Governance and Management of Enterprise IT (GEIT)

Featured articles:

Governance Implementation—COBIT 5 and ISO

IT Policy Framework Based on COBIT 5

Creating the Business Case for ERP System Acquisitions Using GEIT

And more...
I am building for my Future

UPCOMING EXAM DATE
8 JUNE 2013

FINAL REGISTRATION DEADLINE: 12 April 2013

For more information and to register for an ISACA exam, visit isaca.org/myfuture-journal1.
Register by 13 February 2013 and save US $50!
New York Times IT journalist David Pogue wants to have a few words with you in Dallas.

Make plans today to attend North America CACS 2013 featuring world-class networking, customized learning opportunities and special guest speaker David Pogue.

15-17 April 2013

Stay on top of the trends and opportunities of the dynamic technology industry at North America CACS 2013 in Dallas, Texas—the world’s leading audit conference for IT audit, security, governance and risk professionals.

In addition to earning up to 38 CPE hours, you will:

- Be provided with tools and resources immediately applicable to your position
- Enjoy a learning experience tailored to your individual goals
- Network with the world’s most respected IT and IS professionals
- Sharpen your skills

And don’t miss special guest speaker David Pogue of the New York Times.

Register today at isaca.org/NACONF-journal1

Register on or before 18 February 2013 and save US $200!
Columns

4 Guest Editorial: Forget the Governance! What to Do When the CEO Says "Get It Done!"
Erik Guldentops

5 Information Security Matters: Mean Times
Steven J. Ross, CISA, CISSP, MBCP

7 Cloud Computing: Shifting the Focus to Long-term, Value-add Projects With a Cloud Environment
Shahin Pirooz, MCP, MCP+I, MCSE

10 IT Audit Basics: How to Properly Audit a Client Who Uses a Service Organization—SOC Report or No SOC Report
Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA

14 Five Questions With… Eugene Liderman

Features

16 Book Review: IT Governance: A Pocket Guide
Reviewed by Dauda Sule, CISA

17 Governance Implementation—COBIT 5 and ISO
Larry Marks, CISA, CGEIT, CRISC, CFE, CISSP, CSTE, ITIL, PMP

24 IT Policy Framework Based on COBIT 5
Jorge Carrillo, Ph.D., CISA, CISM, CISSP

28 Influence of International Best Practices on the South African Public Service’s Corporate Governance of ICT
T. van der Walt, A. D. Coetsee and S. H. von Solms

33 Creating the Business Case for ERP System Acquisitions Using GEIT
Gregory Zoughbi, CISM, CGEIT, PMP, TOGAF9, ITIL Expert, COBIT 4.1 (F)

39 BYOD Security Considerations of Full Mobility and Third-party Cloud Computing
William Emmanuel Yu, Ph.D., CISM, CRISC, CISSP, CSSLP

43 IT Governance Implementation—Formulating and Presenting Practical Business Cases
Rajesh Bhatia, CISA, CGEIT, PMP, MDP

52 Crossword Puzzle
Myles Mellor

53 CPE Quiz #146
Based on Volume 5, 2012
Prepared by Sally Chan, CEGIT, CMA, ACIS

55 Standards, Guidelines, Tools and Techniques

S1-S4 ISACA Bookstore Supplement

Journal Online

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the Journal? Additional online-only articles will be available on the first business day of each month in which no Journal is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members during 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 February 2013.

BYOD in the Enterprise—A Holistic Approach
Srikanth Ravindran, Rajat Sadanais and Deepa Baranwal

Convenient Quality Control for IT Governance-aware Enterprises
Tugba Yildirim, CISA, CRISC, and Bilgin Metin, Ph.D.

Using Personal Mobile Devices in a Business Setting
Pascale A. Bizarro, Ph.D., CISA, Andy Garcia, Ph.D., CPA, and Jacob Nix

Discuss topics in the ISACA Knowledge Center: www.isaca.org/knowledgecenter
Follow ISACA on Twitter: http://twitter.com/isacanews; Hashtag: #ISACAJournal

Join ISACA LinkedIn: ISACA (Official), http://linkd.in/ISACAOfficial
Like ISACA on Facebook: www.facebook.com/ISACAHQ

Read more from these Journal authors…

Journal authors are now blogging at www.isaca.org/journal/blog. Visit the ISACA Journal Author Blog to gain more insight from colleagues and to participate in the growing ISACA community.

The ISACA® Journal seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The Journal’s noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.
Enterprises around the world are adopting and using ISACA’s research deliverables. Developed to adhere to regulations, build efficiencies and improve the value of information systems, ISACA® is dedicated to providing the most relevant tools to promote growth, innovation and trust.

ISACA publishes globally recognized good practices, frameworks, and a wide range of thought-leading research and value-added guidance relating to risk, emerging trends, governance of enterprise IT, information security, and IT audit and assurance. Through this comprehensive research, ISACA defines the roles of those in the IT trust and value professions worldwide.

Following is a sample of ISACA’s most current research:

**COBIT 5**—Information is driving change in today’s enterprise. Enterprises count on accurate, reliable information on which to base business decisions. COBIT® 5 is the only end-to-end business framework for the governance and management of enterprise IT.

**KEEP UP WITH THE CLOUD**—Assess the value that cloud computing represents to your enterprise and how this value can be achieved, while mitigating the associated risk.

**BYOD**—Who has access to your data? Evaluate how you can accommodate employee requests to provide their own devices, while balancing value, risk and resources.

Your support will assist in offsetting continuing development costs, including additional research deliverables and future enhancements of COBIT.

You can support ISACA and ITGI’s work via:

- A personal gift (US $25* or more) to ISACA or ITGI, which recognizes you as a contributor in the ISACA/ITGI Annual Report.
- A corporate gift from your employer to ISACA or ITGI. Many employers will match an employee gift made to a non-profit organization.

