification/manipulation of those contents. The philosophical assumptions under which software is created and maintained—and the technological realities of the environment in which data are processed—do not provide, at present, any other means for assuring that data remain inherently secure.

REALITIES
Three things need to be recognized at this point:
1. The inherent security of data is not increased/improved by converting it into processible form. The logical constructs that give form to the data themselves are the only things that really make data secure. These logical constructs presume, it appears, that all who use particular data will play by the rules. There is, at present, no sure way of dealing systematically with the security threats created by those who won’t play by the rules. In particular, the attempts to provide data security in a logical context have been less than adequate when subjected to real-world scrutiny. …
2. There is an inherent conflict between the design of currently fashionable friendly software and the attainment of data security. Programs that provide uncurtailed capabilities for modifying and manipulating data essentially compromise...whatever protection can be provided for that data. At best, what results must be a compromise between the two; there is no such thing as a friendly program whose operations enhance the security of the data that it is used to process.
3. Maintenance-aiding hooks and other trapdoors left in a program may reduce the amount of productive time lost when a system fails but their existence (especially when it is not documented) can compromise fatally the security of the data being processed. In internally created programs, they can be disabled/removed during acceptance testing—prior to placing the package into production.

STRATEGIES
The data security enhancing options, unfortunately, are severely limited. There are only three things that can be done in any consistent manner to protect data integrity against some form of compromise:
1. Restrict access to particular data units or entities—and record on a current basis all those access attempts that are made. This is done, typically, by defining both the data entities to be protected and the levels or grades of protection to be provided. Potential program/data users are matched, in what amounts to an access protection matrix. Most data security software products are based in some measure on such a matrix. These products, as already suggested, are subject to various vulnerabilities. The most frequently overlooked is the access mediating role played, in effect, by the individual controlling privilege assignments within the matrix.
2. Obscure the data themselves. This is done through the use of some sort of encryption process. Such a process either changes the way in which the data meaning is represented or rearranges the internal structure of the data themselves. Successful use of a data encryption algorithm requires careful attention to key management. In addition, it appears that any algorithm of this type that could resist successfully reasonably anticipated cryptoanalysis attacks would be too unwieldy to be suitable for extended use. …
3. Verify selectively the internal consistency of the data themselves. There are a variety of value-driven, rather than structurally driven, reasonableness tests that can be applied—either randomly as an independent processing overhead function or when some predetermined event or condition occurs. …
Business Reform and Change Enabled by IT—An Alternative Perspective

Since the beginning of the electronic age, information technology, in its various forms, has enabled business to discharge significant benefits and reforms. During these years, we have seen the automation of processes through to complex analytical innovations that have positively affected organisations at the strategic, tactical and operational service delivery levels.

These changes and reforms have touched us all regardless of our background, culture, age or location on this planet. In fact, technology-enabled benefits and achievements have been so successful in changing our lives that when access or availability is not possible, we are reminded or at least given a glimpse of life before IT. Have you experienced the pleasures of flying out of town when the airport is running on partial or no air traffic control software, finding the automated teller machines are offline, shopping when point-of-sale systems at the supermarket are not working, trying to place a call when your mobile/cell phone network is down, or simply not being able to access the Internet?

We are totally reliant and dependent on these innovations every day of our lives. In fact, they have been so successful that we don’t even think of them as technology innovations, but rather as basic commodities of life.

However, even with this background of success, innovation and change in our lives, a significant number of failures and disasters occur each day—a statistic business strives to improve through the use of IT.

IT commentators regularly remind us that more than US $600 billion is wasted annually on ill-conceived or poorly executed IT projects. To add to this, it is often quoted that approximately 20 percent of projects fail outright, 46 percent are challenged and less than 35 percent are successful. If you are into balanced scorecards, this is not a balanced result for the industry and, more important, for organisations delivering services to their clients/customers. My observation is that government, the not-for-profit sector and the private sector all participate in these failures. In other words, they do not occur only in the private sector.

So, with this failure rate, the successful business initiatives that have been enabled by IT must be doing something special. Or were they just lucky? Is this more about an art rather than science?

If we place a stethoscope on the failed projects to determine what went wrong, what are the symptoms? What is the diagnosis? How could failure have been prevented? How can we ensure it does not happen again? What were the drivers that led to the situation or the outcome?

My observation is that in most cases there is a genuine and honest desire by the relevant players to achieve the right results and benefits for the organisation. Most always strive to streamline, automate and improve the business of the organisation through the use of IT and, wherever possible, enhance the customer/client experience with the organisation regardless of whether it is public, private or not-for-profit.

So what goes wrong when there is so much goodwill?

ISACA’s 40 years of experience in the IT industry confirms that the causal factors for project failures can be sourced back to any point in the project life cycle and can often simply come down to what people/organisations do not know. Valuable tools, methodologies, frameworks, guidelines and briefings highlight the notion that faults can be present in the initial planning stages; the business case development stage; and in any dimension, domain or process during the life cycle of the initiative. Put simply, these are complex undertakings, which require highly skilled and experienced people to diligently manage and lead at all stages from the beginning to end of the initiative. It is evident...
that managing and leading these changes requires broader and more comprehensive business experience and acumen than IT. But, so often we expect the IT folks to have all of the answers, skills and experience, while, in more cases than not, this is unfair, inappropriate and not particularly smart.

The business changes or reforms enabled by IT take the organisation and the staff to places they have never been before, and frequently no book, guideline or framework can provide the answers to all of the challenges presented. The following are a sample of the challenges faced in this environment:

- Underestimation of the organisational culture or multiple cultures in an organisation by the project team. A disconnect or lack of recognition of the importance of this can often cause a project to be rejected before it has commenced.
- Lack of ownership of the business reform/change by key stakeholders at various levels in the organisation. Capturing the hearts and minds of key informal and formal leaders is a critical success factor.
- Underestimation of the level and complexity associated with the change management affecting people, systems and processes
- Undervaluation of the achievements, rituals, practices and processes of the past and present. So many times the ‘baby can be thrown out with the bath water’. Project teams can often become isolated, disconnected and sometimes irrelevant in the medium to longer term if the organisation becomes disconnected, disinterested or disillusioned.
- Underestimation of the inextricable link that needs to exist between the strategy of the organisation (Where are we going?), the structure of the organisation (How will the human, physical and financial resources be organised to achieve the strategy?) and the culture of the organisation (What is important for the people to want to achieve the strategy with the structure provided?)
- Failure to listen to and act upon early warning signs for the project, particularly where the outcomes for the project may be at risk. The use of informal and formal channels of communication is needed to find out what is really happening or not happening.
- Failure to consult, collaborate, communicate and partner with the organisation to make the reforms/changes become real
- Failure to recognise that the project is a business reform/change and not an IT initiative. In other words, it could be said that there is no such thing as an IT project, but rather there are business projects that are enabled by IT.
- Underestimation of the need to clearly spell out roles, responsibilities and accountabilities for the business reform/change. The goal is to never have ‘he said, she said; it’s his, it’s hers; not mine, must be yours; not my problem, must be theirs’ conversation.
- Failure to introduce sound enterprise governance of IT. Yes, it is important to have an enterprise approach to govern IT, which is led and informed by the business, not IT.

This is not intended to be an exhaustive list, but rather a sample of many of the challenges that, if not well planned for and thought through, will see a business reform/change fail regardless of how good it is technically. The list goes some way to confirming a couple of sayings I often use to guide projects: ‘It doesn’t matter how perfect the technical solution is; if it is not owned and embraced by the business, it will not succeed’, or ‘Even if the solution is not technically perfect, if it is well implemented, the users will make it work’.

So, where to go from here? In my view, members and constituents of ISACA and the IT Governance Institute (ITGI) are in the best position globally to observe these failures of the past and present. Accordingly, they are also in the best position to influence and change the system into the future with the depth of experience, acumen and a common body of knowledge and through their frameworks and tools including Control Objectives for Information and related Technology (CobiT) and Val IT. However, the solution to the problem is still broader than this.

ISACA/ITGI members and constituents need to advocate not only at every opportunity and in every forum for the establishment of sound enterprise governance of IT, but also be confident raising many of the cultural, change management and collaborative approaches necessary to make the reforms/changes happen.

ISACA and ITGI have the frameworks and the broader body of knowledge around enterprise governance of IT. However, our immediate priority is to step up to the challenges listed here—they will make or break projects in the future. While we stop short of these cultural, change management and collaborative approaches, we will continue to see the US $600 billion per annum failure list grow. Are you equipped, ready and capable to address these challenges?
Don’t hit the brakes. Renew your ISACA® membership and continue to accelerate your career.

As an IT audit, security or governance professional, increase your professional mileage and master the road ahead.

ISACA fuels your career through:

- **Professional development**: Get a professional edge, broaden your perspective, fine-tune your skills and earn CPE credits.

- **Research and knowledge**: Stay up to date with the latest thought leadership, best practices and professional resources.

- **Community and leadership**: Connect with a global community of more than 86,000 constituents.

ISACA membership will continue to help drive your career to the next level.

Renew your ISACA membership today!

www.isaca.org/renew
I often receive e-mails from readers of volume 5, 2008, of the Journal. Some are in the “Are you nuts? …” category, and a few are even complimentary. When the piece, called “Reliable Security,” was published in this space, I received quite a few lengthy and interesting replies. They were not rebuttals, exactly. I would prefer to say that these readers were keeping the conversation going among professional colleagues. And, no one called me nuts. I would like to use this column to open the conversation further and invite others to join.

INSECURE TECHNOLOGIES
I made the comment: “There are no threats to information technology for which we do not have the tools to combat,” adding in a footnote that I knew I was sticking my neck out and challenging readers to suggest otherwise. Andrew Commons wrote from Australia:

This is only true if information technology is static. Unfortunately, all sorts of new ‘cool’ technology keep appearing where the attack surface is largely unknown. Technology that adequately protected us yesterday is inadequate today, because the goalposts have shifted. This will always be the case.

Sean Price, writing from Northern Virginia in the US, makes a similar point:

New technology frequently brings with it new security challenges. We don’t always have tools immediately available to address weaknesses introduced by the latest toys. Consider P2P [peer-to-peer] tools. A user loads a new toy that allows some level of file (or information) sharing. Others abuse the intended purpose of the same tool and take advantage of the unsuspecting user. Security folk reach and stretch to put yet another finger in the dike. Vendors scramble to reposition their wares as the silver bullet to the latest threat. Gaps exist for quite some time before a real tool emerges to counter the problem.

Both Commons and Price see the problem as based on weaknesses in the technology and, interestingly, both identify the criterion of “coolness” as a motivating factor for using new and insecure technologies. They see a time gap between the introduction of technical innovations and the security tools meant to control them. It has been ever thus. However, data are still stored and transmitted in 1s and 0s, and access is still granted and denied based on unique identifiers. If only there were a system that could keep the data from the prying eyes of unauthorized individuals and make the data available to those who are entitled to read them, the problem would be solved.

Oh, wait. There is such a system, public key encryption, supported by a global method of distributing unique identifiers to enable access to information, i.e., a universal public key infrastructure (PKI). The point of the original article was that we know what to do, but we do not do it, at least not on a scale that eliminates the problem.

HUMAN FRAILTY
Indeed, Olalekan Oladunni, from Nigeria, points out that “humans are prone to error consciously or otherwise, therefore, it would be appropriate to plan, monitor and control information assets requirements and operations.” I completely agree and would like to expand on that point a bit. All
engineered systems are subject to defects. This is because systems—in this case, information systems—are crafted by human beings who, while perfectible, are not perfect. The time, cost and effort required to eliminate all defects are too great to assume that systems will always work as intended over an extended period of time.

As information systems professionals, we should anticipate error and accommodate correction in the design and operation of the systems with which we work. The scale of these corrections differs according to the circumstances. We deal with frequent and routine errors by implementing controls, precisely because we anticipate that mistakes will occur. “Security” is the term we apply to countermeasures against infrequent but devastating flaws. (Information security does not apply only to prevention of malicious attacks. The overzealous and the lazy can outdo the dishonest every time.) Catastrophic failures—man-made or otherwise—require contingency plans. Failure to recognize that people, given enough time, will cause control, security or contingency problems is the root cause of the problems themselves.

To return to the reliability of security, information security professionals are no less prone to error than other mortals. Price adds:

There are a multitude of security professionals who just do not fully comprehend how to conduct security analysis of a system or product. It is not enough to rely on tools to find the weaknesses. … Insufficient documentation is an indication of inadequate security analysis of countermeasure support of a security policy. Again, the problem points to people.

I am more sanguine than he about the “multitude” of inadequate security professionals. My point is that all security specialists, the competent and incompetent together, make mistakes some of the time, albeit the incompetent make them more regularly.

RISK MANAGEMENT
Melody Morgan-Busher from Malta brought a rather interesting analogy to the discussion. I claim no competence in particle physics, but am aware of Werner Heisenberg’s contribution to our understanding of the universe. Morgan-Busher explains Heisenberg’s Uncertainty Principle2 as saying that:

One cannot measure all characteristics of a subatomic particle (i.e., difficult-to-isolate entity) simultaneously. The logic says that one can either know the mass, the speed or the location, but one cannot know all these at a given instant. … I feel that the same may be true for risk. One can be sure of its impact or its probability, but not both at the same time with accuracy—trying to define the nature of a risk more exactly may necessarily lower the awareness of its impact, for example. This concept arises because the thing being measured is highly dynamic, and trying to pin down one dimension necessarily means abandoning other details.

It is refreshing (or, perhaps, mystifying?) to know that there is a scientific principle underlying one of the points that I made in the previous column. I believe that the magnitude of a risk becomes apparent only after a negative event occurs. Analysis and evaluation of risks provide an approximation of the relative scale of those that are apparent. I do not often quote former US Secretary of Defense Donald Rumsfeld, but he was right to say, “There are things we don’t know we don’t know.” Beyond the inevitability of error discussed above, we need to add the assurance of ignorance—or at least uncertainty.

TIME LAG
I noted in the original article that time lag is a cause of unreliability:

[A]t any given time, there are some data, infrastructure or applications that are better protected than others, not because the technology is not available but because the people in charge just have not gotten to them yet.”

Commons seems to agree. He wrote:

[P]rogress always outruns our understanding of the attack surface. This has always been the case. The best approaches to this problem are generic ‘white-list’ solutions. This requires an understanding of
the fundamental attack vectors associated with the technology involved, something that is not always known. This will still be problematic. When we shift something we are familiar with from a ‘green screen’ interface to a cell phone or we introduce something like WiFi into the picture, even the ‘pros’ have a time lag...and the smart bad guys are often smarter than the pros!”

In my opinion, there is a greater problem than unfamiliar risks in new technologies. Almost by definition, the introduction of any technology into a business process creates novel risks. It is not so much that there are unknown attack vectors as much as that the technology itself changes the process. It may fail to prevent sins of omission or commission in the controls over business risks. Thus, for example, the introduction of a new trading system with unfamiliar controls might allow a rogue trader to place unauthorized, devastating transactions. Perhaps this is the price for what Commons skeptically terms “progress”; it may also be another aspect of time lag. Information technology has the effect of speeding misuse without necessarily accelerating security at the same pace.

Finally, I would like to note one of the salient virtues of this Journal. The conversation among fellow security and control professionals that I have related in this column has occurred among folks from Australia, Nigeria, Malta and the US States of New York and Virginia. Of course, a journal like this one does not have the immediacy of a blog, but it is a wonderful place for the exchange of views from around the world.

ENDNOTES
2 For those so interested, the actual Heisenberg Uncertainty Principle is: $\Delta X \Delta P \geq h/2$. Apart from the explanation offered by Melody Morgan-Busher, I have no idea what this means.
One common problem with data is that management is not able to completely identify all of the entity’s data. The larger the organization and the more autonomous business units are within an organization, the more likely it is that the organization has developed data in inconspicuous repositories and, perhaps, failed to comply with policies and procedures about data, assuming adequate ones have been developed.

Structured data, such as those produced by core applications, are readily identifiable. It is the unstructured data that are at risk of being developed and lost in the morass of systems and data, or the hectic pace of business. For example, an employee develops a spreadsheet to make some business process easier to perform and the data in the spreadsheet must meet some threshold established by management regarding criticality or risk associated with financial reporting, compliance, or organizational policies and procedures. Management may not be aware that the business process is being handled in that fashion or that critical data are now housed in a spreadsheet. If management is unaware of this situation, how can it properly control that data? If the IT auditor is unaware of this situation, how can he/she properly conduct the audit? A major issue with unstructured data is that they are growing in volume and type.

Obviously, the limitation here is one of relevance. Neither management nor the IT auditor would want to involve all of the data in the entity in performing their duties. So data would be assessed based on some threshold level of relevance, such as risk, ultimate use or importance. However, there should be some policies and procedures in place to make sure all data have been filtered through this data control model, to ensure that no relevant data have been missed.

The IT auditor should make sure to include in the audit some means of gaining assurance that all relevant data (relevant to the audit...
objectives) have been found by management. That assurance can be attained by interviews with management, review of data policies and procedures, and tracing data back from the end object (e.g., transaction or account balance) to its source. Another helpful technique is to make inquiries of key personnel on the “front line” of relevant business processes.

COLLECT ALL OF THE DATA
Management should have not only identified all relevant data, but collected them by placing them into a system. It may be best for some business process data to be housed in a spreadsheet, but those data should be tied to some kind of system so they can be managed and controlled effectively.

The IT auditors should be cognizant of this fact when they find data in one of the unstructured areas. That is, when IT auditors encounter unstructured data, they should ascertain whether the data have been properly collected—systemized. If the IT auditor determines that the unstructured data are stand-alone, then that will obviously be a concern.

CLASSIFY ALL OF THE DATA
This step is the one in which relevance would be assessed by management. Once data have been identified and collected, management will want to classify the data according to some appropriate model. For management, that classification process would, at a minimum, identify all data that require controls, most likely based on an appropriate risk assessment. Management should have developed policies and procedures associated with this classification, including issues such as risk assessment, systems of collection and controls.

Classification is important in enabling IT auditors to perform audit procedures efficiently and effectively. IT auditors may not be able to test controls or gather appropriate evidence if they have not been given the complete list of relevant data. For example, if the IT auditor by chance finds a spreadsheet being used to calculate the bids of large projects housed by one or two employees on a laptop that has not been classified by management as above the established threshold (e.g., some minimal risk, importance), then the IT auditor would have concerns that the classify step is not working properly. If it is not working effectively, what other relevant (risky) data exist, but have not been classified? How does that situation affect assurance and the IT audit?

CONTROL ALL OF THE DATA
This step is the one with which IT auditors, and auditors in general, are most familiar. Generally speaking, the integrity of data relevant to the IT audit is directly related to the sufficiency of the controls under which the data are gathered, processed, stored and reported.

One of the primary functions of IT auditors today is to evaluate controls. A problem arises if an unknown relevant data source exists and has not been placed under a formal set of controls. Such a situation could exist and go without detection by the IT auditor. Management cannot effectively control data that have not been properly found, collected and classified. Therefore, the IT auditor should have steps or procedures, formal or informal, in place to gain adequate assurance that no data of relevance exist outside a proper system of internal controls.

CONCLUSION
A key component of a typical IT audit is relevant data. The IT auditor should be aware of the steps necessary to make sure controls have been placed around all relevant data. The data life cycle for management should include find, collect, classify and control data, and should be applied to all of the organization’s data.

There is a risk that management has not been able to completely or effectively find, collect, classify and control relevant data. That circumstance creates at least two problems for the IT auditor: the possibility of missing a key source of data in the audit, and the insufficiency of management to control its sensitive data. Thus, the IT auditor should be aware of the significance of stand-alone data when they are discovered.

ENDNOTE
Of course your employees wouldn’t abuse their access to sensitive data.

Unless you left the door open. Find out with Symark’s free 30 day trial.

80% of computer crime is an inside job. With Symark’s Access Control and Identity Management products, you’ll be able to identify and strengthen your security’s weak points, manage access, and allocate privileges. You can track who’s doing what, where and when. And Symark’s security products are easy to deploy and provide rapid ROI. Our commitment to quality products and superior technical support has made us the leading vendor of security administration solutions in heterogeneous UNIX and Linux environments worldwide. For more information, visit our web site at www.Symark.com/30daytrial. And outfox those who would put your company at risk.

Symark’s free 30 day trial:

powerBroker®
UNIX/Linux Access Control & Accountability

www.symark.com
US & Canada: (800) 234-9072
Europe: +44 (0)8704 586 224
International: +1-818-575-4000
Driving Value From Information Security: A Governance Perspective

With the increasing dependence of the corporate world and governments on information systems and technology, the need, importance and relevance of information security governance is well acknowledged and accepted by top management. The questions that still plague organizations at all levels are not whether, why or what to secure; the business policies and risk management framework provide the answers to these questions. Questions of when, how, to what extent and at what cost to secure business and its information systems remain.

Communicating to and convincing the board about nebulous and technical concepts and matters such as information systems and IT security have always been a challenge. The board of directors always prefers bullet points, an executive summary backed by evidence, ideally with supporting financials to help them make quick, effective and correct decisions. These decisions are ultimately made at the board level as part of the governance function.

In the present scenario, those in charge of governance generally expect proposals backed by return on investments (ROI), return on capital employed (ROCE), return on security investment (ROSI), cost-benefit analyses and balanced scorecard (BSC) workings. This article focuses on ways of putting forward a business case for information security and describes the best approach to achieve it.

INFORMATION SECURITY GOVERNANCE

Corporate governance has many dimensions: transparency, accountability, stakeholders’ interests, ethics and fair play, to name a few. It also has many subsets: governance cutting across functional areas of management, marketing, operations, logistics, finance and accounting, supply chain management, and human resource management. Information technology, a fascinating addition to the asset portfolio of a business, is also a part of the subsets to be governed. Hence, IT governance in business is an important feature. However, given the prowess of IT, protecting information system assets (i.e., hardware, software, data) and securing the intangible and tangible assets at all times are predominant desiderata of a corporate information security governance policy. Thus, a new dimension to corporate investment decision making is information security investments.

In time, IS security investment may become a mandatory proposition, not merely to protect businesses against assaults, but to protect the sovereignty and territorial integrity of a country or the world.

Admittedly, in the post 11 September 2001 scenario in the US, reinforced again by repeated terrorist attacks elsewhere, a properly implemented information security management system (ISMS) can make a vital difference to the very existence of any business. With stringent legislation in place requiring companies to secure and protect data and information assets, and the introduction of legislation such as Law 1386 in California (USA) and elsewhere, expenditure on information security is no longer a luxury or an exercise in futility, but has become a pressing need even for the small and medium-sized business.

ISSUES CONCERNING ISMS

The important questions posed before contemporary management are:

- What is the IS security investment and what are its components?
- What are the expected payoffs from the investments—proactive and reactive?
- What are the measures of performance that can be used—ROI, ROCE, ROSI and cost-benefit analysis?

Each of these issues will be discussed in turn.

What Is the IS Security Investment and What Are Its Components?

IS security investment includes, *inter alia*, inputs required to protect the IT prowess of...
business from abuse by delinquents—insiders and outsiders. Thus, security arrangements include investments in people, processes to mind and manage the IT portfolio, data, information, other processes, products, people, other assets and reputation. Security arrangements require outlays on revenue and capital accounts to preempt assaults of any type on the IT prowess of business. Such a watch on IT prowess has to be a 24/7 proposition.

IT security investments must touch all echelons of IT prowess, including the smallest possible corner or cavity of the IS configuration of business.

What Are the Expected Payoffs From the Investments—Proactive and Reactive?
The payoff from any investment is usually evaluated in terms of typical profitability; time-adjusted measures of performance, including ROI; net present value (NPV); internal rate of return (IRR); and other related tools and techniques. In typical security-motivated investments, the expected payoffs are certainly not in revenues or even reduction in costs. However, the least-cost option, in terms of time, money and effort required to put a security system in place, is one technique that can be effectively used. Yet another way of looking at the evaluation of security investment is “fear” on the part of the delinquent—“big brother is watching and we may be caught.” The deterrence generated by the security solution vs. the greed that exists, either of bonanza, monetary gains or satisfaction that the destruction is done, does not matter. The greatest reward or payoff is the likelihood that more and more people will refrain from tampering with IT investments and information systems. The concomitant discipline, single-minded attention to work on the part of internal potential delinquents and the smooth conduct of operations that are compliant with the laws of the land are all potential gains, not fully quantifiable, yet very relevant. Thus, while the denominator of the ROI (investments) can be quantified, the numerator is not bereft of gains that can be effectively articulated, felt and experienced, but not necessarily quantified. However, the historic data relating to losses arising out of delinquencies can be a useful base that is amenable to measurement. If the current losses due to assaults on IT are reduced, the year-on-year reduction in IT losses is a quantifiable piece of information. The fact that IT assets and prowess thereof are protected, and that there are no, or minimal, assaults on IT assets and no loss of life, due to terror-driven infiltration, would bear testimony to the viability and raison d’etre of the security investments.

What are the Measures of Performance That Can Be Used—ROI, ROCE, ROSI and Cost-benefit Analysis?
Decision makers ask themselves: “Which of these options gives me the most value for my money?” That’s the fundamental question that ROI is designed to answer. ROI is frequently used to compare alternative investment strategies. For example, a company might use ROI as a factor when deciding whether to invest in developing a new technology or extending the capabilities of their existing technology.

\[
ROI = \frac{\text{Expected Returns} - \text{Cost of Investments}}{\text{Cost of Investments}}
\]

To calculate ROI, the cost of a purchase is weighed against the expected returns over the life of the item. For example, if a new security project will cost US $1 million and is expected to reduce damages valued at US $5 million over the course of three years, the ROI for the three-year period is 400 percent (the net damages avoided being four times the initial investment).

A simple equation for calculating ROSI is as follows:

\[
\text{ROSI} = \frac{(\text{Risk Exposure} \times \% \text{ Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}
\]

Thus, repeatable and consistent metrics can be extremely valuable—even if they are “inaccurate.”

A simple analytical method of calculating risk exposure is to multiply the projected cost of a security incident (single loss exposure [SLE]) with its estimated annual rate of occurrence (ARO). The resulting figure is called the annual loss exposure (ALE). While there are no standard methods for estimating SLE or ARO, there are actuarial tables that give average statistical values based on actual damage reports. These tables are created from insurance claim data, academic research or independent surveys.

\[
\text{Risk Exposure} = \text{ALE} = \text{SLE} \times \text{ARO}
\]
With a good survey and scoring system for productivity, combined with external measurement of intellectual property value, it becomes possible to quantify risk exposure in a repeatable and consistent manner. Unfortunately, there are a number of serious problems with this “logic”:

• Risks cannot be captured in silos—A properly secured and locked door may fail to mitigate risks if the window next to it is open.
• Security solutions are not stand-alone—The existence and effectiveness of a framework of policies, practices, procedures and other solutions are necessary for security to be viable.
• Security solutions are rarely implemented to be as effective as possible due to an unacceptable impact on productivity.
• Security solutions become less effective over time, as hackers find ways to work around them and create new risks.

A CASE STUDY
Security programs strive to control and minimize loss by preventing undesirable things from happening or mitigating the impact and its effects when they do occur. Consequently, determining the efficacy of a security program and quantifying ROSI is difficult because it requires measuring something that has been prevented: losses that were avoided. Measuring something that has been avoided is extremely challenging and may be impossible in many situations.

A leading computer chip/computer manufacturer developed a model for measuring ROSI in its manufacturing environments that produced a much higher level of accuracy than other methods currently being used. The model has enabled it to make business-driven decisions about security programs, resulting in savings in excess of US $18 million per year in avoided losses. By analyzing historical cyberattack incidents, performing trend analysis of data from similar environments and then extrapolating, the model is able to predict interim trends in security incident occurrence to derive the financial impact of technology adoption for security programs.

This ROSI methodology is scalable, manageable and can be automated, providing managers with an effective tool for calculating value, making decisions, justifying outlays on information security, allocating resources and implementing an optimal level of security. The data set included incident data, such as virus and worm events, tracked for two years, and information from approximately 18,000 computers over the course of 750 days (equivalent to 13 million computer days).

Because the predictions are based on actual incident data rather than an assessment of potential exposure and vulnerabilities, the ROSI approach used by the manufacturer provides a high level of accuracy. This also enables management to compare the value of security programs with nonsecurity initiatives so that the organization is better able to manage and allocate resources, justify security expenditures, predict the value of future security programs, and determine if it is meeting expectations once implemented. This, in the long term, helps to provide the critical data necessary for developing a strategic plan for securing the computing environment.

CONCLUSION
The primary take-home is a structured methodology to budget for IT security based on the previously mentioned approach. Certain key issues to be considered are:

1. Business cases differing from the view of law enforcement and regulatory and government agencies, e.g., settlements of credit card fraud cases
2. Security as a trade-off among cost, convenience and computing performance in terms of flexibility, speed and performance
3. Retrofitting security vs. designing a new system for information security
4. Balancing limited funds, unlimited choices and too many viewpoints
5. Protecting the right things. Think like the hacker, keep the bad guys out, but let the good guys in (in all of these, “good” and “bad,” “right” and “wrong,” are relative terms).
6. Regulatory compliance. One size does not fit all. A bank, a military installation, a manufacturing company, an ISP, a web site, a small business—will all of them react in the same way?
7. Cost of gold plating, bells and whistles in IT security
8. The appropriate level of security, depending on who, where, why, what and how information is protected
9. Experience—perhaps the most expensive, but the most effective teacher. Insecure computers cost time, money and, in some cases, reputation and goodwill, which are much more difficult to replace when lost.

Measuring something that has been avoided is extremely challenging.
Determining the ROSI of information security projects helps in crystallizing the intangible benefits and nonquantifiable considerations. This enables management to weigh all the factors in the right perspective and to arrive at informed decisions, rather than relying on instinct alone. However, given the problems associated with information security in terms of its implementation and effectiveness, especially the dilemma of security vs. openness, conventional ROI/ROSI alone is not an appropriate tool for deciding whether to proceed with information security projects. Rather, this decision should be made on a business-case basis. ROSI would be more appropriate for making a choice between different alternatives of security investment. Hence, ROSI should be tempered with an assessment of the competitive advantage of information security proposals. A balanced scorecard approach coupled with ROSI would be a better alternative (see figure 1).

Costs/benefits of IT security projects largely depend on the human factor, cost and revenue drivers, business objectives, security metrics, and organizational characteristics, which can substantially influence end results. Refining ROSI estimates through learning experience and by comparing estimated and realized ROSI will improve this tool with each successive project, resulting in better calibration and more accurate estimates. Thus, ROSI, with a balanced scorecard focus, will become a tool of choice for the future, in the hands of decision makers.

Figure 1—The Balanced Scorecard Framework Using ROSI

<table>
<thead>
<tr>
<th>Financial</th>
<th>Internal Process</th>
<th>External Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives</td>
<td>Objectives</td>
<td>Objectives</td>
</tr>
<tr>
<td>Measures</td>
<td>Measures</td>
<td>Measures</td>
</tr>
<tr>
<td>Targets</td>
<td>Targets</td>
<td>Targets</td>
</tr>
<tr>
<td>Initiatives</td>
<td>Initiatives</td>
<td>Initiatives</td>
</tr>
</tbody>
</table>

REFERENCEs

EE Times of India, “APAC SMBs Up IT Security Investment by 26%,” www.eetindia.co.in
Surmacz, Jon; “An Ounce of Prevention—Why ROI Is the Wrong Question to Ask About Security,” CSO Online, 8 May 2002
“Finally, a Real Return on Security Spending,” CIO Magazine, 15 February 2002
Kanhere V. S. Kanhere; A. Agarwal; “Budgeting for Information Security an ROI Approach,” InfoSec, 2004
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
Whatever the challenges you face

Modulo Risk Manager helps you manage your IT Governance, Risk and Compliance needs!

Modulo Risk Manager™ provides an integrated solution for:

- Compliance with SOx, PCI DSS, FFIEC, ISO 27001, ISO 27002, CobiT, BS 25999, HIPAA, FISMA, NIST 800-53a, A130, ITIL, ISO 20000, DOD 8500.2, Basel II and more
- Automating risk management and remediation progress measurement
- Consistent, comprehensive, centralized analysis and reporting of risk policies and controls
- Eliminating costly information redundancy and audit silos
- Incident tracking, remediation and Business Continuity Management

Contact us for a presentation
Toll Free: +1 866 663-5802

www.modulo.com
+1 973 744-1617
Top 10 Reasons to Attend ISACA® Conferences

www.isaca.org/conferences

10. **Advance your career and earn CPE hours**
    ISACA conferences present the most up-to-date information to help attendees keep up with trends in their professional field and receive continuing professional education (CPE) credits that fulfill designation requirements.

9. **Interact with leading vendors**
    Vendors have the necessary background to provide industry insight and answer your questions about their technologies and solutions.

8. **Increase your value in your organization**
    Because you will learn from world-class presenters who understand your role, the information presented is current and relevant.

7. **Demonstrate your value to your employer**
    Send a strong message to your employer that you are serious about enhancing your career by gaining knowledge that you can put into action immediately.

6. **Superior content**
    ISACA resources allow for better quality sessions and ensure that content is the most up-to-date and relevant to the issues currently facing the IT industry.

5. **Enjoy a customized learning experience**
    Explore and discuss the topics most important to you—choose to attend sessions from any of the conference tracks/streams.

4. **Global appeal**
    Conferences draw attendees from the international base of members and certified professionals, and at every ISACA conference over 20 countries are represented.

3. **Learn from industry experts who have been in your role**
    Conference speakers and presenters bring their own experiences and share their knowledge to mentor, inspire and provide guidance.

2. **Expand your professional network**
    ISACA conferences serve as an assembly of individuals who are passionate about IT and wish to network with their peers.

1. **Be a part of IT**
    Don’t just sit back and let the IT world evolve around you, be a part of an international organization dedicated to you and your career, and contribute to the growth and advancement of the IT profession.
As business analyst at the City of Salisbury, South Australia, Howard Nicholson is responsible for the implementation of the city’s governance framework, including both internal audit and risk management. Prior to joining the City of Salisbury, Nicholson was an audit manager with Centrelink, one of the largest federal government departments in Australia. As part of a 16-year audit career, he was responsible for undertaking and managing compliance audits, information systems audit, and operational and performance audits.

A member of ISACA for 20 years, he was president of the Adelaide (Australia) Chapter for four years, chair of the ISACA Membership Board for three years, and elected to the ISACA International Board of Directors and the IT Governance Institute (ITGI) Board of Trustees in 2004, on which he continues to serve. He also chairs ISACA’s ISO Liaison Task Force and the CGEIT Certification Board. Nicholson is an associate fellow of the Risk Management Institute of Australasia.

Outside of work and his ISACA commitments, Nicholson enjoys swimming, cycling and most genres of music. He also enjoys reading and is a keen collector and drinker of wine.

Q Could you please explain what ISACA is doing for and with the International Organization for Standardization (ISO)?

A As part of its commitment to providing leading-edge research, support and guidance to members, organizations and the IT business industry in the areas of IT governance, security and assurance, ISACA has applied for, and been granted, Category C Liaison Status with specific ISO groups. Closer ties between ISACA and ISO will foster a better understanding of the work being undertaken to develop standards and guidance in these areas.

Under this formal relationship, ISACA is able to participate in the development of standards and guidelines currently being undertaken by ISO’s Joint Technical Committee 1 (JTC1) Sub-Committee 7 (SC7) and Sub-Committee 27 (SC27). Specifically, ISACA is focusing on the work being undertaken by Work Group 1A (WG1A) within SC7, and Work Group 1 (WG1) within SC27. These groups are responsible for the maintenance of the 38500 standard on the governance of IT and the development of associated standards and guidelines and for the 27000 series of standards, respectively.