Gift Levels range from:

- **Platinum Circle** ......... US $500 or more (Gold Circle benefits + two complimentary publications)
- **Gold Circle** ............. US $250 - $499 (Silver Circle benefits + one complimentary publication)
- **Silver Circle** ............. US $100 - $249 (Recognition in the 2013 Annual Report + lapel pin)
- **Donor Circle** ............. US $25 - $99 (Recognition in the 2013 Annual Report)

* US donors may wish to make their contributions/gifts to ITGI, rather than ISACA, as those funds are deductible for US tax purposes.

To donate today, please either send your gift indicating “donation” to ISACA or ITGI, 1055 Paysphere Circle, Chicago, IL 60674 or donate online during your membership renewal process by visiting [www.isaca.org/renew-donate](http://www.isaca.org/renew-donate).

We sincerely thank you in advance for your contribution and continued support!
I recently had the pleasure of attending a power lunch with several chief information officers (CIOs) when one of them looked at me, knowing I have been a strong advocate of IT governance for years, and threw this issue on the table: ‘What do you do if the chief executive officer (CEO) tells you to “get it done and forget the governance”? You probably go away and just do it, no?’

I should have been faster on my feet to say then and there that there are four good reasons why that is not necessarily the best response. The reasons are:

• **Compliance.** The probability is high that a compliance issue emerges in such a situation. However, because of the questioner’s company’s small size and industry type, that may not have been a major problem.

• **Efficiency.** It is true that it is the prerogative of executives to make the trade-off between cost and timely results when ‘get it done’ is more important for the enterprise. But then, that should be very clear to all involved at the time of the decision.

• **Risk.** While compliance risk may be acceptable in this type of enterprise, there are other liabilities that governance plays an important role in keeping under control—liabilities related to products, employee safety or continuing survival of the enterprise. There are legal standards a judge would use for what is acceptable and what is reasonable (see figure 1) should a liability case emerge. Pointing out that the executive should consider what he/she will say to the judge when this occurs is a way to raise awareness.

• **Effectiveness.** It is clear that, in the case described, governance was not recognised as a mechanism to help achieve effectiveness.

The CEO took the position that he was the sole authority on governance. In this enterprise, the balance of executive and ownership power rests in one person, who probably thinks more as an owner than as an executive.

The CIO accepted that he was the major effectiveness tool. It is true that leadership is a major governance mechanism, even more so in small organizations with short, effective spans of control. The CIO did have a problem with the situation, which reminds me of a similar case a friend of mine related to me: His advice was sought by a CIO about strong differences of opinion at the management level within his company, and my friend suggested the CIO seek another job. This illustrates another version of the CIO acronym: Career Is Over!

However, there is one more version of the acronym that I am reminded of because of the emerging role of the CIO as an influencer and educator. The CIO has to educate executives not only on the intricacies of technology and how it creates value for the enterprise, but also about the necessary governance mechanisms that help make that happen. Therefore, CIO also stands for: Communication Is Obligatory!

So, forget the governance? Yes, but only if more than one of these conditions are true: The enterprise is small, IT is not important and the CEO is the owner.

A version of this article previously appeared in CIONET Belgium. It is reprinted by permission.

---

**Figure 1—Standards for ‘Acceptable’ and ‘Reasonable’**

<table>
<thead>
<tr>
<th>Acceptable: If provable damages do occur, a judge will consider what other companies are doing (‘good practice’) and what international standards prescribe.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasonable: Safety engineering defines it as unreasonable when a user:</td>
</tr>
<tr>
<td>• Does not know there is a risk</td>
</tr>
<tr>
<td>• Does not know what to do about the risk</td>
</tr>
<tr>
<td>• Has no choice as to the cost of what needs to be done</td>
</tr>
</tbody>
</table>

Go directly to the article:  

https://www.isaca.org/journal?page=7&article=9566
Mean Times

As I have said in several recent articles, cyberattacks have become a reality with which global businesses must deal. In the recent past, banks across the US have suffered denial-of-service attacks, for which a hacker group calling itself Izz ad-Din al-Qassam Cyber Fighters claimed credit. In other countries, RasGas, a leading producer of liquefied natural gas was hit with a virus and Aramco, in Saudi Arabia, had 30,000 computers wiped clean by the Shamoon virus, which replaced data with images of a burning American flag. US Secretary of Defense Leon Panetta has warned that his country—and, by extension, the rest of the world—is facing the possibility of a “cyber-Pearl Harbor” and is increasingly vulnerable to foreign computer hackers who could dismantle the US’s power grid, transportation system, financial networks and government.

In fact, emerging cyberattacks against the US’s critical infrastructures are rapidly outstripping the ability of security and risk management professionals to maintain high availability and uptime assurances. Where in the past increased threats have prompted security and risk managers to heighten the intensity of backup and replication arrangements and move to near-instantaneous recovery capability, a traditional recovery approach ironically may be exactly the wrong solution for an advanced cyberattack—and might dramatically lengthen eventual recovery time for the IT infrastructure—perhaps far beyond typical recovery scenarios. Although national infrastructures are the current targets of advanced cyberattacks, these issues readily apply to general, nondefense enterprises as well, as attacks grow more sophisticated, stealthy and more broadly focused on economic espionage threats.

FAILURE, NOT DISASTER

Many organizations focus their security systems to detect and prevent malicious penetration of their information technologies. They have also built robust disaster recovery capabilities in case their data centers are destroyed. In many organizations, the information security and disaster recovery functions occupy separate silos. Cyberattacks (and the even more frightening possibility of all-out cyberwar) expose organizations to the possibility of major systems disruptions and loss of data; functional separation between information security and disaster recovery could multiply the exposure. Most organizations are completely unprepared for this, even after spending significantly on disaster recovery preparedness.

It is a truism that all engineered products will fail if given enough time. That is often expressed as the mean time to failure (MTTF), which every engineer hopes will be very long and that the mean time to repair (MTTR) will be very short, if and when failure does occur. Simply put, software fails—purchased and in-house developed software, software as a service (SaaS) and other cloud implementations. Hardware fails, which is why preventive maintenance is so important. Information security systems are also engineered products and they too will fail over time, especially given the stress of dedicated, malicious attacks that are motivated more by a desire to harm the systems’ owners than to disclose private information or commit fraud. If that were not worrisome enough, there is evidence that cybermalware has been embedded within chips at time of manufacturing—with an attack essentially built-in before the hardware is even delivered.

TRADITIONAL DISASTER RECOVERY PLANS AND CYBERATTACKS

Without understating the need to prevent successful attacks, consideration must be given to the possibility that the attackers may be shrewder or more patient than the defenders and that sooner or later the walls surrounding information systems will prove too low or too flimsy to prevent damage—perhaps catastrophic damage. It is at this point that disaster recovery plans—traditionally based on the transfer of data, hardware, software and networks to a
backup location—prove insufficient. If a primary location has been brought down, there is no benefit to bringing up the failed systems elsewhere; the attacker will just strike again. (In fact, the infection or flaw may already be buried deep within software and data. So-called recovery at a backup site will only bring the problem along with it.)

Traditional disaster recovery planning is not applicable because recovery times following a cyberattack cannot always be controlled and recovery points are only as meaningful as the trust an organization can place in its backups. Applying the techniques of traditional disaster recovery to a security system failure is likely to be counterproductive. Instead, it is necessary to carry out several steps:

1. Recognize that systems are under attack, assess the likely attack method, contain the damage and prevent its spread.
2. Prevent recurrence of the attack by removing the malicious code, repairing other vulnerabilities illuminated by postattack analysis and improving security controls.
3. Restore software and data on primary computers in their original data centers from a trusted image. Note that replicated data and backup tapes are not necessarily trusted, depending on the nature and timing of a cyberattack.
4. While all of this is happening, manage the resulting crisis caused by an attack and minimize its impact on the business.

ORGANIZATION AND PLANS

Recovering from such an unfortunate event as a cyberattack requires both organizational and technical plans consistent with the most up-to-date guidance from international and local computer emergency response teams (CERTs). There needs to be an organizational structure to guide an organization through recovery and a plan for the steps to take.

In other disruptive events, a rather senior level of management must determine that a crisis exists and then deploy funds, personnel, material and skills to respond. In a cyberattack, those entrusted with dealing with the problem must have the authority to initiate emergency actions immediately, only then notifying senior management of what has occurred. Simply put, cyberattacks roll out with such blinding speed that waiting for approval from above may undermine the very response that is needed.

While the specific steps for recovering from a cyberattack are necessarily driven by the particular circumstances of an attack, it is patently foolish to wait until it occurs to plan for recovery. Fortunately, many organizations have already developed plan components that can be adapted for the circumstances of a cyberattack.

The unique element in cyberattack recovery is a recovery in place plan (RPP). As noted, existing disaster recovery plans are unlikely to be effective in the circumstances of a cyberattack. However, few, if any, organizations have plans for the recovery of all or a great percentage of their systems at the same time, under hostile circumstances. But almost all have processes, documented or not, for server configuration, storage allocation and network redirection, among others. These can be built upon to plan for rapid recovery from a cyberattack, beginning with a “bare metal” restore of the most critical systems and then rolling forward to trusted images of the data and software.

It is important to recognize that recovery from a cyberattack is a repair of a failed system and to recognize the consequences of that failure, more than restoration, following a disaster. The MTTR can be shortened only with a combination of skilled individuals merging the disciplines of IT systems architecture and support, information security, and disaster recovery.

ENDNOTES

3 Fineren, Daniel; “UPDATE 1—Qatar’s RasGas Hit by Computer Virus,” Reuters, 30 August 2012, http://in.reuters.com/article/2012/08/30/qatar-rasgas-idINL6E8JUD1K20120830
BRE Properties Inc. develops, acquires and manages multifamily apartment communities throughout Arizona, California, Colorado and Washington, USA. In 2004, BRE’s IT group was focusing most of its resources on infrastructure support, leaving minimal time for the development and implementation of business intelligence systems and applications.

“We spent 70 percent of our time on short-term issues like email outages, network attacks, virus clean-up, user support and slow network performance,” said Steve Jensen, BRE’s vice president of information technology. “We wanted to shift our focus to long-term, value-add projects like business intelligence, applications and enhancements.”

To shift that focus, BRE needed a robust IT environment as a backbone. It would need to deliver high availability and uptime, be flexible enough to support the company’s continued growth, and offer reliable access to help improve productivity among 800 employees working in various locations throughout four states.

Additionally, the company also wanted weekend and after-hours support. While BRE had three employees who spent a large part of their day answering tech-support questions, it was not enough to handle the service calls that would ultimately arise outside traditional business hours because a significant percentage of the company’s employees worked weekends and evenings in remote locations.

As the company planned to move its headquarters, BRE’s executives believed the time was right to embark on an upgrade of its technology and processes. The first decision they had to make was whether they could achieve their goals with in-house IT staff and resources. They quickly realized that would not be possible with the approximately 15 IT employees the company had at the time. To build, deploy and maintain the infrastructure that the publicly held company now required, BRE knew it would incur significant capital expenditures and it would have to hire external consultants to develop and build the solution. This process could take several months, and BRE wanted to move more quickly. In addition, to achieve a solution with the redundancy and high availability it desired, it would need deep network and server expertise, as well as proactive management and 24/7 monitoring capabilities.

“Although our IT environment would be supporting mission-critical tasks, we decided that we wanted to outsource the development and management of it in order to focus our attention on business growth,” said Jensen. “Partnering with an expert cloud service provider made much more sense than assigning more resources to build the infrastructure and support users in-house.”

After a thorough review of cloud computing and hosted IT service providers, BRE chose CenterBeam Inc., whose hosted IT services model allowed BRE to access the resources, expertise and tools to deliver and manage the enterprise-class solution it required, and continue to stay up-to-date with the latest technology—all from the cloud.