ISACA members have a wealth of knowledge in relation to IT governance, IT assurance and IT security. By channeling this knowledge and experience through ISACA’s ISO Liaison Task Force and working with ISO, all parties will benefit. ISACA and ITGI have already made significant contributions through the exchange of knowledge and experience and by making components of their intellectual property (IP) available.

Q What does ISACA see as the advantages to this relationship?

A The relationship will provide access to ISO, a well-respected global body, and, through this, ISACA and ITGI will be able to raise their profile across business and industry. It will also enable ISACA and ITGI to be part of the development and establishment of standards and guidance that are in accord with their thinking and IP. This is critical to ensure that ISACA members, businesses and industry benefit from the provision of guidance that meets their needs.

It will also provide greater exposure for Control Objectives for Information and related Technology (CoBIT) and Val IT, and for the various briefings and research products released by ISACA and ITGI. Showing that such products assist enterprises in aligning with ISO standards not only raises ISACA’s and ITGI’s profiles as thought leaders, but also ensures a greater take-up of their IP.
How is ISACA responding to or working on the ISO IT governance standard?

Currently, ISACA is a key player in the deliberations of WG1A in JTC1 SC7. This group is charged with the maintenance and ongoing development of the recently released standard 38500 on the governance of IT. It is also responsible for the development of guidance to support this standard, including the development of subsequent and related standards. A subgroup of ISACA’s ISO Liaison Task Force is working closely with other delegates on WG1A to ensure the best outcomes for ISO and ISACA/ITGI.

ISACA has also established a global network of subject matter experts who will provide assessment of, and input to, the various draft documents circulated by WG1A, through our WG1A subdelegation. This will ensure that the development process is supported by the best analysis and advice that ISACA and its members can provide.

What other opportunities exist for ISACA/ITGI within ISO?

There are a vast number of activities being undertaken by ISO in the area of standards development, and many of these may relate to current research and development efforts of ISACA/ITGI. However, without careful management, our involvement could become a never-ending call on resources. ISACA/ITGI will review the opportunities and risks presented by the relationship on a regular basis to ensure that the opportunities are maximized.

Like any business venture, we have to be careful that the value we generate from the relationship outweighs the costs. While there may be many areas where ISACA members believe ISACA/ITGI should be involved, we have to ensure that we target our resources at the areas that will provide the greatest level of payback for the association and its membership.

If the current engagement continues to bear fruit, resources are available, and we are able to demonstrate that, through this involvement, we are benefiting our members as well as ISO and the industry in general, we may seek other areas of interest.

Does the relationship with ISO benefit the individual members within ISACA?

As discussed previously, involvement with ISO will raise the profile of ISACA and ITGI, so all members will benefit from this increase in recognition of the association and institute. Further, it should ensure a closer alignment of relevant ISO standards and guidance with ISACA/ITGI IP and products. This will put ISACA members at an advantage in providing services to meet ISO requirements, through their familiarity with ISACA products, particularly the certification programs.

This relationship also provides those ISACA members who have extensive skills and experience in the areas of cooperation to be involved in the process of creating new guidance. This is a great opportunity for continuing professional development and for members to give something back to the association and the profession.
A New Formula For A Basic Concept

Yes, we said CR²G not GRC. NEMEA thinks it’s only logical to start at the beginning and follow the natural process toward good governance. And, we’ve added a new element; the R² for Risk and Remediation. We think it’s only logical to figure out what’s broken, fix what needs attention, determine the residual risk and then decide how to govern in the future.

Our fully automated, on-demand software products are designed to help you set up a rigorous and logical CR’G program that you can manage without tapping into your valuable IT resources. Now you can stay on top of evolving regulations and standards across all departments, and make better business decisions for a minimal subscription price. And, all you’ll need to manage compliance, assess risk, and monitor your progress is a web browser. We don’t offer you canned software solutions. Our software tools help you engineer and conduct a logical CR’G program of your own. COBIT 4.1, ISO/IEC 27001 & 27002, ITIL, SOX, PCI-DSS, plus 20 additional, industry specific standards and regulations are included for your use.

- **Determine Compliance Posture**
- **Define, Validate & Assess Key Risks**
- **Manage & Track Remediation Efforts**
- **Compress Internal Audit Time**
- **Reduce Duplication & Redundancies**
- **Benchmark & Create Timely Reports**
- **Improve Business Performance**
The specialised nature of IS auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are cornerstones of ISACA’s professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

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

- **Guidelines** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

**Control Objectives for Information and related Technology (ConT®)** is an IT governance framework and supporting tool set that allow managers to bridge the gaps amongst control requirements, technical issues and business risks. ConT® enables clear policy development and good practice for IT control throughout commonly understood and well-respected framework. ConT® therefore, its usage enables the understanding of business objectives and the C

**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 2008**
- **G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008**
- **G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008**
- **G5 Audit Charter Effective 1 February 2008**
- **G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008**
- **G7 Due Professional Care Effective 1 March 2008**
- **G8 Audit Documentation Effective 1 March 2008**
- **G9 Audit Considerations for Irregularities and Illegal Acts Effective 1 September 2008**
- **G10 Audit Sampling Effective 1 August 2008**
- **G11 Effect of Pervasive IS Controls Effective 1 August 2008**
- **G12 Organisational Relationship and Independence Effective 1 August 2008**
- **G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008**
- **G14 Application Systems Reviews Effective 1 October 2008**
- **G15 Planning Revised Effective 1 March 2002**
- **G16 Effect of Third Parties on an Organisation’s IT Controls Effective 1 March 2009**
- **G17 Effect of Non-audit Role on the IS Auditor’s Independence Effective 1 July 2002**

**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 2003**
- **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**

- .010 Responsibility, Authority and Accountability
- .020 Independence
- .030 Professional Independence
- .040 Organisational Relationship
- .050 Professional Ethics and Standards
- .060 Due Professional Care
- .070 Competence
- .080 Skills and Knowledge
- .090 Continuing Professional Education
- .100 Planning
- .110 Control Planning
- .120 Performance of Work
- .130 Supervision
- .140 Evidence
- .150 Effectiveness
- .160 Periodic Reporting
- .170 Follow-up Activities
- .180 Follow-up

**Code of Professional Ethics Revised May 2003**
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 head of value management 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 ISACA’s Val IT Steering Committee.

This is the fifth of six articles to be published in this column on the practicalities of introducing and establishing Val IT. These articles draw from the authors’ many years of experience working with enterprises to introduce and embed value management. The previous four articles (found in volumes 3, 4 and 6 of 2008 and volume 1 of 2009) described how to recognise the need for Val IT, the five basic steps for introducing Val IT, how to establish the Val IT value governance process and the challenges of implementing portfolio management. The final article of the series, scheduled to appear in volume 3, 2009, will cover the critical success factors for introducing Val IT.

AN INTEGRATED APPROACH
The Val IT framework is designed to help enterprises find the answers to four key questions, one of which is ‘are we getting the benefits?’2 The Investment Management (IM) domain within Val IT contains guidance on a number of practical and proven governance principles, processes and practices. This guidance covers three key components:
• Business cases, needed for informed investment decisions
• Programme management, for successfully managing delivery and change
• Benefits realisation—the set of tasks required to actively manage the realisation of programme benefits

These three components are essentially integrated, as they are all focused on successfully delivering the benefits promised in the business case.

There has been increasing focus on benefits in business cases over the last decade to describe the value that is created from investments, both financial and non-financial. It is even more important in the current environment of shrinking incomes and budgets to provide assurance to boards making investment decisions that their capital is being well spent and is creating value for the enterprise. Yet, if one were to ask these same boards how confident they feel that the business cases they have been approving would actually realise the benefits projected, one would find that business executives simply do not believe many of the benefits promised in business cases. Why is this?

It may be due to a lack of quality in business cases, or a lack of faith in the enterprise’s programme management capability. What these executives might not realise is that even with a good business case and sound programme management in place, their ability to fully realise the benefits promised will be severely hampered unless there is also an effective benefits realisation process throughout the full economic life cycle of the investment.

As a discipline, benefits realisation is non-existent or immature in many enterprises. So, what should an effective benefits realisation process involve? How should the benefits from investments get accounted for, reported and harvested? Who is involved and who is accountable?

BUSINESS CASES—COMMON MISTAKES
The foundation of benefits realisation is the business case, yet many organisations have less-than-effective business case practices, including:
• Making benefits predictions that are clearly not achievable
• Lack of explanation as to what type of financial benefit is expected, e.g., avoided cost vs. direct savings, or revenue protection vs. incremental revenue
• Lack of clear understanding as to how or whether the benefits will be converted from ‘enabled’ to ‘realised’ or ‘banked’. For instance, where a change programme delivers a workload
reduction, the benefits forecast might be described as ‘direct savings’ using an assumed reduction in full-time employee (FTE) numbers—a benefit that the organisation cannot actually ‘bank’ because it has no plan to eliminate or re-deploy those FTEs.

- Attempting to convert every benefit stated into a financial value with calculations often so complicated that they are impossible to understand
- Focusing on use of metrics that will ‘prove’ that the benefits have been realised, as a stand-alone exercise, in ‘n’ years time, with no opportunity to check progress along the way
- Not counting the cost of internal resources that are regarded as ‘free’
- Not factoring in risks or dependencies in terms of how they may affect the projected benefits
- Lack of ownership and accountability for benefits realisation other than the appointment of a high-level sponsor

**EMERGING THINKING**

As a broader base of experience develops around benefits realisation, there is an emerging view that sees benefits realisation as significantly more strategic and dynamic than purely passive reporting:

- It is about business value, not IT value. IT almost always provides new capabilities that then need to be exploited or leveraged by the business for business benefits to be fully realised.
- Benefits need to be measured routinely and reporting must be integrated with other planning and reporting functions—not regarded as an optional and stand-alone exercise.
- What is measured and monitored is important, but it is vital to understand who is empowered and responsible for making decisions if monitoring reveals that benefits are not on track.

**PRACTICAL GUIDANCE**

The following is some practical guidance (see figure 1 to determine where to find additional information) to consider when implementing benefits realisation processes:

- **Take a pragmatic approach that reflects the enterprise’s current maturity in value management, as well as management’s culture and appetite for change.** Moving the organisation progressively toward better practice is going to be more effective than aiming immediately for best practice.

- **Identify the aspect of benefits realisation that is causing the biggest issue, and fix that first.** For instance, if the biggest issue is the quality of business cases, then consider steps such as providing a coaching/guidance service, issuing standard templates and ‘good’ examples, introducing a validation/quality assurance mechanism, and ensuring that the secretariat of the relevant decision body rejects substandard business cases.

- **Ensure that sponsors are in place and understand and accept their accountability for benefits realisation.** Although widely accepted in theory, executives who readily take

---

**Figure 1—Practical Guidance and Additional Resources**

<table>
<thead>
<tr>
<th>Summary of Implementation Guidance</th>
<th>Val IT Framework 2.0 Processes</th>
<th>Getting Started With Value Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consider the enterprise’s current capability maturity in value management.</td>
<td></td>
<td>Chapter 4</td>
</tr>
<tr>
<td>• Identify and fix the biggest issue first.</td>
<td></td>
<td>Chapters 2 and 5</td>
</tr>
<tr>
<td>• Ensure that sponsors are in place and accountable.</td>
<td>IM1</td>
<td></td>
</tr>
<tr>
<td>• Enlist appropriate owners for intermediate outcomes.</td>
<td>IM4, IM5</td>
<td></td>
</tr>
<tr>
<td>• Keep benefit information up to date and act on variances.</td>
<td>IM6, IM8</td>
<td></td>
</tr>
<tr>
<td>• Run the process through the full economic life cycle.</td>
<td>IM6, IM9, IM10</td>
<td></td>
</tr>
<tr>
<td>• Ensure that lessons are learned.</td>
<td>IM10</td>
<td></td>
</tr>
</tbody>
</table>
accountability for the overall business benefits expected in a business case are a rarity. There is a big difference between a sponsor who says ‘keep me informed’ and one who has ‘skin in the game’. Sponsors may need coaching regarding their responsibilities.

- **Ensure that intermediate benefits are identified and have appropriate owners.** In most, if not all programmes, there will be intermediate benefits along the way that contribute to the ultimate business benefits. The overall sponsor may not be best placed to ensure the realisation of these intermediate benefits—responsibility may better lay with managers in individual business units, such as IT, finance, human resources or sales. A benefits mapping process will help to identify the intermediate benefits that are expected and the most appropriate owners.

- **Maintain current benefits information—either forecast benefits or actual performance—and act on any variance from original targets.** Benefits are not static; benefits forecast at the outset will change over time. If the programme plan changes, the benefits’ forecast should be revised accordingly. As ‘actual’ figures start to come in, forecasts should be revisited and adjusted. Any variance between the original and current forecasts needs to be explained, and appropriate action taken.

- **Ensure that accountability for the benefits realisation process runs through the full economic life cycle of the investment.** Benefits realisation is required from investment selection right through the programme plan and often beyond the official end date of the programme. This is because most programmes, especially IT-enabled change programmes, do not fully realise their benefits until long after the initial investment has been made, i.e., after most of the required capabilities have been delivered and the delivery team has been disbanded. The IT provider may have supplied the delivery team, but the benefits are going to be realised over time by the receiving business units. Recognising this, the programme closure report, usually done just before the delivery team disbands, should account for all the benefits that were expected up to that point, and should project the remaining benefits expected beyond that point, for which the sponsor remains accountable. The final post implementation review should compare the final benefits realised to the original business case. How long to forecast and report benefits is a common question. Quite often, benefits are forecast and reported for up to 24 months after the projected programme closure date. If an opportunity to recover or increase benefits’ delivery is identified during this period, there should be a facility for the sponsor to request funding for a simple task (such as enhanced training) that could make the difference between partially or fully realising the end benefits, without having to create a fresh business case.

- **Ensure that lessons are learned and reflected in improved practice.** Programme closure reports and post implementation reviews are often completed just to get a tick in the box, with little thought given to producing meaningful and helpful content. A summary of lessons learned in the course of implementation is very helpful for other delivery teams involved in similar programmes and also helps decision bodies to better understand the risks involved in similar business cases. This information should be made available to the relevant people—ideally in an easily accessible format.

**ENDNOTE**

1 Based on the ‘Four Ares’ (Are we doing the right things? Are we doing them the right way? Are we getting them done well? Are we getting the benefits?), as described by John Thorp in his book *The Information Paradox*, written jointly with Fujitsu, first published in 1998 and revised in 2003

**EDITOR’S NOTE**

Readers are encouraged to review Val IT ([www.itgi.org/valit](http://www.itgi.org/valit)), 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 it with key governance stakeholders within their enterprises.
Crossword Puzzle

By Myles Mellor
www.themecrosswords.com

ACROSS
1 Improve efficiency of business processes
7 Factor to weigh in all IT project planning
10 Going public abbr.
12 The understood do’s and don’ts in a company and agreed on ways of operating; this has to be considered as part of IT governance and planning
14 Estimate the relative importance of
15 Home country of Silicon Valley
16 “Dear” one, in letters
18 Product sales channel
19 Database term: stores information
21 Binary
22 Expanded
24 Expressed awe for
26 Zeros
27 Underestimate, undervalue, for example
28 Tech dept.
29 Clerk
30 Finish, with “up”
34 Green light
35 Mental illusion
37 Cautions
40 Confidant
41 Recent
43 Very important factor for executives and managers and all concerned in IT governance in any business
44 Lateral or directional?
46 Printing mistake
47 Huge

DOWN
1 Subject referred to in this quote “There are no threats to information technology for which we do not have the tools to combat”
2 Basic building blocks of trust
3 Being involved in corrupt practices
4 Empty promises
5 Type of address
6 Easy decision
8 Vital factor in the success of IT projects in businesses, at every level
9 Layers
11 Operating system, e.g.
13 Bring into play
17 Integrated circuit, abbr.
20 Symmetric difference
23 One of the main drivers of IT innovative projects
25 To give sworn testimony
29 Check out the views of
31 Goes with zero in computing
32 In demand
33 Session to get questions answered
34 Ford __
36 Blueprint
37 Internationally accepted set of guidance materials for IT governance throughout an enterprise
38 Framework and supporting publications addressing the governance of IT-enabled business investments
39 Do something as a result of information
42 Employer number, abbr.
45 Desktop

(Answers on page 60)
ISO 27001 Training

ISO 27001 Lead Auditor

The ISO 27001 Lead Auditor course provides you with the knowledge necessary to perform an audit or take charge in the auditing of an ISMS, information security management system.

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.

Certified by the RABQSA

ISO 27001 Lead Implementer

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

The training is also aligned with best practices with regards to project management according to 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”.

For more information, contact us at training@veridion.net
Business benefits of IT projects are indirect results of complex interactions between technology and business processes in which the technology is embedded. The benefits often include substantial intangible components and take time to materialize since changes in customer perception and business processes are not instantaneous phenomena. There is a dearth of good methods for estimating the magnitude and timing of business benefits resulting from an IT project. Consequently, ascribing monetary values to these outcomes becomes problematic, compromising project assessment.

This article describes a conceptual and computational approach that represents the mechanics by which an IT project generates its specific business benefits, allowing the magnitude of these benefits to be computed and assigned a monetary value. The method can be adapted for use in a variety of project evaluation techniques, including a return on investment (ROI) or balanced scorecard approach. Managerial guidelines are included for its deployment. The approach can improve IT project management and contribute to IT governance practices.

Best practices in IT governance identify “effective and efficient IT investment and portfolio decisions” as an important objective and insist on the definition of “formal investment criteria such as ROI, payback period and net present value (NPV).”¹ In essence, to evaluate or justify an IT project, it needs to be linked to its business benefits, the benefits must be quantified and a monetary value needs to be assigned to these outcomes. However, connecting the dots from a proposed project to its business benefits continues to be a challenge for several reasons.

First, a significant portion of the direct benefits may be intangible.² These intangibles indirectly result in observable behavior that does have monetary value, such as increased purchasing by satisfied customers. However, it is not easy to deduce the magnitude of these indirect effects, leaving two disagreeable alternatives: ignore intangible benefits and undervalue the project, or assign value based on subjective impressions about these benefits and possibly overvalue the project.

Second, benefits often occur later in the system life cycle. Time taken to implement the technology and, more important, revised business processes means that benefits may not accrue until well after implementation is complete and most of the costs have been incurred. It is difficult to deduce the timing of benefits, yet any ex ante project evaluation demands that the timing be considered in the analysis.

More generally, the major difficulty in assessing IT projects is that the business benefits resulting from them are indirect nth order effects of complex interactions among the technology, organization and business processes. The difficulty of articulating these interactions clearly and precisely makes it hard to assess a proposed IT project based on quantified costs and benefits.

Financial metrics, such as ROI, NPV and internal rate of return (IRR), are commonly used to evaluate IT project proposals. The basic input required for all these methods is a revenue stream that the project is expected to generate over a specified time horizon, \( R_1, R_2, R_3, \ldots, R_N \). Then they incorporate the time value of money in some form. For example, the well-known expression for NPV is:

\[
\text{NPV} = \frac{R_1}{(1+i)} + \frac{R_2}{(1+i)^2} + \frac{R_3}{(1+i)^3} + \ldots + \frac{R_N}{(1+i)^N} - C_0
\]

In this expression, \( i \) = periodic interest rate and \( C_0 \) is the cost of the project incurred at time zero. An ROI calculation would estimate the present value of revenue \( R_{pv} \) and cost streams \( C_{pv} \) and compute the ratio \( (R_{pv} - C_{pv})/C_{pv} \). An IRR calculation would compute the value of \( i \) that makes project NPV zero. Thus, even though capital budgeting methods vary in their
computations, they are only as good as the estimates of revenue and cost, which in turn depend on how well costs and benefits have been quantified.

Traditional capital budgeting methods have been enhanced using the balanced scorecard (BSC) approach. The objective is to balance financial criteria with nonfinancial criteria. The BSC encourages a richer assessment of projects beyond just the financial view, but does not specify how to quantify the nonfinancial criteria. For example, IT governance guidelines for the Commonwealth of Virginia, USA, prescribe a BSC approach to justify IT investments by state agencies. Figure 1 shows a page of the document that identifies criteria for the stakeholder perspective. Notice that the “scores” are not numbers, but letters (G, Y, R) corresponding to the colors green, yellow or red, and the process by which information from the third column yields these colors is not specified. Moreover, the sources in the third column require that benefits be identified and quantified. In short, the core problem of quantifying business benefits of an IT project remains, even in an evaluation process such as BSC, which is seemingly richer than a straight financial analysis.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Score</th>
<th>Evaluation Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. To what degree does the proposed investment result in significant tangible and intangible benefits for stakeholders?</td>
<td>G = Significant tangible and intangible benefits identified and justification provided Y = Tangible and intangible benefits identified and no justification provided R = No benefits identified</td>
<td>Proposal—F. Financial Estimate 1. Cost-benefit analysis summary</td>
</tr>
<tr>
<td>2. To what degree does the proposed investment target stakeholders that have been chronically underserved by IT investment?</td>
<td>G = Underserved stakeholders identified and justification provided Y = Underserved stakeholders identified and no justification provided, or stakeholders adequately served at present R = Stakeholders adequately served with existing assets now and over the proposed investment’s life</td>
<td>Proposal—B. Project Purpose 1. Business problem 2. Project business objectives 3. Core business activity impact Project Charter—E. Project Description Scope and Management Milestones 1. Project description 2. Scope</td>
</tr>
</tbody>
</table>
METHODOLOGY

The foregoing discussion indicates that the weak link in estimating project benefits is an inadequate articulation of precisely “how” these benefits are generated. Literature observes that “…traditional capital budgeting models have failed to estimate true IT values due to their inability to measure complex interactions within the organization” and “…an IT performance measurement and management system must focus on the causal relationships and linkages.” Therefore, the way to address this core problem in IT project valuation is to capture the mechanics by which information processing effects of the project result in business outcomes. The methodology proposed here is based on systems thinking principles that provide formal constructs to represent the causal structure of a system and, thus, capture the interaction among technology, business processes and the resulting business benefits. The suggested approach is illustrated with the following example.

A GENERIC IT PROJECT

When a customer calls into a call center, the business can use that session to sell new products/services or perform other tasks that enhances its relationship with the customer. A proposed IT project will make technological enhancements to increase the service capability. The specific enhancements are not important for this illustration, but figure 2 suggests different areas where this could occur. For example, the database server capacity might be increased, the Private Automatic Branch Exchange (PABX) software may be upgraded for more efficient call distribution to agents, the agent’s terminal can be enhanced for greater functionality, etc.

Expected business benefits include:
• Cost savings resulting from a decrease in the number of agents required
• Reduction in customer turnover
• Increase in number of new customers attracted to the firm

How can the business benefits be quantified to help make the business case for this hypothetical project? Both difficulties mentioned in the introduction are present here. As service capacity improves, customers will spend less time on hold, have their queries answered more effectively and have a more satisfying experience. However, this benefit is intangible and can be monetized only when the turnover rate starts to decrease. Additionally, the benefit is not immediate since existing customers take time to perceive and react. As existing customers become more satisfied, word-of-mouth effects will attract a larger volume of new customers. These two observable business benefits occur much later, after implementation costs have already been incurred.

The preceding narrative description of how and when the observed benefits are generated can be represented more precisely using the systems thinking construct, called a causal loop diagram (CLD), as shown in figure 3.

There is evidence that it is not difficult for nonexperts to develop such a CLD after a brief introduction to systems thinking constructs. The advantage of a CLD over a narrative in making the business case for the project is that it forces proponents to articulate the mechanisms by which business benefits will be generated. They are forced to make explicit their mental models of these benefits and sharpen the arguments for making the business case for the project.
For example, using figure 3, one can be more precise about how the call center project generates business benefits. Loop B1 (Firm’s Customer Base → Average Service Level → Satisfaction Level of Existing Customers → Departing Customers → Firm’s Customer Base) is a negative feedback loop and says that, in the absence of service capacity changes, if the firm’s customer base increases, the call center’s service level will decrease, which in turn will reduce satisfaction levels and gradually lead to an exodus of existing customers. Similarly, Loop B2 (Firm’s Customer Base → Average Service Level → Satisfaction Level of Existing Customers → Firm’s Reputation for Service → Arriving New Customers → Firm’s Customer Base) indicates that the arrival of new customers increases the firm’s customer base, which, in the absence of a service capacity increase, will reduce service levels. After some delay, this will lower the firm’s reputation for service and choke off the inflow of new customers. The proposed project will increase service capacity, which means that B1 and B2 will interact to gradually increase the firm’s customer base to a new equilibrium level. In short, using the CLD, those evaluating the project can inspect the reasoning carefully for errors of omission or commission. For instance, one could point out that figure 3 is missing all the potential benefits on the operations side, e.g., call center staffing and agent turnover. An informed decision would then have to be made as to whether or not those back-end benefits should be included in the analysis of this project. If they are included, an expanded causal loop of benefits would result.

The CLD of figure 3 can be converted into an equivalent causal structure, called a stock flow model, as shown in figure 4. The conversion process is well defined in the systems thinking methodology and details can be found elsewhere. What is relevant here is that a stock flow model can be implemented in software to yield a computational tool whose scenario simulations take the analysis beyond qualitative reasoning and provide numerical estimates of the magnitude and timing of benefits. Figure 5 shows a sensitivity analysis where the model was simulated for three different values of project duration. When the duration is short, the firm’s customer base increases to its new steady state much sooner than when the project duration is long (i.e., the y axis of figure 5 is normalized). Using historical data on revenues generated by a single customer, it should be possible to put a monetary value on realizing the business benefit significantly earlier, which can then be compared to the additional cost of shortening the project duration. So, the tool allows evaluators to quantitatively evaluate cost-benefit trade-offs and the timing of business benefits.

Figure 6 shows another simulation run that indicates that customer turnover rate is expected to drop from 9 percent to about 5 percent, and that this reduction will take about 40 weeks to materialize. Historical data on the costs incurred in attracting a new customer and the revenues generated by existing customers can then help quantify this reduction in turnover rates. For purposes of this illustration, the absolute values of variables in these graphs are less important than observing how the proposed method has the ability to estimate both the magnitude and timing of the business benefits associated with the project.
Managerial guidelines for deployment of this approach are shown in the form of a grid (figure 7). The x-axis represents the anticipated project budget, while the y-axis represents the relative proportion of “soft benefits” within the total benefits claimed for the proposed project. Soft benefits mean intangible benefits and their resulting observable business outcomes over time. The rationale behind the grid is simple: if the project budget is small, the costs associated with developing and calibrating stock flow models of the project’s benefits probably cannot be justified. Hence, neither the southwest nor the northwest quadrant of the grid recommends going to a full stock flow model to justify the project. The traditional financial metrics and analyses should continue to be used, supported by narratives of the benefits. When the budget is low and soft benefits are high, adding only the causal loop diagrams to the existing justification approach is recommended to enhance the narrative justification of benefits. The additional cost incurred with developing a CLD would be modest.

If the project budget is large, the expected benefits from the project would also be large, and it would be prudent to quantify these benefits as accurately as possible, because the consequences of a mistake are more serious. This scenario is covered by the southeast and northeast quadrants of the grid. When the budget is large and the proportion of soft benefits is low (the southeast quadrant), it is recommended to utilize traditional financial metrics, but deploy the stock flow model of benefits to obtain a more accurate estimate of the timing of revenues that would serve as input into the financial calculations. Since the proportion of intangible benefits is low in this scenario, purely financial metrics should suffice, but it is important to estimate the timing of project benefits. As the scope of the project is large, its outlays will probably occur over a period of time and the benefits will be realized over several periods. If the budget is large and the proportion of soft benefits high (the northeast quadrant), execution of the full stock flow modeling is recommended to quantify the different criteria that go into a BSC-type assessment. The additional effort required for the modeling can be supported by the large project budget, and this type of modeling would also help to quantify the nonfinancial criteria prevalent in the BSC assessment. In summary, the grid helps judiciously deploy the approach into existing practice in a way that balances the costs and benefits of the method.

**CONCLUSIONS**

Evaluating an IT project, or making a business case for one, continues to be a difficult task. IT is used not just to reduce labor costs, but to also compete, obtain new business and increase revenues. As IT projects continue to permeate all aspects of organizations and their business processes, the benefits they yield can be multifaceted and far-reaching. Whenever an IT project is proposed, proponents always have a mental model of how its benefits arise, but that logic may be ill-formed and imprecise, making it hard to make a
business case convincingly. The approach discussed in this article will improve the precision with which such mental models of benefits can be articulated and, thereby, advance the conceptual foundations and practice of IT project assessment. The method proposed here is flexible enough to be integrated into existing assessment approaches such as ROI and BSC. Thus, adopting it would not require wholesale changes to existing practice, which is another reason for its consideration by the practitioner community for ex ante justification of IT projects.

ENDNOTES
1 IT Governance Institute, Control Objectives for Information and related Technology (CobiT), USA, 1996-2007, www.isaca.org/cobit
3 Epstein, M.I.; A. Rejc; “How to Measure and Improve the Value of IT,” Strategic Finance, 2005, p. 34
8 Ibid.
10 Op cit, Coyle
11 Op cit, Senge
When did governance and risk management begin being thought of as nonrevenue generating? Could it have been about the time that organizations, products and services got so complex that businesses could no longer be understood end to end? Focus was lost on the basics—the business basics that every shopkeeper (convenience store, hardware store, specialty farm, dress boutique, lawn service, web store) knows.

For the shopkeeper, governance and risk management are neither complex nor nonrevenue generating. For the shopkeeper, they are just part of smart business—part of earning a profit for serving customers. What shopkeepers have that others often do not are:

• An end-to-end view of how their business works
• Full accountability for profitable growth
• The ability to balance the cost and benefit of governance and risk management to achieve those objectives

In this article, the example of the shopkeeper will be used to help readers recover and communicate a more proactive, value-added view of governance and risk management. This fundamental understanding is all the more important today, because the difficult economic environment demands tough choices. This is the view intended by Val IT, Control Objectives for Information and related Technology (CoIT) and Risk IT, the enterprise risk management framework currently in development by the IT Governance Institute (ITGI).

Moving forward in this journey requires one to think about maturity. In this article, with its wide audience and various levels of maturity, maturity will be reviewed from a different angle—one that will hopefully be helpful to all readers regardless of their organization’s maturity level.

Specifically, several myths and misunderstandings about governance and risk management, which have made it more difficult for firms to generate profitable revenue, will be discussed. These myths can hinder an organization moving from 0 to 1 as much as they can an organization moving from 3 to 4 (especially when the move involves broadening maturity across the enterprise).

These myths and misunderstandings are particularly dangerous because they not only misguide actions; as they circulate through the organization (whether actively or passively through behaviors that imply them), the injury grows.

To make them easier to consider and overcome, they can be divided into three groups:
1. Those involved in structuring the way decisions are made
2. Those involved with structuring and guiding a program
3. Those involved with applying tools and techniques more efficiently and effectively

A WORD ON WORDS
The terminology must first be reviewed. People are often unclear on exactly what “governance” and “risk” mean. It is not that the terms are unclear. Rather, they have been used in such a precise way by different groups that the varying definitions make them appear unclear. These different approaches bump into each other as each matures and seeks a more holistic approach and definitions. So, their differences become more noticeable and more confusing to the casual listener. Take, for example, terms like “car” or “child.” These are used everyday, but they have very different meanings with significant legal or other consequences depending on context.

“IT governance,” according to CoIT 4.1, is “the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise’s IT sustains and extends the organization’s strategies and
objectives. Other ITGI materials provide additional insight, including the important point that governance happens in layers (organizational layers). Of course, ITGI’s primary view of the five IT governance focus areas is alignment, value delivery, risk management, performance measurement and resource management. Other definitions of governance, including those outside of ITGI, stress terms such as “accountability,” “decision rights,” “performance” and “desirable use of IT.” A practical way to think of governance is getting the right information to the right people at the right time to make the right (or at least better) decisions. Then, of course, ensuring accountability so those decisions actually happen as intended.

Remembering the shopkeeper analogy, governance exists from the first day a store owner hires the first manager and, thus, the shopkeeper is no longer directly managing all affairs of the store. In an IT governance context, it is about how the shopkeeper uses IT—among other resources such as people, cash, equipment and intellectual property—to drive profitable revenue over time through the use of those assets. This is return.

Return, of course, is not easy to obtain. One cannot put US $10 in a magic return machine and get a guaranteed US $12 back. How one uses US $10 or any other assets comes at a risk in pursuing return. Some uses of assets work better than others. In convenience stores, the shopkeepers decide which items to stock and how much to stock. There is a risk of buying too much or too little. In an IT sense, will the new web site reach above the noise and generate new return or be lost in a sea of competitors? Should one invest in onsite, offsite or no data backup?

“Risk management” is defined as “the coordinated activities to direct and control an organization with regard to risk” (in this context, the term “control” is used as a synonym for “measure”).

A “risk” is simply the chance that a change will occur. Specifically, it is the likelihood the change will occur multiplied by the impact if it does. Like “car” and “child,” the word “risk” is used in many different contexts. Sometimes it has been used in a specific way for decades (as when it refers to an investment portfolio, industrial failure or automobile insurance policy), and sometimes it is used imprecisely in casual use (as when someone says “reputation risk” when they really mean reputation damage as a consequence of a negative change).

Organizations can communicate more easily by being:
- Sensitive to people using terminology distinct to their professional backgrounds and bridging that terminology gap
- Aware when people are using terms casually rather than precisely

With this setting of the stage, it is now time to move on to the first group of myths and misunderstandings—how decisions are made.

HOW, WHEN AND BY WHOM DECISIONS ARE MADE
An often-mentioned myth or misunderstanding is that better governance and/or more risk-aware governance will take too much time or cost too much. This is typically mentioned by people who:
- Think that “governance” means only dead-weight compliance
- Are getting more resources under the current governance structure than is appropriate (and, thus, feel threatened by more transparent and accountable decision making)

There are at least two variations on this theme:
- One focuses on paperwork and worries that governance is a “feed the monster” exercise of reporting. On the risk side, the phrase “drowning in spreadsheets” comes to mind. Like storybook myths and fears, there is some truth here. Initiatives have been implemented that are too heavy on process and too light on changed decision making for improved value and outcomes. Governance can get out of balance. There may be sufficient processes to get the right people involved with the right information at the right time. But there may be too little automation, so that manual paperwork gets out of control.
- Another worry about improved governance says that involving the right people at the right time will stretch out decision making and slow business responsiveness. The question implied here is whether the added decision makers/overseers are actually the right people or not. As the saying goes, too many chefs can be a problem in the kitchen. On the other hand, leaving out key people has created problems, particularly those involving requirements that are costly to add or fix after time has passed. In the world of IT, this is especially bad when requirements from various lines of business, geographic areas, or legal or compliance perspectives are missed until late in the game.
Two other myths are even worse, because they represent gaps in senior management culture/judgment:

- The first is a view that improved governance is not needed because leaders of business lines, initiatives or projects are smart people, and they should just make it work. That’s why they are managers. This culture implies that leaders are not smart if they cannot—on their own—solve the governance problems that are in their way. This is just an office version of playground dares. This is really an abdication by those senior managers who should be putting a shared governance process in place to resolve these challenges across the organization. A shared process can help avoid one-off and inconsistent solutions to common oversight problems. Even if the specific solution is not the same in each situation, a common process for resolving the issue can reduce time and save cost.