BRE needed a solution that could easily scale to meet the company’s future growth without significant capital expenditure (CAPEX) investment. It also required a robust IT design for business continuity and disaster recovery, which included its hosted collaboration suite, network and server management and monitoring, server backup, endpoint security, and 24/7 end-user support. The solution covered more than 100 network devices and 770 endpoint devices under management at 44 sites in four US states. It provided services to more than 800 employees—700 of whom received end-user support from CenterBeam—and encompassed more than 850 email boxes and 150 mobile devices/smartphones.

Shahin Pirooz, MCP, MCP+I, MCSE, has nearly two decades of experience in operations management, account leadership, project management and customer relationship management. He serves as chief security officer and chief technical officer of CenterBeam. Pirooz has held critical leadership roles with leading organizations, including EDS, with responsibilities for key clients including Palm, Philips, VLSI, Netigy and others. He offers deep technology expertise covering areas such as IT architecture (development, design, planning and implementation), as well as core tools, operating systems and programming languages.
THE RESULTS: SAVINGS, SECURITY, SUPPORT, SIMPLICITY AND STRATEGY

It took only a matter of weeks to re-architect the real estate company’s network and implement the new hosted IT solution. The fast deployment timeline enabled BRE to start seeing the results almost immediately (figure 1):

- **Savings**—By outsourcing in a cloud environment, rather than building an in-house support infrastructure, Jensen believes that the company achieved a significant savings, offsetting operational costs of hardware, software and design; eliminating software and hardware maintenance contracts; maintaining storage and network capacity; and not needing to purchase expendable supplies, such as backup tapes.

In addition to the financial savings, BRE’s IT staff and employees saved valuable time. Instead of spending time trying to react to network outages or attacks, or answering other employees’ tech support questions, the IT staff could focus on its core mission of developing and supporting business intelligence and applications.

BRE’s employees at its headquarters and those working from its several remote locations also experienced time savings and improvements in efficiency with the cloud solution. With 24/7 support available, there was virtually no wait if they needed assistance with a technical issue or had a question about how an application worked. In addition, because the service provider is continually updating its solution, BRE employees have access to the most current productivity applications to help them do their jobs with ease.

- **Security**—Using the cloud significantly enhanced BRE’s network security through continual updates to security software and constant monitoring of network resources and endpoints. When a virus affects the entire company, the service provider works quickly with BRE to eradicate the threat.

The improved endpoint security is of particular importance to BRE because its employees are highly reliant on mobile devices to work while on the go or at apartment sites. With this solution pushing out updates and inspecting security policies, all of BRE’s devices—from servers and desktop computers to smartphones—are equally protected from security breaches.

- **Support**—BRE now has access to 24/7 live help desk and customer-care support, which accommodates all levels of users, answering questions that range from routine ones asked by less tech-savvy employees to complex queries from power users. Additionally, response time has significantly improved. Calls are answered within 60 seconds, and if online diagnostic tests will take more than 10 minutes, the service provider offers the option of logging back onto employees’ computers after they have left for the day, so worker productivity is not impacted.

- **Simplicity**—As BRE continues to add apartment leasing offices across the western United States, its service provider has simplified the IT installations by bringing in staff to help set up each new office.

- **Strategy**—Jensen acknowledges that it was hard to imagine how BRE’s 12-person IT staff could have been expected to cover the full spectrum of IT needs—from the base layer architecture to the sophisticated business intelligence and executive dashboard reporting solutions. “We really benefited from a technology partner…to fill in the pieces and provide the expertise that keeps us up to date with fast-moving technological advancements,” Jensen said.

Its service provider... has expanded BRE’s IT team on a temporary basis to support the company’s growth.

| Security: Mitigated 1,000+ virus attacks | Support: Closed over 9,000 cases last year with 99% satisfaction | Simplicity: Accelerated IT support for new sites by 50% | Strategy: IT focus on business intelligence systems and apps grew from 30% to 70% |

Figure 1—Results of Implementation
Now, the time the IT staff spends on infrastructure support has significantly decreased from its previous 70 percent to 30 percent. Jensen said that 70 percent of the IT staff’s time is focused on business intelligence and applications that directly impact the company’s bottom line, instead of dealing with email and virus issues. “Leveraging cloud computing and hosted IT services has allowed us to put the IT focus into a higher value-added arena, and that is huge for us,” he added.

The ability to monitor the health of all of BRE’s network devices and proactively address any problems through the cloud is another valuable service improvement for BRE. “If we do have an outage on a router, our provider is aware of it before we are,” said Jensen. “In the past, we often had to wait for our employees to alert us that they were not getting email, or could not get online, which often lengthened the duration of the outage.”

BRE continues to evolve over time, most recently in 2010, redesigning its network for the second time to help address multiple challenges, such as use of link filtering and endpoint and mobile device management.
The new standards from the American Institute of Certified Public Accountants (AICPA) on service organization controls have created a situation in which IT auditors, especially Certified Information Systems Auditors (CISAs), are particularly needed and useful. Usually, the controls of interest associated with the service organization (SO) are embedded in IT, about IT or are IT (e.g., automated controls). In the case of Service Organization Control (SOC) 2 and 3 report engagements, there is an even greater need for a subject matter expert, such as a CISA®, to identify and evaluate the controls associated with the five Trust Services Principles, which are the benchmarks of those engagements and associated controls.

However, this article focuses on SOC 1/Statement on Standards for Attestation Engagements (SSAE) No. 16 engagements because of the unique situation regarding the user auditors who are evaluating internal controls over financial reporting (ICFR), usually IT auditors, and their need to have a SOC 1 Type II report to cover the controls of interest at the SO. This is complicated by the fact that sometimes the SOC 1 report is somewhat ineffective and may not exist at all. The latter is sometimes accompanied by the presence of another independent controls report, such as an International Organization for Standardization (ISO) report.

What should user auditors do under these circumstances and what is their responsibility to be compliant with the risk-based standards of the AICPA?

**WHERE TO START?**
The fundamental thought process is to remember what the standards require of the user auditor and to keep that as the driver of the audit plans, procedures and processes, rather than becoming engrossed in what is right, wrong, bad or strange.