- The second is a view that says “we do not have time for governance, we are focused on making revenue.” This view implies that (1) the organization does not already have a governance process and/or (2) whatever is being done currently is bringing together the right people at the right time with the right information to make the right decisions to drive revenue (or, better, return). Of course, it’s apparent that governance always exists, it is just a question of clarity, efficiency and effectiveness. It may be that the organization is already great (and just does not use the word “governance,” which is fine). However, it is more likely that its revenue is being damaged because it is not making decisions that focus resources on the best revenue opportunities or it pursues revenue without thinking enough about the risks and costs of seeking that revenue. Examples include high-growth firms that are burning cash too quickly due to excessive marketing and sales costs and the sales vice president who wants to sign a contract that stretches an organization’s ability to deliver. This said, revenue should not be the main financial metric because it is only part of the story:
  - Return is much more helpful, because it brings attention to how well resources are used in bringing revenue in the door.
  - In this way, return helps focus on waste and points to opportunities for improvement.

So what would the shopkeeper in the little store think about all of this?

- Shopkeepers have the advantage of knowing the business end to end, so they know whom to involve, including parties in their extended enterprise, such as suppliers, customers, accountants and more.

- Because the shopkeepers’ personal time is involved, they seek repeatable solutions to save them time and effort in the future.

- Finally, because the shopkeepers are spending their own money, they are concerned about risk as well as return, to help revenue grow more cost-effectively. Yes, small business owners often take lots of risk with their homes and their families’ financial security at stake. But because they know their businesses (and the IT dependencies) end to end, they are more likely to be truly aware of the extent of the risk they are taking in offering a new product, opening a new location, making an IT investment or signing a new customer contract.

In short, the decisions are all about risk and return to more effectively use resources, including IT. The more dependent the business is on IT, the more crucial the IT decisions become.

These areas of governance processes and decision making for improved value are so pervasive that they are touched on in multiple documents from ITGI. A few of the most important are:

- **IT Alignment, Who is in Charge?**—This is an overview of the strategic alignment focus area and a good initial read.

- **Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0**—See especially chapter 1 and the Responsible, Accountable, Consulted and Informed (RACI) charts in chapter 6.

- **Board Briefing on IT Governance, 2nd Edition**—See especially the checklist in appendix A, which includes speed of decision making, and the emerging enterprise model in appendix H, which stresses the need for adaptability and agility.

By definition, improved governance should bring added efficiency and effectiveness in making decisions that drive more value. If the organization’s governance is not doing this, it should stop. Something is wrong.

For example, in addition to the ITGI materials, IBM uses an approach to help select a governance style appropriate to the organization based on a number of key success factors. In short, governance should help the organization become more resilient, responsive and agile (pick your favorite term) in...
both protecting it and taking advantage of opportunities that arise from change events. This is not just revenue, but revenue when the pressure is on to perform.

Now that the key points on the who, how and when of decision making have been covered, it is time to move down one level into programs, using risk management as the example.

GUIDING PROGRAMS
At this level, the first thing to look at is some common mistakes made (and the myths they create).

As a reminder, there are two forms of risk management.
• Risk in the **financial management** sense of risk and return, looking at it from the perspective of risk in IT investment projects as well as IT risk in business operations that can be reduced through some improvements in culture, process or automation (this is the form primarily used in Val IT)
• Risk in the **operational management** sense, looking at the IT risk that is in the current technology environment and how to better manage that risk (this is the form used in ConIT)

In this discussion about programs, IT risk will be primarily viewed from an operations management standpoint (for simplicity), but the financial view will also be noted.

The common mistakes with regard to programs include the following.

1. **“Silo y and IT Risk”**
IT risk is often viewed silo by silo, rather than as parts of a system that is needed to produce some IT services for the business. In the same way that a factory has many components on an assembly line to produce a product, IT has many aspects—the complexity of which increases with the complexity of the IT and business environments.

IT risk is not only IT project management, network intrusion prevention, IT change management, disaster recovery, energy availability, people protection or any other silo or type of IT risk. Like a factory, airplane, automobile or any other system, everything has to work together. Weak links are a key focus.

From a program perspective, when IT risk is separated into silos, each of those silos consumes resources performing similar steps of risk management, the owners of each silo conduct their own evaluations and take their needs to the business, and each silo struggles to demonstrate business value to a business activity. Yet, showing business value is difficult when risk is viewed in pieces, and it is even more difficult to see which risks most need investment to fix. In the factory example, which is greater: the risk of out-of-stock parts or the risk of equipment failure?

Taking an end-to-end view based on a given business activity not only provides more immediate business value, but also saves time and effort by reducing duplicate work and making priorities more clear to the organization.

Shopkeepers see this easily. They see the end-to-end business. Shopkeepers are concerned about the risk of inventory going bad as well as the risk of not making a sale because the shop is out of stock. They are concerned about wireless hacks into the store’s point-of-sale (POS) system and recovery of corrupted accounting data. When shopkeepers consider what to improve, they make the trade-off between improving POS system performance and reducing wait time at check out. As above, they understand the business end to end, are accountable end to end, and make risk and return balancing decisions.

2. **“We Are Practical. We Let Our Program Evolve. We Do Not Need a Plan to Improve.”**
Again, there is a bit of truth here, especially if the program is already quite mature. Of course, everyone wants to be “practical,” because that word is attractive. However, those with quite mature programs generally arrived there by understanding that a program needs the right information from the organization and the appropriate business-driven target to achieve that maturity. High returns do not just happen by themselves.

In short, risk management, governance, value assurance or any other program needs a clear objective and path to get there. Lacking a clear objective, a program can be doomed from the start to just wander in the desert. Lacking a clear pathway (including tools to improve efficiency), the objective is always a bit out of reach because it is overwhelming to the organization in terms of time and effort. When the organizational culture deprives the program of this clear objective, success becomes far more difficult to achieve.

The lesson here: well-defined plans and governance mechanisms are key.

A shopkeeper learns this lesson every day. Because small businesses do not have the cushion of big enterprises’ organizational, information and financial buffers, excessive risk and insufficient return in small businesses show up fast.
With regard to program management, the publications and approaches of ITGI have even more to say:

- Both Val IT and CobiT have a repeating focus on business objectives that requires an end-to-end view of a business activity. The references repeat in each of the process groups.
- The need for a continual, informed, targeted improvement process is described in both Val IT and CobiT, including their maturity models and process steps. It is even baked into the purpose of CobiT: “...continuous improvement and monitoring of good IT-related practices.” The control loop diagram of CobiT is predicated on this thought.
- The Board Briefing puts it this way: “For effective IT governance to be implemented, enterprises need to assess how well they are currently performing and be able to identify where and how improvements can be made. This applies to both the IT governance process itself and all the processes that need to be managed within IT.”
- With these and other quality-assurance-driven views of continual improvement, it is surprising that so many organizations’ cultures still take a “practical evolution” view of improvement. For those organizations where it is most difficult to communicate, the IT Governance Global Status Report—2008, figure 51, may be helpful. When 749 respondents ranked the two principles that delivered the most value, the second-highest-rated principle was “continuous improvement exists among value delivery practices.”

In short, getting to revenue (and, better, return) requires making a series of sales and delivery steps occur, so the register can ring. And many potential stumbles can prevent a sale. Worse, stumbles can also hurt profit and reputation, which can impair future revenue. By crossing the silos, looking end to end and having a focused objective against which to plan improvements, organizations can move forward. Without these, return faces high risk.

This leads to the last group of myths and misunderstandings—those involving tools and techniques.

**TOOLBOX FOR IT RISK AND RETURN MANAGEMENT**

There are many tools left in the toolbox or left unused by the average practitioner. While it is okay to select tools appropriate to the task, it is important to know that a screwdriver drives screws (and why one might prefer screws to nails), that is, which tools to choose and why.

This section focuses on tools used for IT risk management because of the newness of this topic to many *Journal* readers and because of the upcoming release of Risk IT (the new framework from the IT Governance Institute).²

The following sections will describe a few tools and their misconceptions.

1. **“Top IT Risk Lists Can Guide Our Focus.”**

   “Please send in your top five IT risks by October 1; read the e-mail.”

   These e-mail blasts go to select individuals at many enterprises. Widely used, they are helpful for many organizations starting down the IT risk management path.

   Yet, they have weaknesses, including the selection of respondents, depth of knowledge of respondents, clarity of what a risk is, timeliness of information, and extent of linkage between business exposures and the dependencies on IT. These are just a few of the reasons why top-risk lists should be used with great caution.

   Caution is further urged because, while these collected views are plugged into rather scientific-looking charts and graphs, no amount of window dressing makes up for weaknesses in the initial data quality.

   Thinking back to shopkeepers, such lists can be generated in less time than it takes to have a cup of coffee. However, the extent to which it is an accurate reflection of real risk is based on the fact that shopkeepers can see both the business activities and the IT dependencies. To the extent that shopkeepers do not understand IT, the same alignment or dependency problem exists. To the extent that shopkeepers do not understand wireless networks, business partner IT connections or storage capacity, they will be blind to the range of potential risks.

   Real IT risk analysis requires informed insight and real data.

2. **“Self-assessments Are Our Primary Risk Management Tool.”**

   In many ways, self-assessments represent an extension and improvement over the “top IT risk lists.”

   Yet, far too many organizations build their IT risk management programs around risk (also known as risk and control) self-assessments. These are helpful to get a qualitative view of risk and controls for firms just starting down the path. However, they make several key assumptions:

   - That the respondents have an informed view
• That controls or other indicators are actually sufficient in design scope and accurate in use
• That the data are timely and complete enough to predict and avoid problems in IT projects, operational stability, availability, protection and recovery

Back to the shopkeepers, self-assessments are less necessary because of shopkeepers’ more complete knowledge of their business. However, shopkeepers might still lack visibility into much operational data just because of the quantity of the data—everything from inventory levels to server performance to data recoverability.

In short, self-assessments are a helpful tool, but should not be a primary tool.

3. “If We Only Had ‘The’ Standard Risk List.”
Risk checklists, of the type often published in magazines or other industry sources, provide a sense of comprehensiveness. They are a significant improvement over top five lists and many self-assessments, if the risk list is more comprehensive and helps the organization see a broader potential range of threats to a broader range of assets. Yet, the breadth is only as good as the list.

While risk lists might look at threat types (hackers, floods), assets (servers, networks, buildings) or consequences (reputation, fines), they usually do not show how these threats interrelate (or even all these types). So while risk lists can be helpful on the organization’s path to maturity, they can also become a distraction as IT risk managers go in search of the ultimate risk checklist, instead of understanding their organization’s business processes and dependencies on IT. Nothing replaces knowing one’s own business.

In each of the examples so far, what is missing is scenario analysis. Scenario analysis is simply a mapping of different situations that can threaten or provide an opportunity for an organization. Scenarios are part of everyday life. For example, a little boy accidentally throws a ball through a neighbor’s window and glass gets everywhere. Consequently, there are costs to repair the window and clean up, and to the boy’s reputation.

In scenarios, there are actors, actions, objects, impacts and consequences. A similar type of scenario analysis helps organizations understand the range of potential changes that can threaten their IT resources or provide ways for IT to help take advantage of business opportunities.

Of course, scenario analysis can be handled poorly. If the number of scenarios is small and/or not well considered, there is very little benefit. To be effective, scenario analysis must help more people see more risks and more responses.

4. “Risk Is About Playing the Averages.”
Organizations will often look at what is most likely or a combination of likelihood and impact. This is often adapted from accounting risk management. While this is appropriate for risk-based financial auditing, IT systems are different because they are, well, systems and because they are running real operations.

Systems deal with interactions and the likelihood that a problem in one place will be passed to others. Also in systems, little causes can lead to big problems. A “little” error in software updates or equipment failure can have a huge impact on the business.

In this area, Risk IT can offer assistance, especially the framework and guidance sections on risk IT purpose and principles, risk IT foundation, risk IT process model, and technique guidance on scenario analysis. This is also supported by the risk aspect of Val IT (where risk is pervasive as part of risk and return management of a portfolio of IT investments) and ConIT (mostly in the Plan and Organize [PO] 9 process).

IBM has implemented an approach to help implement frameworks such as ConIT and Val IT on matters of risk: The Resilient Enterprise Blueprint. The blueprint is used to help understand the dependencies of business processes on IT, understand the risks to those IT resources, and diagnose and prioritize actions to better manage risk to desired levels.

**CONCLUSION**
Compliance is only nonvalue-added when either (1) it is disconnected from revenue or (2) government requirement exceeds business value. ConIT and Val IT do not talk about “compliance” as much as they talk about “outcomes,” where compliance is one set of outcomes along with other value and performance measures. By combining compliance and performance outcome reporting, organizations can save time and effort.

In considering all the myths and misunderstandings, one reason that people make the wrong decision is that they either overestimate the cost of doing it right or underestimate the
consequences of doing it wrong. The opportunity here is to better show one’s organization the pain of failure and how to more easily do the right thing.

How? One might start by doing like the shopkeeper and taking an end-to-end, accountable view that balances risk and return. Think simple.

Thinking simple can help one design governance mechanisms for the organization that bring accountable decision makers together so that their behaviors are driven in a way that is end to end, clearly accountable and with balanced risk and return. In this way, the power of improved governance and risk management to drive return can be demonstrated.

Finally, one might consider using the items previously mentioned as a “health check.” The more negative behaviors an organization exhibits, the more difficulty it will have in implementation and the less value it will deliver.

ENDNOTES
3 For more information on the Risk IT framework, please see www.isaca.org.

According to ITGI’s Val IT™ framework, companies that do the following tend to reap significant rewards. Does your organization:

- Continually monitor, evaluate and improve on IT value delivery practices?
- Manage its IT-related initiatives as a portfolio?
- Monitor IT initiatives through their full economic cycle?
- Recognize the different categories of IT-related investments and manage them according to their needs?
- Define and monitor key metrics and respond quickly to changes?
- Assign accountability to appropriate stakeholders to improve benefits derived from IT?

If your organization follows these principles, we’d like to hear from you! Write an article or case study on your organization’s experiences managing IT. Please contact Deborah Vohasek at news@isaca.org.

Further detail about these principles can be found in

CISM Review Manual 2009
ISACA

The CISM® Review Manual 2009 is a comprehensive reference guide designed to assist individuals in preparing for the CISM exam and individuals who wish to understand the roles and responsibilities of an information security manager. The manual has evolved over the past five editions and now represents the most current, comprehensive, globally peer-reviewed information security management resource available.

In response to the evolving field of information security management, the extensively expanded and revised 2009 version of the CISM Review Manual continues to move away from the topic of technology and closer to the strategic governance and management aspects of security. There is increasing emphasis on the overarching concepts essential for effective information security management in addition to focusing on the critical thinking and sound judgment required for the development and management of increasingly massive and complex security systems and related processes. This publication includes a new and expanded approach to the development of effective security management metrics, based on research projects sponsored by the IT Governance Institute® (ITGI®). There is a substantial increase in the scope and depth of coverage on the subject of risk management. An expanded focus and structural improvement is included for information security program development as well as a greater concentration on architecture and metrics. The improved approach to management metrics has been carried through to the section on information security management providing processes to improve overall effectiveness. Also included are case studies to assist a candidate in understanding current practices, definitions of terms most commonly found on the exam, practice questions similar in content to the certification exam and references to additional study materials. This manual can be used as a stand-alone document for individual study or as a guide or reference for study groups and chapters conducting local review courses. It is a primary reference resource for information security managers seeking global guidance on effective approaches to governance, risk management, program development, management and incident response.

The 2009 edition has been developed and is organized to help prepare the CISM candidate in understanding the essential concepts and studying the following job practice areas:

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

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

ISACA

The CISM® Review Questions, Answers & Explanations Manual 2009 consists of 450 multiple-choice study questions that have previously appeared in the CISM® Review Questions, Answers & Explanations Manual 2008 and the 2008 Supplement. These questions are not actual exam items, but are intended to provide 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 2009.

CISM Review Questions, Answers & Explanations Manual 2009 Supplement
ISACA

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

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

CISM Practice Question Database v9
ISACA

The CISM® Practice Question Database v9 combines the CISM Review Questions, Answers & Explanations Manual 2009 with the CISM Review Questions, Answers & Explanations Manual 2009 Supplement into one comprehensive 550-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 CISM 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 ISACA® Journal, formerly Information Systems Control Journal, articles referenced in the CISM Review Manual 2009. Available in CD-ROM format or as a web site download.

MDB-9  English Edition—CD-ROM
MDB-9W  English Edition—Web site download

To order CISM review material for the June/December 2009 exams, see the order form on page S-8 in this Journal or visit the ISACA web site at www.isaca.org/cismbooks.
Value of IT: Beyond the Theoretical

For years, business and IT leaders have sought to convey the value of IT. Boardroom discussions have requested it, managers have attempted to measure it and IT professionals continue to aggregate hordes of information to develop metrics to measure it. This effort continues to have one key deficiency—that is simply that there is an end. A report, a presentation, a dashboard with many colors seem to culminate as the peak and final destination for presenting value cases for IT. The often discussed, but never executed, process of measuring value in continuum seems to always fade behind other business objectives and priorities.

GOVERNING VALUE
The above scenario is very common. In most respects, the fault lies with the lack of governance—nearly a modern-day cliché for IT and information systems (IS) professionals. The lack of IT governance continues to be an epidemic today in IT. In a study conducted by senior scientists at the Massachusetts Institute of Technology (MIT) Sloan School of Management, senior managers at 300 worldwide enterprises were asked whether they knew how IT was governed within their company. On average, only 38 percent of surveyed managers responded positively.\(^1\) Results from this and other similar studies cite a lack of IT governance as a primary culprit in the lack of awareness and direction from many leaders in IT.

Relating governance deficiencies to the issue of value begins with the realization that IT governance is crucial in supporting IT objectives, which should be built upon clearly defined business objectives. IT and business governance serve as the fundamental building blocks for value governance. By clearly illustrating how IT workflows and investments support defined IT objectives, subsequent governance efforts to these two fundamentals (IT and business objectives) can be continuously sustained and seen in the light of value. Governing value across IT investments essentially translates into guidance. A governance group should continuously guide an IT organization to follow developed policies, standards, guidelines—all of which should be created in support of IT and business objectives. Regrettably, members of the organization rarely bridge the idea of governance to IT and business objectives. The lack of effective and ongoing communication (of these values) is more the rule than the exception in most organizations. Governance groups provide a slightly better role of communicating policies, standards and exception criteria than relating back to the bigger picture of objectives. In a world where continuous monitoring of networks, end points and data access is commonplace, there exists a great void in continuous and effective communication of the workflow depicted in figure 1.

What is valuable originates with the strong understanding of a company’s business objectives. IT objectives, in support of those goals defined by the business, should provide the criteria on which IT governance is executed. Efforts or acquisitions that do not translate back to supporting an IT objective should not be supported, regardless of other inferred value propositions that may come from internal IT groups or even vendors.

Governance, therefore, provides the strategic efforts that ensure value perception.\(^2\) Defining preferred platforms, supported/nonsupported network protocols and data privacy controls are simply a few exemplary workflows sponsored by IT governance that help ensure that IT efforts remain on point. Indirectly, IT governance is guiding the actions of its constituents, so that their processes and purchases do not deviate off course.

Tony UcedaVelez, CISA, CISM, GSEC, is the founder of VerSprite, an Atlanta-based risk advisory firm specializing in strategic security initiatives that support business objectives. For the past 10 years, UcedaVelez has worked with numerous Fortune 500 organizations in the areas of risk management, application security, security governance, vendor risk management and network security. He has published articles revolving around the theme of strategic security processes, including topics on application threat modeling, maximizing the return on security investment via the Val IT framework, and a hybrid approach to vendor risk management efforts. UcedaVelez has presented these topics at various ISACA events. He is a frequent guest speaker for TechRepublic’s webcast events related to information security and risk management. UcedaVelez serves on the board of the Information Systems Security Association’s international election committee and is a member of OWASP and ISACA. He can be reached at tonyuv@versprite.com.
IT governance should, however, address the value dilemma head-on, as well as define the criteria for which it will be measured. After all, what factors assist in measuring value in IT? Is it return on investment (ROI), improved efficiency as reported by other internal metrics in other groups (e.g., marketing, sales) or improved company morale (as measured and reported by human resources)? These are the questions that should be asked by a governance group—a team composed of a cross-section of business and IT executives within an organization.

**THE COLLECTION AGENCY: APPLYING VALUE GOVERNANCE**

Moving beyond the theoretical, this article also examines how value governance can be applied to a sample generic case of debt collection.

Management for XYZ Collection Agency LLC has defined one key business objective: maximizing recovery levels. As part of this objective, it has defined how these levels will be measured. Forms of measurement such as collection efficiency (CE) ratios and days sales outstanding (DSO) are used to measure how effective the agency is in maximizing recovery levels.

In an effort to improve upon the CE ratios at the collection agency, the business turns to technological innovation to reduce DSO numbers. In this case, the business may know of technological investments that can help collect outstanding accounts faster. One IT investment highly sought by the business in this case is the autodialer with predictive software, which is used to improve the efficiency in which calls are made and tracked to delinquent consumer accounts. Without the use of the autodialer, outbound calls are made manually by collection employees. This takes a substantial amount of time to find a relevant account, dial the number and deal with busy lines, disconnected phones or no answers. In this case, the autodialer with predictive software is able to quickly find valid phone numbers and queue up a qualified list of targets for the collections agent. Busy calls are never sent to a collections representative, nor are calls that have disconnected phone numbers. In these cases, accounts are also automatically updated by the autodialer.

So, how does an organization govern the value of this worthwhile, yet costly, investment? It begins with determining the value that the organization is attempting to create via the purchase of the autodialer as well as the value that should be sustained by its ongoing use and maintenance. XYZ Collection Agency did define a business objective that could be positively affected by some business automation via the autodialer.

However, what are the costs associated with managing this new technology? Do sufficient resources exist to support this new technology? How well does the new technology integrate into the IT infrastructure? These are just some of the questions that value governance is able to address collectively.

**BEYOND AUTOMATION**

The use of business automation and artificial intelligence (AI) automatically suggests value for many business leaders. Automation can often be hyped to the point where all other important criteria for measuring value take a backseat. In the collection agency, the concerns about integration, resource commitments and ongoing support costs may not outweigh the short- and long-term cost savings that an autodialer can provide. However, when more complex IT investments, such as enterprise resource planning (ERP) systems, are not examined against other key criteria, determining value can easily get lost in the discussion.

Given the ever-increasing global marketplace and recent economic challenges facing many enterprises, optimization is the new frontier beyond automation. With the term “optimization,” there is an incorrect association that it is elusive, unobtainable and unable to adjust to changing conditions. Rita Heise, CIO at Cargill, attested to this in a roundtable discussion sponsored by Dartmouth’s Tuck School of Business, as shown in the following excerpt:

> Heise asserted that process optimization and flexibility are not necessarily incompatible.  
> “What you hear most often is ‘Oh, we’re going down this process, there goes all of my flexibility. I have no capability to do anything.’ I would strongly disagree with that. I think it’s really being disciplined enough to get that flexibility.”

Heise’s reference to the word “discipline” is key in this passage as it provides a good transition to applying value frameworks in governing processes within an organization. Value frameworks need to encompass control points that address value-added metrics in automation and also support process optimization.
The discipline behind achieving and maintaining process optimization is the same discipline needed in ongoing value governance. To the point made earlier, measuring value in continuum is essential in providing a true sense of value over time. Value judgments over a short period of time eclipse several factors that negate or sustain perceived value assessments for IT. The Val IT model today provides a flexible framework for ongoing value governance.

The Val IT framework is comprised of three layers: Value Governance (VG), Portfolio Management (PM) and Investment Management (IM). These layers reflect various forms in which investment portfolios effectively support management objectives, thereby sustaining value within the organization. It should be noted that value, at the portfolio level, measures IT investments in aggregate. This is done to facilitate reporting efforts, as case-by-case reporting would inevitably confuse and numb the audience for these efforts.

Before diving into value governance, it is worth emphasizing again that value governance plays the pivotal role in both practice and theory (via the Val IT framework). The IT governance team, one of potentially many governance groups within an organization, will need to get executive endorsement of its efforts for governing value across IT investments. Executive support begins with visible executive sponsorship of the IT governance group as a respected enabler and overseer to IT investments. With this sponsorship, the governance team can strategically begin to apply value governance practices with greater collaboration. At this point of the framework, the governance group is working independently to achieve the items listed in figure 2.

The processes associated with VG are also layered in a hierarchy that flows downward. Establishing the framework and its supporting processes surrounding governance, monitoring, and establishing controls will take time, awareness and education. Regardless of executive sponsorship, if a strategic and clearly devised framework is not present, adoption and subsequent use of any value governance strategy will lose luster among its business audience. In essence, this layer of the Val IT model reflects the formation of strategy, policies, roles and processes to be followed in continuous value measurement.

Forming the foundation of any process around measurement is always difficult, yet rewarding. Roughly 25 percent higher profits can be experienced by firms with superior IT governance practices. Additional information reveals that these top-rated institutions were able to develop customized governance programs that looked inward for strategic direction, developing business objectives and identifying metrics for measurement.

Portfolio Management

The goals associated with portfolio management are best defined by the IT Governance Institute (ITGI), as shown below:

*The goal of portfolio management is to ensure that an organization’s overall portfolio of IT-enabled investments is aligned with and contributing optimal value to the organization’s strategic objectives.*

In support of this goal, it is important to sustain the processes that are related to managing portfolios of IT investments (figure 3).

**Value Governance**

Value governance has primarily been discussed thus far outside of a framework. To correlate its efforts to the Val IT framework, one can look at the following components that are defined within the first and most important layer of the Val IT framework.

<table>
<thead>
<tr>
<th>Figure 2—Value Governance in Val IT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Governance (VG)</td>
</tr>
<tr>
<td>Establishing the governance, monitoring and control framework</td>
</tr>
<tr>
<td>Providing strategic direction for the investments</td>
</tr>
<tr>
<td>Defining the investment portfolio characteristics</td>
</tr>
</tbody>
</table>

**PM organizes IT investments into groups of individual investment programs. PM represents the manner in which IT investments are collectively organized from projects to programs under one portfolio. This form of organization is**
brilliant as it provides the whole picture when governance officials begin to assess value for IT investments. However, as with VG, there are critical success factors that should be obtained to ensure accuracy of what is presented to the governance board. Before understanding what these are, refer to figure 4, as a representation of what IT portfolios, programs and projects reflect within the Val IT model.

Program knowledge and project management expertise are essential components of portfolio management and investment management (IM), as will be discussed later in this article. The first key point relates to VG at the project level. Since projects (pertaining to a program and, in turn, the portfolio) do not receive the needed governance oversight, project managers would need to be well versed in the principals of VG in order to act locally within their respective projects and help navigate actions such as acquiring services, assets and/or resources in conformance to VG principle. In essence, this simply translates to additional business requirements during the systems development life cycle (SDLC) process for the project. By acting in this manner, the project manager is better equipped to convey VG principle from within the project and potentially reduce wasteful spending. As part of project management efforts, the following variables can be communicated vertically to the program level:

- Budgetary shortfalls
- Resource restraints
- Unexpected costs
- Change in business processes
- Project scope changes
- Inability to comply with defined requirements
- Overall project delays/extended project timelines

The second essential component to PM is program management. These workflows may be formally realized by either the project management office (PMO) or a program management group overseeing a multitude of interrelated projects. This process is integral to PM in that it is able to provide a 10,000-foot view of projects, services, processes, asset acquisitions and more. A collection of programs equates to the units of measure within PM in Val IT. Effective program management provides the ability to group projects based upon a common criterion. PM reviews a collection of programs, which encompasses a collection of IT projects. If these portfolios are not grouped according to some common criteria, value assessments at the portfolio level will include investments that should not have been grouped together. A recommended practice would be to build a portfolio of IT programs/projects by business function. In doing so, value can be measured against both general IT objectives and the business objectives for that business unit.

Investment Management
This layer of the Val IT model translates to effective money management. The seven functions defined in figure 5 extend value efforts focused on money management. This is further reflected in the IM goal, as defined by ITGI:

The goal of investment management is to ensure that an organization’s individual IT-enabled investment programs deliver optimal value at an affordable cost with a known and acceptable level of risk.

In support of this goal are the seven guiding factors for achieving effective IM for IT investment programs.
Amid the seven functions listed in figure 5, the most critical for ongoing value management are the last two: managing the program, and monitoring and reporting program performance. It should be stated that these are the most important related to ongoing value management. Identifying business requirements is extremely important in that it justifies and correlates the IT investment to a business objective. However, a large part of business requirements, defined at this stage, should already have been inspired by efforts in the VG domain.

Processes across governance, portfolio and investment management are tied across multiple points at the project and program level. Therefore, simply measuring cost factors for internal processes that support a specific project would produce inaccurate results as those processes sustain investments in other portfolios as well and would then be accounted for during multiple intervals. Instead, applying investment assessments should be limited to the program level as the highest point within the investment portfolio. ITGI also supports these points within the Val IT model.

Figure 6 shows the Val IT processes that relate to management processes, as well as where project-related functions specific to project costs are relevant. Cost management at the project level is manageable at the IM layer of the model. Aggregation of costs at all levels of the IT program is tracked in relation to the following key questions (known as the Four Ares):

- Are we doing the right things?—Identifies gaps in strategy to negate further wasteful spending on nonsupportive value governance initiatives
- Are we doing them the right way?—Are standards being adhered to? Are we deviating from technological core competencies? What cost factors are associated with methods that deviate from internally defined standards by governance groups?
- Are we getting the benefits?—Ongoing reporting measures against IT program initiatives funnel up to the portfolio level for reporting
- Are we getting them done well?—Are the expected results within the expected time frame? If not, have they introduced additional costs in services, asset acquisitions, licensing, etc.?

Missing from figure 6 are the many interrelationships among the PM and IM layers. The back and forth among Val IT components (e.g., IM6 and PM5 within the Val IT model) allows for continuous refinement of value assessments in relation to value governance objectives, standards, investment criteria, financial return metrics and projected time estimates. As part of this effort, Responsible, Accountable, Consulted and Informed (RACI) exercises at the VG layer would be able to define which organization resources ultimately are responsible, accountable, consulted or informed in the value measurement or reporting processes.

<table>
<thead>
<tr>
<th>Figure 6—Interrelationships Throughout Val IT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value Governance (VG)</strong></td>
</tr>
<tr>
<td>Establish informed and committed leadership.</td>
</tr>
<tr>
<td>Align and integrate value management with enterprise financial planning.</td>
</tr>
<tr>
<td>Define and implement processes.</td>
</tr>
<tr>
<td>Establish effective governance monitoring.</td>
</tr>
<tr>
<td>Continuously improve value management practices.</td>
</tr>
</tbody>
</table>

| **Portfolio Management (PM)**                 |
| Establish strategic direction and target investment mix. |
| Evaluate and select programmes to fund.        |
| Determine the availability and sources of funds. |
| Manage the availability of human resources.    |
| Monitor and report on investment portfolio performance. |
| Optimise investment portfolio performance.     |

| **Investment Management (IM)**                |
| Develop and evaluate the initial programme business case. |
| Understand the candidate programme and implementation options. |
| Develop the detailed candidate programme business case.  |
| Develop the programme plan.                    |
| Launch and manage the programme.               |
| Develop full life cycle costs and benefits.    |
| Update operational IT portfolios.              |
| Monitor and report on the programme.           |
| Retire the programme.                          |

Source: ITGI, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, 2008, figure 9
VALUE DELIVERY: DEFYING THE SKEPTICS

Attributed to a Fortune 500 CIO: “The board governance fad is being kept alive by a bunch of consultants and academics ... there is no evidence that board governance matters to shareholders. When I see some evidence, I’ll take this more seriously.”

The above quote reveals one of many sentiments by business leaders who shared their thoughts in a survey conducted by McKinsey and Institutional Investor Inc., in the mid-1990s. More than 10 years later, these sentiments are still lingering in the minds of many executives. Contrary to rhetoric from skeptics, resource-deprived departments or late adopters to process efficiency, IT value management is not a fad or newly devised ploy by IT consultants. In fact, demand for a greater understanding of managing value in IT has increased substantially, given the many difficulties in measuring it. This can be inferred by one of the most recent global surveys conducted by PricewaterhouseCoopers (commissioned by ITGI), where only 60 percent of roughly 750 respondents believed that IT provided substantial value to the business. This sharply drops to 30 percent of respondents who believed that IT provided only “some value.” While these results can be looked at in multiple ways, one thing is clear: most of the respondents did not feel confident about the level of value that IT brings to the business. Reverting back to this article’s opening statements and many of the points made herein, value management requires an ongoing effort of monitoring and reporting, and needs to be built upon a disciplined foundation of governance that is omnipresent throughout the organization.

Val IT provides a flexible framework in which its various layers do not require a separate set of resources for the framework to flourish. The components of Val IT are made so that existing organizational resources can become embedded within the various functions defined by the framework. A cross-section of executives, program managers, project managers, project leads, business analysts and financial analysts can all take part in sustaining the framework’s processes. As with anything else, the development of a robust Val IT framework within an organization adheres to a maturity life cycle of process. At its inception, a comprehensive understanding and application may not result in clear value reporting methods. However, a developing program is sure to find itself ahead of the curve by understanding which investments provide value to the enterprise.

ENDNOTES

1 Weill, Peter; Jeanne W. Ross; “How Effective is Your IT Governance?” Center for Information Systems Research, MIT Sloan Management, vol. V, no. 1B, March 2005
3 Collection efficiency is the ratio of debt collected to total debt outstanding for an account over a specific period of time.
4 Days sales outstanding expresses the average time, in days, it takes a company to convert its account receivables into cash.
5 Glassmeyer/McNamee Center for Digital Strategies, “Leveraging the Enterprise Through Process Transformation,” Tuck School of Business at Dartmouth, 2005
6 Weill, Peter; Jeanne W. Ross; IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business Publishing, May 2004
7 IT Governance Institute, Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, 2008, www.itgi.org
8 UcedaVelez, Tony; “What’s the Return on Your Security Investment?,“ Journal of Corporate Accounting & Finance, Wiley Periodicals Inc.
9 Op cit, Thorp
10 Felton, Robert F.: Alec Hudnut; Jennifer Van Heeckeren; “Putting a Value on Board Governance,” The McKinsey Quarterly
Prepare for the **2009 CISA Exams**

**ORDER NOW**—2009 CISA® Review Materials for Exam Preparation and Professional Development

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

---

**CISA Review Manual 2009**

ISACA

The CISA® Review Manual 2009 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 information systems (IS) auditors and the knowledge required to plan, manage and perform IS audits. The Study Guides edition also features new content based on the IT Assurance Framework™ (ITAFTM), recently published by ISACA. ITAF is a comprehensive assurance model that incorporates standards and good practices, providing guidance on the design, conduct and reporting of IT audit and assurance assignments; defines terms and concepts specific to IT assurance; and establishes standards that address IT audit and assurance professional roles and responsibilities, knowledge and skills, diligence, conduct, and reporting requirements. The CISA Review Manual 2009 also includes brief chapter summaries focused on the main topics and new case studies to assist a candidate in understanding 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. 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 2009 edition has been developed and is organized to help prepare the CISA candidate in understanding the essential concepts and studying the following job practice areas:

- IS audit process
- IT governance
- Systems and infrastructure life cycle management
- IT service delivery and support
- Protection of information assets
- Business continuity and disaster recovery

**CRM-9** English Edition
**CRM-9F** French Edition
**CRM-9I** Italian Edition
**CRM-9J** Japanese Edition
**CRM-9S** Spanish Edition

---


ISACA

Developed each year, the CISA® Review Questions, Answers & Explanations Manual 2009 Supplement and 2008 Supplement are recommended for use when preparing for the 2009 CISA exam. Each edition consists of 100 sample questions, answers and explanations based on the current CISA job practice areas, using a process for item development similar to the process for developing actual exam items. The questions are intended to provide the CISA candidate with an understanding of the type and structure of questions that have typically appeared on past exams, and were prepared specifically for use in studying for the CISA exam.