**Gain an Understanding of the Relevant Process**
The risk-based standards of the AICPA require the auditor to gain an adequate understanding of the processes involved—in this case, an understanding of the processes existing between the SO and user entity. A map or diagram is usually helpful in gaining an understanding of processes. The traditional accounting process flow is helpful to remember in developing a map or diagram: Initialize → Authorize → Record/Journalize → Report.

A more applicable flowchart would be one that incorporates the SO and its impact (see figure 1). The additional steps are key focal points. These three intermediate steps—export to SO, SO process/service and import from SO—help the IT auditor to identify where and what controls should be in place. They also represent the impact and effect of the SO on the accounting process flow and the underlying financial data.

The user auditor must answer questions about exactly what processes are taking place, where they are taking place, how the SO processes interact and interface with user entity systems and data files, and what controls should be in place throughout all of those processes.

**Gain an Understanding of the Export/Import Controls and Processes**
The key to evaluating controls at the SO by the user auditor is to understand the process. An important element of these tasks is that data are usually being exported to the SO for it to process and provide its service, and then the resulting transactional data are imported by the user back into its accounting records. The user entity almost always has some controls and/or processes associated with the export and import steps that end up being complementary controls to the SO controls and its processes.
The user auditor needs to gain an understanding of the three steps (Figure 1) related to the SO. For example, if the SO is a payroll provider, the user might have some manual review of the pay data that are being sent to the SO to make sure they are complete and accurate (similar to assertions about this class of transactions or resulting account balances). That review process is a key complementary control to whatever controls the SO has in place to process the incoming data to generate payroll checks and to properly process all of the financial factors associated with payroll, such as taxes. Of course, the user entity might also have either an automated reconciliation or IT-dependent control that serves the same purpose as manual review.

Later, when the checks and payroll data are imported back to the user, the incoming data might be subject to some reconciliation by the user. That control is complementary to those used by the SO in performing its service and can be manual, automated or IT-dependent.

Part of this analysis is not only evaluating what controls are in place, but also thinking through what controls should be in place, which will be referred to herein as the “anticipated controls.” The IT auditor needs to go through that thought process to determine if any key controls are missing.

The end goal is to have some comfort and assurance that the SO controls, the complementary user controls or a combination of the two provide adequate assurance about the underlying financial data.

**SOC 1 REPORT EVALUATION**

The next step would be to see if the SO has a SOC 1 report. If it does, the IT auditor would probably be asked to evaluate the SOC report to see if it adequately describes assurance over the anticipated controls. If the key relevant controls are addressed, the user auditor can proceed with the audit program. That evaluation process would include gathering evidence that those key relevant controls are designed effectively, placed into operation and operating effectively (i.e., a SOC 1 Type II report).

The key steps in fulfilling the user auditor’s responsibility are as follows:

- Make sure the controls identified in the SOC report (or alternative report) are the key relevant controls (clarified SAS No. 70).
  - If there is no SOC 1 report:
    - Consider an alternative applicable report, if present, and whether it can be used.
Auditor needs to examine ways to change the nature, timing and extent of audit procedures to gain adequate assurance. For instance, extent could be changed by pulling a larger sample size to test transactions that were affected by the SO’s processes. The user auditor also has the option of relying on complementary controls—if they sufficiently provide assurance over the SO’s process and resulting transactions and, thus, provide compensating controls.

The preferred report is a SOC 1 report that gets the controls right—that is, a SOC 1 report that includes anticipated controls. However, there are occasions where no SOC 1 report exists. For instance, PayPal has a large presence in e-commerce payment systems, yet it has no SOC 1 report. Such entities do sometimes have an alternative report. The key thing to remember in this situation is what was discussed in the “Where to Start?” section and in the basic steps list. That is, the process using a different type of report is basically the same process. Care should be taken in exercising judgment to consider comfort and assurance that the alternative report provides.

That is, it is possible that an alternative report could include the relevant, anticipated controls and some assurance about these controls. While it may not be as substantive or reliable as a SOC 1 report, that does not mean it cannot be used or relied upon. The process described previously should assist the IT auditor in reaching a sound conclusion about the SO and controls when using an alternative report.

Some examples of potential alternative reports are listed in table 1. When an alternative report is used, it is particularly important to include an IT auditor because the average financial auditor may not have heard of these reports nor know how to interpret them.

- If no alternative is present or usable, focus on complementary controls.
- If complementary controls provide an inadequate level of assurance, consider changing the nature, timing and extent of procedures to obtain the appropriate level of assurance (skip rest of steps).
- Obtain evidence that those controls (the anticipated controls) are designed effectively, were placed into operation and operated effectively during the period (something many alternative reports will not be able to provide, including even SOC 2 and SOC 3 reports).
- Document evidence. Standards do expect the documentation to map the controls at the SO to the complementary controls at the user and the applicable management assertions and account balance or class of transactions.
- Determine what tests of controls should be conducted, i.e., where risk of material misstatement (RMM) can be reduced, and allow the user auditor to reduce substantive procedures (change nature, timing and extent of procedures), e.g., reduce the sample size of a procedure.

If the IT auditor (user) relies on a SOC 1 report, the evaluation needs to be documented. The mapping mentioned previously is a key aspect of documentation as it relates to specific user management assertions and user complementary controls. The point is to connect specific SO controls to specific management assertions and account balances. That mapping could be accomplished by a sophisticated system, a spreadsheet or even some manual documentation.

The presence of a SOC 1 report is not justification to “check a box” marking the audit step as done with no further work. Such a reaction would result in a failure to comply with the risk-based auditing standards. Secondly, the presence of a SOC 1 report does not automatically lead to a reduction in sample size. Any reduction in sample size should be based on evidence obtained by applicable tests of controls.

The SOC 1 report, however, may not cover the anticipated controls to a level of sufficiency. For example, there could be one or more key anticipated controls that are not in place, or there could be one or more key controls that are not operating effectively as described in the SOC report. A Type I report does not provide for testing of controls and operating effectiveness and, thus, limits the ability to use the report to gain audit efficiencies. A SOC 3 report is of little to no value because it does not describe the tests and results. In either case, the user auditor needs to examine ways to change the nature, timing and extent of audit procedures to gain adequate assurance.

For instance, extent could be changed by pulling a larger sample size to test transactions that were affected by the SO’s processes. The user auditor also has the option of relying on complementary controls—if they sufficiently provide assurance over the SO’s process and resulting transactions and, thus, provide compensating controls.

A REPORT, BUT NOT A SOC 1 REPORT

The preferred report is a SOC 1 report that gets the controls right—that is, a SOC 1 report that includes anticipated controls. However, there are occasions where no SOC 1 report exists. For instance, PayPal has a large presence in e-commerce payment systems, yet it has no SOC 1 report. Such entities do sometimes have an alternative report.

The key thing to remember in this situation is what was discussed in the “Where to Start?” section and in the basic steps list. That is, the process using a different type of report is basically the same process. Care should be taken in exercising judgment to consider comfort and assurance that the alternative report provides.

That is, it is possible that an alternative report could include the relevant, anticipated controls and some assurance about these controls. While it may not be as substantive or reliable as a SOC 1 report, that does not mean it cannot be used or relied upon. The process described previously should assist the IT auditor in reaching a sound conclusion about the SO and controls when using an alternative report.

Some examples of potential alternative reports are listed in figure 2. When an alternative report is used, it is particularly important to include an IT auditor because the average financial auditor may not have heard of these reports nor know how to interpret them.
Those standards include: (1) the replacement of the service side of SAS 70, Statement on Standards for Attestation Engagements (SSAE) No. 16, “Reporting on Controls at a Service Organization” and the concomitant Service Organization Control (SOC) 1 report, an engagement that is formulated as an agreed-upon procedure (AUP) and follows the applicable attest standard, AT 801, and which is specifically for evaluating internal controls over financial reporting (ICFR) related to the SO; (2) SOC 2 report, again is an AUP engagement that follows AT 801, but is about controls as described in the Trust Services Principles of the AICPA; and (3) SOC 3 report, again an AUP engagement following AT801, and is the only SOC report with unlimited distribution, and addresses the Trust Services Principles.

While the SOC 2 report may provide adequate ICFR coverage on some entities, for the most part, a SOC 2 will not be an effective report to use for reviewing SO in terms of ICFR. A SOC 3 is even less effective because it has such limited information in it (e.g., it eliminates tests and results details).

A Type I report provides for no operating effectiveness tests of the controls in place. Therefore, since the full scope of this process includes effects of the further audit procedures, especially opportunities for reducing substantive tests, the Type II report is the focus of this article. Any time SOC 1 is mentioned, it is by default referring to a Type II report.

The presence of an effective SOC 1 report is a great tool for the IT auditor who is involved in a financial audit for a user who has an SO that is in scope. However, it is not uncommon for an SO in scope to not have an effective SOC 1 report. Sometimes the report is present, but not effective. Sometimes there is no SOC 1 report at all. However, the IT auditor may be able to rely on either complementary user controls or an alternative controls report (e.g., an applicable ISO report). One key thing to remember is that the steps and auditor process are essentially the same in all cases because the goal or purpose is the same.

**CONCLUSION**

The risk-based standards include Statements on Auditing Standards Nos. 104–111. SAS No. 109 “Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement” is of particular interest. SAS No. 103 has some applicability as it relates to proper documentation.

**ENDNOTES**

1 Those standards include: (1) the replacement of the service side of SAS 70, Statement on Standards for Attestation Engagements (SSAE) No. 16, “Reporting on Controls at a Service Organization” and the concomitant Service Organization Control (SOC) 1 report, an engagement that is formulated as an agreed-upon procedure (AUP) and follows the applicable attest standard, AT 801, and which is specifically for evaluating internal controls over financial reporting (ICFR) related to the SO; (2) SOC 2 report, again is an AUP engagement that follows AT 801, but is about controls as described in the Trust Services Principles of the AICPA; and (3) SOC 3 report, again an AUP engagement following AT801, and is the only SOC report with unlimited distribution, and addresses the Trust Services Principles.

2 While the SOC 2 report may provide adequate ICFR coverage on some entities, for the most part, a SOC 2 will not be an effective report to use for reviewing SO in terms of ICFR. A SOC 3 is even less effective because it has such limited information in it (e.g., it eliminates tests and results details).

3 A Type I report provides for no operating effectiveness tests of the controls in place. Therefore, since the full scope of this process includes effects of the further audit procedures, especially opportunities for reducing substantive tests, the Type II report is the focus of this article. Any time SOC 1 is mentioned, it is by default referring to a Type II report.

4 The risk-based standards include Statements on Auditing Standards Nos. 104–111. SAS No. 109 “Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement” is of particular interest. SAS No. 103 has some applicability as it relates to proper documentation.

5 IT-dependent controls are those that are partly manual and partly automated.
Eugene Liderman

Eugene Liderman is the director of public sector technology within the office of the chief technology officer (CTO) at Good Technology. His primary responsibility is to assist customers in navigating the unique mobile security challenges that exist within the US Department of Defense (DoD) and federal spaces. Prior to this role, he served as the director of special markets and focused on emerging technology as well as alliances to help provide innovative solutions for Good Technology's security-conscious customers.

Prior to joining Good Technology, Liderman was a senior exchange engineer with the Office of the Chief Technology Officer at the District of Columbia. His responsibilities included architecting and supporting the consolidation and migration of the district's dispersed 40-plus NT 4.0 Domains into one central Active Directory Forest and Exchange 2003 organization, which housed more than 35,000 mailboxes. Additionally, Liderman was responsible for deploying the district's first wireless initiative and maintained the infrastructure thereafter. He has spoken at numerous conferences on topics ranging from networking, directory services, email, wireless email, mobility and information security.

Outside of work, Liderman enjoys the same things he does at work—finding the ultimate smartphone apps, accessories and gadgets. He is a techie at heart.