**2009 Editions**
- QAE-9ES English Edition
- QAE-9FS French Edition
- QAE-9IS Italian Edition
- QAE-9JS Japanese Edition
- QAE-9PS Polish Edition
- QAE-9SS Spanish Edition

**2008 Editions**
- QAE-9ES English Edition
- QAE-8FS French Edition
- QAE-8IS Italian Edition
- QAE-8JS Japanese Edition
- QAE-8PS Polish Edition
- QAE-8SS Spanish Edition

---

**CISA Practice Question Database v9**

ISACA

The CISA® Practice Question Database v9 combines the CISA Review Questions, Answers & Explanations Manual 2008 with the CISA Review Questions, Answers & Explanations Manual 2008 Supplement and 2009 Supplement into one comprehensive 800-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 ISACA® Journal, formerly Information Systems Control Journal, articles referenced in the CISA Review Manual 2009. 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 80 MB of available space
- CD-ROM drive
- Display with recommended resolution of 1024 x 768

**CDB-9** English Edition—CD-ROM
**CDB-9W** English Edition—Web site download
**CDB-9S** Spanish Edition—CD-ROM
**CDB-9SW** Spanish Edition—Web site download

---

**CISA Online Review Course**

ISACA

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

To order CISA review materials for the June/December 2009 exams, see the order form on page S-8 in this Journal or visit www.isaca.org/cisabooks.
The Hidden Values of IT Risk Management

Risk management is not a new activity for many organizations. This is true because risk, by definition, presents a threat to value and, therefore, it is in the best interest of an organization to manage it. The processes for lowering loss exposures to acceptable levels is something well understood across many industries and fields, most notably in financial risk management for banking and insurance companies.

Despite the recognition and maturity of risk management at an enterprise level, the principles and methodologies of IT-specific risk management are much newer and have led to the birth of new models for operational risk mappings. Until recently, the complexities of the decisions that were required to be made and implemented within the IT domain tended to insulate it from the same level of business alignment routinely expected from other business units and from the other elements of the risk management family.

However, due in part to increasing regulatory expectations and requirements that, in turn, have resulted from an ever-increasing dependence on IT and exposure to IT-specific risk for critical business functions, the discipline has taken on new importance and prominence within the management portfolio of many organizations' governance, risk and compliance (GRC) and security functions.

The security aspect is included, since “risk management provides the rationale and justification for virtually all information security initiatives.” In essence, information security as a knowledge domain and specialization exists primarily to manage risks to information and IT resources. Risk is, in fact, the proximate cause of IT security. The recognition and convergence between traditional risk management methodologies and IT security-based risk are increasing due to the potential for financial efficiency gains that may be realized from better prioritized remediation efforts and from the potential for well-informed risk decision making.

**STANDARDS AND FRAMEWORKS**

ISACA and the IT Governance Institute (ITGI) are currently developing Risk IT, an IT enterprise risk management (ERM) framework that should significantly assist management as well as auditors in the work of control assessment and remediation identification. This new framework aims “to fill the gap between generic risk management frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO)’s *Enterprise Risk Management—Integrated Framework* (ERM) and Australia/New Zealand AS/NZ 4360, and detailed (mostly security-related) IT risk management frameworks.”

Risk IT is being developed to address all levels of IT risk, from the strategic to operational levels.

The US National Institute of Standards and Technology (NIST) defines IT risk management as “the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT environment.”

**STANDARDS AND FRAMEWORKS**

Timothy Abram, CISA, CGEIT, CISSP, MCSE:Security, MCSA, Security+, has 14 years of security experience and has been involved with the design, audit and control remediation work for companies of all sizes. He has seen a range of security postures, working to secure both a smaller technology company and the Western Canadian division of a large retail corporation with more than 1,000 locations and more than CAD $13 billion in sales.
structured and organized identification, analysis, evaluation and deployment, followed by an effective remediation and monitoring program.

**ENTERPRISE RISK MANAGEMENT**

IT risk management is one component of broader ERM. ERM is an approach to managing key business risks and opportunities to maximize shareholder value. Within the scope of IT, risk management tends to focus on pure risk or what is often referred to as “hazard risk”—the kind of loss exposure that comes into existence as a result of the threat of accidental loss to technology assets.

The number and variety of risks that affect or are a direct result of IT activities are extensive and cover a wide range of risk sources. The risks can be organized into categories and together the full list helps to describe the risk profile of the organization.

Although no risk model can offer a complete picture, tables and classifications can help provide focus on key risks and facilitate completeness. Symantec, for example, categorizes IT risk elements into four groupings: security risk, availability risk, performance risk and compliance risk, as shown in figure 1.

However, it is possible to use the more generic confidentiality, integrity and availability classifications as well, since all IT risk can ultimately be distilled into those core constituents.

**GOALS OF IT RISK MANAGEMENT**

The primary intent of any risk management exercise is to, first, reduce the cost of risk related to an organization's activities and, second, to reduce negative impacts related to the uncertainty of outcomes. Put another way by NIST, “minimizing negative impact on an organization and the need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems.” These two purposes have measurable return on investment and deliver value on many levels, including:

- Ensuring optimal allocation of resources within an organization
- At the highest level, making the organization a safer investment and thereby commanding a correspondingly higher shareholder value

**Preloss Objectives**

Prior to any losses, the goal of a risk management program is to ensure an economy of operations. That is to say, the cost of controls (and the risk program itself) should not exceed the total potential savings. This is achieved through the application of prudent and appropriate controls where cost and benefit are favorable or intersect. In addition, a preloss goal is to deliver “tolerable uncertainty,” which means providing assurance about the scope of what is possible and how each potential outcome may be treated. By understanding the full breadth of risk possibilities and depth of impact, suitable decisions to reduce or even add risk can be made.

The preloss goal of providing legality is also an important component of the risk program as it relates not only to “duty of care” tort liability, but also to administrative laws and regulations related to technology, including the US Sarbanes-Oxley Act, Japan’s J-SOX, Payment Card Industry (PCI) Data Security Standards (DSS), the US Health Insurance Portability and Accountability Act (HIPAA), and Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) and Bill 198 (also known as the “Canadian Sarbanes-Oxley” Act).

**Postloss Objectives**

After a loss, the goal of risk management is to ensure survival, followed by, and closely related to, continuity of operations. This objective includes technical and business elements that combine to ensure...
that critical functions can continue to operate under a variety of loss scenarios.

The risk management program provides a method for planning, organizing, leading and allocating resources to mitigate the effects of accidental loss. In brief, risk management is part of the due diligence owed by a public company or agency to its shareholders.

So, at an organizational level, risk management is a governance dimension, and, therefore, support for risk management principles and processes is a clear demonstration of management’s care, as illustrated in figure 2.

Setting an effective strategic “tone at the top” helps ensure that risk management is “baked into” the organization and considered a part of every manager’s job—not an afterthought with output distributed in silos across myriad business units. The trickle down to IT operational management is a duty to help ensure that the types of controls, the cost of controls and the implementation of them are all appropriate for the resources or information that is being managed.

**TYPES OF ENTERPRISE IT RISK**

Financial risk management professionals like to group loss exposures into four kinds: property, liability, personnel and net income loss. For IT professionals, the spotlight tends to shine most brightly on the first kind of exposure, property—an exposure that establishes the possibility that an organization will sustain loss as a result of destruction, theft or loss of use. Translated into technology terms of reference, this would be the threat to confidentiality, integrity and/or availability within the application, information infrastructure and people resource pools.

Liability exposure is the potential loss resulting from a claim that an organization’s failure to the duty of care owed resulted in property damage or bodily injury to another party. In an increasingly regulated environment, the demands of due diligence have elevated the need for effective and demonstrable risk management processes, including those involving IT.

The threat of personnel loss is the risk to an organization that results from the death, disability, retirement or resignation of an individual that deprives the organization of specialized skill or knowledge that cannot easily be replaced. This risk can be a factor for IT because of the number of permutations and combinations of complex technology in each organization, and a resulting need for specialized skill sets to support specific infrastructure and applications.

**RISK ASSESSMENT**

The primary tools of an IT risk manager are risk assessment and analysis. This is because it is only through a thorough assessment process that a complete picture of IT risk can be drawn. Once this is complete, it can then provide the organization with the necessary information to make appropriate, properly prioritized and cost-effective risk management technique selections.

Of course, any successful risk assessment relies heavily on the completeness of the threat list. Compiling a complete list can be challenging and is commonly known as the problem of

---

**Figure 2—IT Governance Institute’s IT Governance Focus Areas**

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise’s appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

Source: ITGI, CoIT 4.1, 2007, figure 2
the “unknown unknowns.” Since we do not know about what we do not know yet, experience and analysis become valuable assets during this stage of risk management. In many cases, using expertise beyond the boundaries of the organization can provide additional benefits as a result of objectivity and potentially broader exposure experience.

**RISK MATRIX**

A risk matrix focuses on the dimensions of loss frequency and loss severity. Sometimes these are called likelihood and impact, respectively. The subjective, or qualitative, approach to this relationship is well understood in the risk management profession and is illustrated in the Prouty approach shown in figure 3.

![Figure 3—Illustration of a Frequency and Loss Exposure Prouty Matrix](image)


While these dimensions help direct the kind of control that is appropriate, to assign priority, the existence of a threat source, an attack vector or a vulnerability must be considered. If any of these factors is nonexistent, the risk is effectively reduced to zero, no matter how severe the impact might be. This is intuitively obvious, since a threat does not exist if there is no vulnerability to be exploited and/or no attack vector or source from which it can originate. The multiplicative properties of this relationship lend themselves to calculating IT risk by multiplying the values together to derive the IT risk factor.

That value can be used to calculate a relative loss exposure, and, by multiplying the factor by asset value, it is possible to attach a monetary value to each risk. This equation is often quoted in IT reference sources. “With few exceptions, whether related to financial, physical or technological resources, different types of risk can be calculated using the same universal formula. Risk can be defined by the following calculation: Risk = asset value X threat X vulnerability.”10

These values can be prioritized against each other and used along with the exposure elements in the frequency and severity matrix to guide potential responses. This prioritization and response category is a valuable resource, as it allows the organization to make remediation investments in the most cost-effective way possible. It also may identify risks that the organization can safely assume without the need for remediation.

**THE VALUE OF RISK MANAGEMENT CONTROLS**

To drive value from risk management, it is critical that a management program extend past simply assessing and analyzing, but also follow through with implementation and remediation plans to lower the risk profile for the organization. “Risk and control are virtually inseparable—like two sides of a coin—meaning that risks first must be identified and assessed and then managed and mitigated.”11

There are a number of accepted risk control techniques that can be used, including concepts such as avoidance, prevention and reduction.

Prevention addresses the frequency of occurrence, whereas reduction addresses the severity of a particular loss. As well as control techniques, risk financing techniques that include insurance, transfer and retention can be utilized. Any risk that is not controlled, avoided or financed must be retained. Acceptable retention levels are subject to the risk appetite of the organization and should be formally derived and approved. Sometimes retention can be the most economic risk financing available. In all cases, it is the technique of last resort—the final option for loss exposures that simply cannot be insured or transferred. Risk that is retained is sometimes called “residual risk,” and when it is accepted, it is considered to have been “assumed.”

**RISK MANAGEMENT PROGRAM**

As with other management programs, such as quality’s plan-do-check-act (PDCA)/Deming cycle of continual improvement, it is expected that the risk management program be monitored and revised through a process feedback loop. IT risk must be routinely evaluated as a result of the changing threat, vulnerability and exposure landscape.
In this way, the program can adequately respond to new loss potential that could have evolved or been added since the last review. It also allows for the reevaluation of mitigation strategies to determine if new controls or countermeasures may have become more desirable than those previously implemented, thereby improving business efficiencies while still controlling risk exposure. This is an often overlooked business efficiency gain resulting from a cyclical, program-based approach to IT risk management.

**CONCLUSION**

No organization could ever eliminate all risk and remain viable. That is a simple fact of business life. By their very nature, some risks must be lived with, and this is perfectly acceptable, especially as the likelihood/frequency and impact of a risk become smaller and smaller. The value in risk management comes from having the knowledge about those occurrence factors and the resulting impact. With that knowledge, it is possible to prioritize and control risk efficiently and effectively. However, without such knowledge, only reaction and uncertainty would result.

IT risk management is one facet of ERM that is concerned with protecting an organization’s information assets and systems. Risk management in its broadest sense is a cornerstone of overall corporate governance, since it ultimately helps drive shareholder value by providing investors assurance about the risks to their money. Therefore, IT risk management should be considered a program, rather than a periodic project focused on IT security controls. As a program, IT risk management may consider, on a continuous basis, the full range of risk responses and can include the ability to take on additional risk for higher returns as a result of risk-aware decision making.

While driving value from nonrevenue-generating activities can be a challenge, in the case of IT risk management, the hidden values will be uncovered as a result of a well-implemented program.

**REFERENCES**


**ENDNOTES**

2 For more information on the Risk IT framework, please see www.isaca.org
7 *Op cit*, NIST, p. 4
8 Baranoff, E.; S. Harrington; G. Niehaus; “Risk Assessment,” AICPCU/IIA, 2005
9 Davis, Chris; Mike Schiller; Kevin Wheeler; *IT Auditing. Using Controls to Protect Information Assets*, McGraw-Hill, 2007, p. 351
I have read one of your previous columns on incident management. How do you differentiate a ‘problem’ from an ‘incident’? Can we consider an incident and a problem to be synonymous? If not, can you please explain and shed some light on what the term ‘problem management’ means with reference to controls?

Though there are some instances where we can see the problem management process get triggered proactively, the key aim of problem management is to minimise or reduce the negative impact of events/incidents caused by human/mechanical errors within the IT infrastructure and at the same time prevent their future recurrence.

The key aim of the incident management process is to restore normalcy as soon as possible after the incident, mainly through workarounds or by utilizing secondary options. The aim is not to have an immediate permanent solution in place without doing proper homework. Problem management, on the other hand, aims to identify the root cause behind one or more incidents (should a trend be identified) and work towards a permanent solution to the problem, where feasible.

Let us discuss some basic principles.

I wish to take the liberty of extensively quoting from some of the IT Infrastructure Library (ITIL) standards on problem management.

The problem management process is intended to reduce both the number and severity of incidents and problems on the business. Therefore, part of problem management’s responsibility is to ensure that the previous information is documented in such a way that it is available to both the first-line and the second-line staff. This is not simply a matter of producing documentation. What is required includes:

- The information to be indexed so that it is easily referenced by simple and detectable triggers from new incidents;
- Regular inspection to ensure the continued relevance of documentation in the light of changing:
  - Technology
  - Available external solutions
  - Business practices and requirements
  - In-house skills
  - Frequency and impact of recurring incidents
  - Interpretation of internal best practice
- That the process must be subject to a detailed review;
- Staff using the information to be trained to understand the depth and power of the information available, how to access and interpret it, and their role in providing feedback on its relevance and ease of use;
- A suitable repository for the information—typically based on an integrated service management tool which can capture it at logging or first-analysis stage of the incident handling process.

Problems and known errors can be identified by:

- Analyzing incidents as they occur (reactive problem management)
- Analyzing incidents over differing time periods (proactive problem management)
- Analyzing the IT infrastructure
- The provision of a knowledge database
- Developers/vendors when new products are introduced.
A ‘problem’ is a condition often identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant.

A ‘known error’ is a condition identified by successful diagnosis of the root cause of a problem and the subsequent development of a ‘workaround’.

Problem control focuses on transforming problems into known errors.

Whenever the root cause for the reported incidents has been identified and a decision has been made to resolve it, the change management process will be triggered to implement the desired resolution. However, information such as the proposed workarounds or work-in-progress status of the resolution and details of proposed permanent fixes, if any, must be communicated to the relevant stakeholders.

The previous quote contains some of the theoretical principles as provided by ITIL. However, from a practical point of view, here are my tips:

1. A mature problem management process will have a built-in tracking system to list and track all problems until their closures.
2. Not all known errors need resolution. Sometimes, the cost of resolution may be too prohibitive and it may make more economic sense to live with the workarounds. However, the local management must be aware of the scenario and the details of the costs vis-à-vis benefits analysis work undertaken.
3. Similar to the classification of incidents, the problems must be classified. They can be classified using a number of factors such as, but not limited to, impact, urgency and priority. It is important to note that urgency and priority are two different items. Urgency indicates the extent to which the resolution of the problem can bear a delay, whereas priority indicates the relative order in which the problems can be addressed in terms of closure.

4. Management must ensure that relevant tools and diagnostic aids are made available to the problem management staff in order for them to do their job effectively.
5. Many times, the diagnosis of the problem can be related to the non-existence of a control or, in some extreme scenarios, an excessive control may be the culprit.
6. The problem management function that proactively identifies trends and potential problem sources with an aim to work towards the resolution of such problems will always be seen as a better value creator than someone doing some post-mortem work. That said, there are some problems that can be addressed in a reactive manner only.
7. On many occasions, the audit work done either by the internal auditors or those from external entities may uncover something that can indicate the existence of a potential problem. The problem management group must be made privy to such audit reports so that the root causes of many of the symptomatic issues can be identified and closed.
8. There is no point in aiming to have a strong problem management process when the related supporting processes, such as incident management, change management, release management and configuration management, remain weak. In particular, it is essential to have a structured change management approach to identify the problem and resolve it permanently.
9. Metrics should be used to measure the effectiveness and efficiency of the problem management processes and controls.
10. Creating awareness of all the above is key; without awareness, all the controls and processes will simply remain theory and not be placed into practice.