Q What do you see as the biggest threats being addressed by IT security professionals? How can businesses protect themselves?

A IT security professionals address a wide variety of threats in today's multitasking environment (i.e., multidevice [desktop, laptop, tablet, smartphone], multinetwork, multilocation [at the office, satellite office, from home, on the road]). Risk can be put into three buckets:

1. **External threat**—When someone from outside is trying to gain access to sensitive data or cause malicious harm to the infrastructure and/or environment
2. **Internal threat**—When someone from inside is trying to gain access to sensitive data or cause malicious harm to the infrastructure and/or environment
3. **Negligence**—Often the biggest risk; in any security policy or framework, the end user could be the weakest link.

The first two areas of risk have typically been mitigated using common techniques in the information security/information assurance arena, such as intrusion prevention software (IPS), intrusion detection software (IDS), data loss prevention (DLP) and continuous monitoring (CM). The third risk type is often the hardest to combat because the user is unknowingly increasing the risk of sensitive data being leaked and/or exposed—not for malicious reasons, but as a result of doing too much or not enough. At the end of the day, the security and usability counterbalance is inversely proportional. When one is high, the other remains low. In cases where security is high and the usability is low, end users will often try to get around the system to make it easier for themselves. The best way to deal with this type of risk is to provide training on a regular cadence to the end user community regarding the common attack vectors they should be aware of on their desktop/laptop as well as their smartphone/tablet. In addition, the IT security group needs to find a balance between the security policies it implements and the usability it provides as the end result.

Q How do you see cloud computing changing the way we do business? What risk is involved with cloud computing and how are our businesses addressing such risk?

A Cloud computing is an interesting paradigm where the chief information officer (CIO) in any organization gets excited because of the potential cost savings and possible productivity gains as a result of having the organization's data stored in a location that is convenient for the entire workforce. At the same time, the chief information security officer (CISO) in the organization gets nervous because the security controls in place to secure data and prevent them from being exposed are basically out of his/her control and, instead, he/she has to rely on the cloud provider for this. In addition, what happens in the rare case when the cloud goes down? Most organizations want to maintain control, and with a cloud solution that is not how things work.
I see many organizations both in the public as well as the private sector adopting cloud computing; the only difference is the type of data they allow to be stored in the cloud as well as the definition of the cloud service itself (e.g., public cloud vs. private cloud). The type of data stored in the cloud depends on the vertical market’s statutory requirements and the sensitivity of the enterprise’s data. In the US federal government, for example, aside from email being migrated to the cloud in a limited way, public-facing nonsensitive data get published to a commercial cloud, whereas, in the private sector, more companies are moving a greater percentage of their data to the cloud.

The US federal government (including the US Department of Defense) is a big proponent of a private cloud concept. Examples include the Defense Information Security Agency (DISA) providing email as a service (MAIL.MIL) to the US Army, or the Department of Homeland Security (DHS) providing centralized email and collaboration to all of their subordinate agencies. A private cloud enables the agency to have additional assurances that its data are stored in a more secure manner and in compliance with applicable regulatory requirements (e.g., the US Federal Information Security Management Act [FISMA] and the Federal Risk and Authorization Management Program (FedRAMP). Commercial clouds, on the other hand, have lower levels of compliance.

Q How do you see the role of governance of enterprise IT (GEIT) changing in the long term?

A I see the GEIT framework continuing to be utilized as a baseline methodology, but when it comes to things like smartphones and tablets that have a rapid life cycle, I envision a greater agility in managing changes. Otherwise, it becomes too much of a burden to onboard and manage newer technologies, which may stifle innovation.

Q How can the cybersecurity problem be addressed? Is this something for government only or is the involvement of nongovernmental organizations required?

A Cybersecurity impacts everyone, not just government. To combat this ongoing threat, the public and private sectors in the US have teemed up through various conferences, programs, committees and working groups. Sometimes these groups consist of specific verticals, such as system integrators/defense contractors, working specifically with their counterparts in the US Department of Defense, and other times, there is representation from various verticals such as health care, finance and government.

Two famous quotes by Sir Francis Bacon sum it up really well. First, “knowledge is power.” The hope is that these various means of interaction between private and public sector organizations provide a platform to share the knowledge gained by these various representatives so that everyone can increase their mitigation strategies against the ongoing cybersecurity threat. The other quote is, “Silence is the virtue of fools.” This applies because the common theme these days is: “It is not a matter of if we have been breached, it is just a matter of when we find out.” Organizations that have been breached need to speak up and educate other organizations on lessons learned around what the potential attack vector was, how they were able to discover it and how they will mitigate it in the future.

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

A My biggest workplace/career challenge has always been around following our own advice, whether it was as an IT consultant, a system administrator working for the government or in my various roles working for a software company. In each one of these roles, it was essential to follow the exact same policies and procedures that we mandated or recommended to others, because if we could not put ourselves in that same situation, we would never have been able to catch some of the potential pitfalls or threats with that particular approach. This covers a wider spectrum than just information security; this also applies to productivity. For example, in my current role, to be truly credible with our customer base, I follow the same stringent guidelines around how I secure my smartphone devices, but at the same time, I make it a priority to try to accomplish as many tasks as I can using my smartphone and/or tablet device because that is what we preach to our customers. As a result, I have 250-plus applications on my iOS devices—I am constantly downloading the latest and greatest business-productivity applications to see whether they add any value as well as create any risk.
IT Governance: A Pocket Guide

IT Governance: A Pocket Guide highlights important issues relating to corporate IT governance, showing how IT can help organizations achieve their goals and objectives. The book is presented using nontechnical terminology that can be easily understood. As such, it will appeal to the management of organizations, IS managers, chief information officers (CIOs), chief information security officers (CISOs) and IS auditors as a guideline for establishing an organizational IT governance framework. Professionals and those seeking to become professionals in IT governance management, security and audit will also find the book useful as a reference guide because it outlines a framework for IT governance. That said, the book is largely directed toward top management tasked with instituting a proper framework for IT governance, as well as to anyone wanting to put an organization on track with regard to balancing IT and business goals.