The ITIL publications and the international standard on Service Management, namely ISO 20000, are good resources that will be useful to bring a further understanding to this topic.
Quiz #123
Based on volume 6, 2008, Emerging Issues
Value: 1 hour of CISA/CISM/CGEIT continuing professional education (CPE) credit

TRUE OR FALSE

AXELROD ARTICLE
1. Traditional security metrics gauge the functionality and efficiency of preventive security measures, frequently leading to appropriate security decisions.
2. Metrics report how well policies, processes and controls are functioning, and whether or not desired performance outcomes are being achieved.
3. Functionality testing is designed to ensure that applications do what they are supposed to do, whereas the purpose of security testing is to check that applications do not do what they are not supposed to do.
4. The advantage of using “Score” as a metric is that this type of measure can provide high precision by tallying and averaging and, thus, obtaining a long decimal extension, which is a measure of precision.
5. Although measurability and usefulness are in contention when it comes to security metrics, readily available metrics can be used, if they are used with an appropriate level of thoughtfulness and understanding.

SATHIYAMURTHY ARTICLE
6. The conventional approach to managing IT risks requires a paradigm shift from vague decision-making techniques to a data-driven pragmatic approach.
7. In the case of threats associated with historical events, the calculation of the cost at risk requires expert judgment in close liaison with other key elements, such as the service impacted and service commitments.
8. The risk prioritization exercise aids the business in controlling the analyzed risks through risk treatment plans that are based on the organization’s risk acceptance level.
9. The value-driven approach will eventually improve an organization’s capability for effectively managing its IT risks and, in turn, complying with fiduciary demands.

HENDERSON ARTICLE
10. More mature systems development practices, as required for CMMI compliance, can facilitate Sarbanes-Oxley compliance.
11. The type of application system being developed does not affect how developers use the methodology.
12. The development of a unique and highly complex system will require the same disciplined process as development of a simple application system.
13. A key benefit of IS auditors participating in the systems development process is that they can ensure that development teams create the appropriate systems documentation when it should be created.

HARE ARTICLE
14. The access the privileged user has to critical foundational setups may leave the user with the ability to change the business process, compromise the defined controls and/or circumvent the company’s change management process.
15. Monitoring of privileged users is done by maintaining an audit trail of all activity for the privileged users, which is built into the design of ERP systems such as Oracle’s eBusiness Suite or SAP.
16. A limitation of enabling the profile option called “Sign-on: Audit Level” is that the Sign-On Audit Forms report merely tells that the form was opened; it does not indicate whether the user solely viewed the data or made changes to the data.
17. The use of logs to monitor transactions entered by privileged users may be a sound technique depending on the types of logs and other capabilities of the privileged users, but they have system performance risk.

POON ARTICLE
18. Although testing after software development is a primary means to detect software failures and to prevent faults from propagating through to the final production system, it may not always be cost-effective.
19. In the black box approach, test cases are generated according to information derived from the specification document without requiring the knowledge of how the programs are written.
20. Detection of the occurrence of combinable choices and composite choices is possible when, during the identification of potential categories and potential choices, the constraints among potential choices in the formation of complete test frames and the execution behavior associated with these choices are also considered.
Get noticed...

Advertise in the ISACA® Journal

For more information, contact advertising@isaca.org.

Answers—Crossword by Myles Mellor
See page 29 for the puzzle.

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current Journal subscribers. An electronic version of the quiz is available at www.isaca.org/cpequiz; it is graded online and is available to all interested parties.

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

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

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

A passing score of 75 percent will earn one hour of CISA, CISM or CGEIT CPE credit.
MEMBERSHIP APPLICATION
Join online and save US $20.00
www.isaca.org/join

Please complete both sides
U.S. Federal I.D. No. 23-7067291
www.isaca.org
membership@isaca.org

[ ] MR.  [ ] MS.  [ ] MRS.  [ ] MISS  [ ] OTHER

Name

FIRST

MIDDLE

LAST/FAMILY

Date

MONTH/DAY/YEAR

PRINT NAME AS YOU WANT IT TO APPEAR ON MEMBERSHIP CERTIFICATE

Residence address

STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE/ZIP

Residence phone

Residence facsimile

AREACOUNTRY CODE AND NUMBER

AREACOUNTRY CODE AND NUMBER

Company name

Title

Business address

STREET

CITY

STATE/PROVINCE/COUNTRY

POSTAL CODE/ZIP

Business phone

Business facsimile

AREACOUNTRY CODE AND NUMBER

AREACOUNTRY CODE AND NUMBER

E-mail

Send mail to
[ ] Home  [ ] Business
[ ] Chapter Affiliation
[ ] Chapter Number (see reverse)
[ ] Member at large (no chapter within 50 miles/80 km)
[ ] I do not want to be included on a mailing list, other than that for Association mailings.

How did you hear about ISACA?

1. [ ] Friend/Coworker  6. [ ] Local Chapter
2. [ ] Employer 7. [ ] Certification Programs
3. [ ] Internet Search 8. [ ] Direct Mail
4. [ ] Information Systems 9. [ ] Educational Event
5. [ ] Other Publication

Please note: Membership in the association requires you to belong to a chapter when you live or work within 50 miles/80 km of a chapter territory. The name of the chapter is indicative of its territory. If you live farther than 50 miles/80 km from a chapter territory, select member at large. Chapter selection is subject to verification by ISACA International Headquarters. Cities listed in parentheses are a reference to where the majority of chapter meetings are held. Please contact your local chapter at www.isaca.org/chapters for other meeting locations.

Current field of employment (check one)

1. [ ] Financial/Banking
2. [ ] Insurance
3. [ ] Public Accounting
4. [ ] Transportation
5. [ ] Aerospace
6. [ ] Retail/Wholesale/Distribution
7. [ ] Government/Military—National/State/Local
8. [ ] Technology Services/Consulting
9. [ ] Manufacturing/Engineering
10. [ ] Telecommunications/Communications
11. [ ] Mining/Construction/Petroleum/Agriculture
12. [ ] Utilities
13. [ ] Legal/Law/Real Estate
14. [ ] Health Care/Medical
15. [ ] Pharmaceutical
16. [ ] Advertising/Marketing/Media
17. [ ] Education/Student
99. [ ] Other

Level of education achieved (indicate degree achieved, or number of years of university education if degree not obtained)

1. [ ] One year or less  7. [ ] AS
2. [ ] Two years 8. [ ] BS/BA
3. [ ] Three years 9. [ ] MS/MBA/Masters
4. [ ] Four years 10. [ ] PhD
5. [ ] Five years 99. [ ] Other
6. [ ] Six years or more

Certifications obtained (other than CISA, CISM, CGEIT)

1. [ ] CPA  5. [ ] CC
2. [ ] CA  6. [ ] CAP
3. [ ] CIA  7. [ ] CFE
4. [ ] CISSP 99. [ ] Other

Work experience (check the number of years of information systems related work experience)

1. [ ] No experience 4. [ ] 8-9 years
2. [ ] 1-3 years 5. [ ] 10-13 years
3. [ ] 4-7 years 6. [ ] 14 years or more

Current professional activity (if not your title, please select the BEST match)

1. [ ] CEO, President, Owner, General/Executive Manager
2. [ ] CAE, General Auditor, Partner, Audit Head/VP/EVP
3. [ ] CISO/CSO, Security Executive/VP/EVP
4. [ ] COO/CTO, Info Systems/Technology Executive/VP/EVP
5. [ ] CFO, Controller, Treasurer, Finance Executive/VP/EVP
6. [ ] Chief Compliance/Risk/Privacy Officer, VP, EVP
7. [ ] IT Audit Director/Manager/Consultant
8. [ ] Security Director/Manager/Consultant
9. [ ] IT Director/Manager/Consultant
10. [ ] Compliance/Risk/Privacy Director/Manager/Consultant
11. [ ] IT Senior Auditor (External/Internal)
12. [ ] IT Auditor (External/Internal Staff)
13. [ ] Non-IT Auditor (External/Internal)
14. [ ] Security Staff
15. [ ] IT Staff
16. [ ] Professor/Teacher
17. [ ] Student
99. [ ] Other

Date of Birth

MONTH/DAY/YEAR

Payment due

[ ] Association dues $ 130.00 (US)
[ ] Chapter dues (see reverse) $ (US)
[ ] New member processing fee $ 30.00 (US)*

PLEASE PAY THIS TOTAL $ (US)

* For student membership information please visit www.isaca.org/student

Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2009. No rebate of dues is available upon early resignation of membership.

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).

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.

Method of payment

[ ] Check payable in US dollars, drawn on US bank
[ ] Send invoice (Applications cannot be processed until dues payment is received.)
[ ] MasterCard  [ ] VISA  [ ] American Express  [ ] Diners Club

All payments by credit card will be processed in US dollars

ACCT #

Print name of cardholder

Expiration date

MONTH/YEAR

Signature

Cardholder billing address if different than address provided above:

Send mail to

Home  [ ] Business

for student membership information please visit www.isaca.org/student

Member at large (no chapter within 50 miles/80 km)

I do not want to be included on a mailing list, other than that for Association mailings.

How did you hear about ISACA?

1. [ ] Friend/Coworker  6. [ ] Local Chapter
2. [ ] Employer 7. [ ] Certification Programs
3. [ ] Internet Search 8. [ ] Direct Mail
4. [ ] Information Systems 9. [ ] Educational Event
5. [ ] Other Publication

Please note: Membership in the association requires you to belong to a chapter when you live or work within 50 miles/80 km of a chapter territory. The name of the chapter is indicative of its territory. If you live farther than 50 miles/80 km from a chapter territory, select member at large. Chapter selection is subject to verification by ISACA International Headquarters. Cities listed in parentheses are a reference to where the majority of chapter meetings are held. Please contact your local chapter at www.isaca.org/chapters for other meeting locations.

Current field of employment (check one)

1. [ ] Financial/Banking
2. [ ] Insurance
3. [ ] Public Accounting
4. [ ] Transportation
5. [ ] Aerospace
6. [ ] Retail/Wholesale/Distribution
7. [ ] Government/Military—National/State/Local
8. [ ] Technology Services/Consulting
9. [ ] Manufacturing/Engineering
10. [ ] Telecommunications/Communications
11. [ ] Mining/Construction/Petroleum/Agriculture
12. [ ] Utilities
13. [ ] Legal/Law/Real Estate
14. [ ] Health Care/Medical
15. [ ] Pharmaceutical
16. [ ] Advertising/Marketing/Media
17. [ ] Education/Student
99. [ ] Other

Level of education achieved (indicate degree achieved, or number of years of university education if degree not obtained)

1. [ ] One year or less  7. [ ] AS
2. [ ] Two years 8. [ ] BS/BA
3. [ ] Three years 9. [ ] MS/MBA/Masters
4. [ ] Four years 10. [ ] PhD
5. [ ] Five years 99. [ ] Other
6. [ ] Six years or more

Certifications obtained (other than CISA, CISM, CGEIT)

1. [ ] CPA  5. [ ] CC
2. [ ] CA  6. [ ] CAP
3. [ ] CIA  7. [ ] CFE
4. [ ] CISSP 99. [ ] Other

Work experience (check the number of years of information systems related work experience)

1. [ ] No experience 4. [ ] 8-9 years
2. [ ] 1-3 years 5. [ ] 10-13 years
3. [ ] 4-7 years 6. [ ] 14 years or more

Current professional activity (if not your title, please select the BEST match)

1. [ ] CEO, President, Owner, General/Executive Manager
2. [ ] CAE, General Auditor, Partner, Audit Head/VP/EVP
3. [ ] CISO/CSO, Security Executive/VP/EVP
4. [ ] COO/CTO, Info Systems/Technology Executive/VP/EVP
5. [ ] CFO, Controller, Treasurer, Finance Executive/VP/EVP
6. [ ] Chief Compliance/Risk/Privacy Officer, VP, EVP
7. [ ] IT Audit Director/Manager/Consultant
8. [ ] Security Director/Manager/Consultant
9. [ ] IT Director/Manager/Consultant
10. [ ] Compliance/Risk/Privacy Director/Manager/Consultant
11. [ ] IT Senior Auditor (External/Internal)
12. [ ] IT Auditor (External/Internal Staff)
13. [ ] Non-IT Auditor (External/Internal)
14. [ ] Security Staff
15. [ ] IT Staff
16. [ ] Professor/Teacher
17. [ ] Student
99. [ ] Other

Date of Birth

MONTH/DAY/YEAR

Payment due

[ ] Association dues $ 130.00 (US)
[ ] Chapter dues (see reverse) $ (US)
[ ] New member processing fee $ 30.00 (US)*

PLEASE PAY THIS TOTAL $ (US)

* For student membership information please visit www.isaca.org/student

Full payment entitles new members to membership from the date payment is processed by International Headquarters through 31 December 2009. No rebate of dues is available upon early resignation of membership.

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).

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 7 August 2008 through 31 May 2009.
<table>
<thead>
<tr>
<th>Chapter Name</th>
<th>Chapter Number</th>
<th>Country</th>
<th>Dues</th>
</tr>
</thead>
<tbody>
<tr>
<td>H Kong</td>
<td>64</td>
<td>$60</td>
<td></td>
</tr>
<tr>
<td>Bangalora</td>
<td>138</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Cochín</td>
<td>176</td>
<td>$15</td>
<td></td>
</tr>
<tr>
<td>Coibemtoro</td>
<td>152</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Hyderabad</td>
<td>164</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Kolkata</td>
<td>156</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Chennai</td>
<td>99</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>Mumbai</td>
<td>145</td>
<td>$35</td>
<td></td>
</tr>
<tr>
<td>New Delhi</td>
<td>140</td>
<td>$15</td>
<td></td>
</tr>
<tr>
<td>Pune</td>
<td>159</td>
<td>$17</td>
<td></td>
</tr>
<tr>
<td>Vijawada</td>
<td>200</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Indonesia</td>
<td>181</td>
<td>$35</td>
<td></td>
</tr>
<tr>
<td>Osaka</td>
<td>103</td>
<td>$85</td>
<td></td>
</tr>
<tr>
<td>Tokyo</td>
<td>89</td>
<td>$80</td>
<td></td>
</tr>
<tr>
<td>Korea</td>
<td>107</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Lebanon</td>
<td>181</td>
<td>$35</td>
<td></td>
</tr>
<tr>
<td>Macao</td>
<td>98</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td>93</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>Muscat, Oman</td>
<td>168</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Karachi, Pak</td>
<td>148</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Lahore, Pak</td>
<td>196</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>Manila, Phil</td>
<td>136</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Jeddah, Ar</td>
<td>163</td>
<td>$70</td>
<td></td>
</tr>
<tr>
<td>Riyad, Ar</td>
<td>154</td>
<td>$0</td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td>70</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>Sri Lanka</td>
<td>141</td>
<td>$15</td>
<td></td>
</tr>
<tr>
<td>Taiwan</td>
<td>142</td>
<td>$50</td>
<td></td>
</tr>
<tr>
<td>Bangkok, Tha</td>
<td>109</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>UAE</td>
<td>150</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>CENTRAL/SOUTH AMERICA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buenos Aires, Arg</td>
<td>124</td>
<td>$25</td>
<td></td>
</tr>
<tr>
<td>Mendoza, Arg</td>
<td>144</td>
<td>$25</td>
<td></td>
</tr>
<tr>
<td>LaPaz, Bolivia</td>
<td>173</td>
<td>$25</td>
<td></td>
</tr>
<tr>
<td>Brasilia, Bz</td>
<td>202</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>Rio de Janeiro, Bz</td>
<td>203</td>
<td>$10</td>
<td></td>
</tr>
<tr>
<td>São Paulo, Bz</td>
<td>166</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>Santiago, Chl</td>
<td>135</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Bogotá, Colomb</td>
<td>126</td>
<td>$25</td>
<td></td>
</tr>
<tr>
<td>San José, Costa Rica</td>
<td>31</td>
<td>$33</td>
<td></td>
</tr>
<tr>
<td>Quito, Ec</td>
<td>179</td>
<td>$15</td>
<td></td>
</tr>
<tr>
<td>Guadalajara, Mex</td>
<td>201</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Mérida, Yucatán, Mex</td>
<td>101</td>
<td>$50</td>
<td></td>
</tr>
<tr>
<td>Mexico City, Mx</td>
<td>14</td>
<td>$65</td>
<td></td>
</tr>
<tr>
<td>Monterrey, Mex</td>
<td>80</td>
<td>$50</td>
<td></td>
</tr>
<tr>
<td>Panamá</td>
<td>94</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>Asunción, Paraguay</td>
<td>184</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Lima, Perú</td>
<td>146</td>
<td>$15</td>
<td></td>
</tr>
<tr>
<td>Puerto Rico, Pr</td>
<td>86</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Montevideo, Urug</td>
<td>133</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>Venezuela</td>
<td>113</td>
<td>$20</td>
<td></td>
</tr>
<tr>
<td>EUROPE/AFRICA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td>157</td>
<td>$45</td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td>143</td>
<td>$70</td>
<td></td>
</tr>
<tr>
<td>Sofia, Bulg</td>
<td>189</td>
<td>$40</td>
<td></td>
</tr>
<tr>
<td>Croatia</td>
<td>170</td>
<td>$50</td>
<td></td>
</tr>
<tr>
<td>Czech Republic</td>
<td>153</td>
<td>$130</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>96</td>
<td>$50</td>
<td></td>
</tr>
<tr>
<td>Estonia</td>
<td>162</td>
<td>$30</td>
<td></td>
</tr>
<tr>
<td>Finlan</td>
<td>115</td>
<td>$15</td>
<td></td>
</tr>
<tr>
<td>France (Paris)</td>
<td>75</td>
<td>$140</td>
<td></td>
</tr>
</tbody>
</table>

**Call chapter for information**

**US dollar amounts listed below are for local chapter dues. While correct at the time of printing, chapter dues are subject to change without notice. Please include the appropriate chapter dues amount with your remittance.**

For current chapter dues, or if the amount is not listed below, please visit the web site, www.isaca.org/chapdues, or contact your local chapter at www.isaca.org/chapters.
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 prefer IT Audit experience.

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

CLIENTS: Large companies in most 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 IT Audit experience is 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 (Microsoft Word formatted)
   Fax: 415-921-5309 Attn.: Don May, Managing Director
   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.