The book is made up of seven chapters. The first chapter covers the importance of IT governance and defines the term. Chapter two highlights the drivers for IT governance, including competitive advantage, regulatory requirements, security, and strategic alignment between IT and business objectives and goals. Operational and strategic risk management is covered in chapter three, with reference to statistics from research on IT project failures by the Standish Group. Chapters four and six buttress the effects of inadequate IT governance and the benefits, respectively. The basis of and the recipe for a good and successful IT governance framework are presented in chapter five. The book concludes with the Calder-Moir IT governance framework in the final chapter, explaining how the framework can be used to organize IT governance issues for management and related parties. Additionally, related reference materials are listed in the appendix.

The book, being a pocket guide, is very brief and not exhaustive on the topic, which is appropriate as it is meant to be only an abbreviated presentation to top management to help them understand and appreciate the importance of IT governance. The book does this in an excellent way by presenting a business case for IT governance (on page 35), using the results of a survey that showed most organizations would pay an 11 percent premium for the stock of an organization that has good governance practices. Also, survey respondents indicated that organizations with above-average IT governance had profits 20 percent above those with poor IT governance, despite having the same strategy for business.

EDITOR’S NOTE
IT Governance: A Pocket Guide is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650.
ISACA has revised its governance and management of enterprise IT (GEIT) framework from COBIT® 4.1 to 5, incorporating:

- New GEIT principles
- An increased focus on enablers
- A new process reference model
- New and modified processes
- Practices and activities
- Goals and metrics
- Inputs and outputs
- Responsible, Accountable, Consulted and Informed (RACI) charts
- Process capability maturity models and assessments

The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies (ISO member bodies). This organization is responsible for preparing international standards through its committees staffed by members from government, business and nonprofit organizations on a worldwide basis. ISO is in the process of developing a standard (ISO/IEC JTC 1/WG6 N 261) to assist its members with initiating and implementing governance on an accurate and complete basis.

Two separate models to assist in implementing governance exist: COBIT® 5 Implementation (formerly the IT Governance Implementation Guide), issued with the newly released COBIT® 5 framework to address the demand for implementation guidance, and the ISO Governance Model (ISO 38500:2008 Model for Corporate Governance of IT). COBIT® 5 Implementation provides an implementation approach based on quality improvement life cycles. Yet, a step-by-step, unified approach to follow in implementing GEIT that crosses the ISACA and ISO approaches does not readily exist.

This article provides a checklist or mechanism that spans the ISACA and ISO approaches and identifies common questions that need to be considered during the GEIT implementation process.

ISO has identified the elements of implementing governance over IT as:

1. The need to establish an enabling environment to implement governance. An environment required to enable or foster the implementation of GEIT includes:
   - Sponsorship and responsibilities
   - Stakeholder engagement
   - A baseline (governance) environment
   - Gap analysis to provide focus
   - Striving to improve continuously
   - A governance IT structure that includes:
     - Stakeholder expectations
     - Internal environment
     - External environment

2. Maintaining an understanding of key aspects of the organization so that IT-related assessments and decisions can be realistically made. Key considerations include:
   - Business strategy, risk appetite and performance
   - Strategic change initiatives
   - Assurance reporting, including audit and risk
   - Culture of the organization and tone at the top
   - Organizational maturity and levels of skill
   - Key IT services and how they are provided

3. Keeping apprised of external factors that may drive business opportunities and risk, thereby mandating IT-related business change responses, including:
   - Regulatory environment
   - Technological advances
   - Generational trends
   - Skills availability
   - Competitive forces
   - Stakeholder requirements

ISO standards as well as ISACA’s COBIT 5, which is oriented around the enterprise’s business goals, indicate that it is important to adopt an outcomes-based approach to GEIT, rather than to apply the ISO/IEC 38500 framework to specific operational aspects of IT. This will ensure that the organization is appropriately guided or steered.
in its use of IT, rather than operationally managed, which is the approach of the more detailed process- and/or controls-oriented frameworks, the outputs of which generally provide the inputs in support of GEIT. ISO’s implementation approach is described in Figure 1. ISO 38501 is in draft and the approach may change, but this article tries to provide an idea of a possible implementation approach.

While ISO recommends an outcomes-based approach to GEIT, it does not indicate how this should be implemented to “people on the ground.” That is, ISO does not provide a step-by-step list of actions that are needed to achieve the desired outcome.

ISACA’S GOVERNANCE MODEL
COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use. The framework addresses both business and IT functional areas across an organization and considers the IT-related interests of internal and external stakeholders. Organizations of all sizes, whether commercial, not-for-profit or in the public sector, can benefit from COBIT 5.

COBIT 5 is based on five key principles for GEIT: 1. Meeting stakeholder needs 2. Covering the enterprise end-to-end 3. Applying a single, integrated framework 4. Enabling a holistic approach 5. Separating governance from management

The COBIT 5 framework describes seven categories of enablers:
1. Principles, policies and frameworks are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
2. Processes describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
3. Organizational structures are the key decision-making entities in an organization.
4. Culture, ethics and behavior of individuals and of the organization are very often underestimated as a success factor in governance and management activities.
5. Information is required for keeping the organization running and well governed, but at the operational level, information is very often the key product of the organization itself.
6. Services, infrastructure and applications include the infrastructure, technology and applications that provide the organization with IT processing and services.
7. People, skills and competencies are required for successful completion of all activities, and for making correct decisions and taking corrective actions.

ISO VS. ISACA GOVERNANCE MODEL
With at least two published governance models, is one better than the other? Should each one be used in different situations?

Most enterprise stakeholders and executive management are aware of the importance of general control frameworks (such as Committee of Sponsoring Organizations of the Treadway Commission [COSO]’s Enterprise Risk Management—Integrated Framework, Code of Connection [CoCo], the UK Corporate Governance Code, and King III) with respect to their fiduciary responsibility; however, organization stakeholders and executive management may not necessarily be aware of the details of each framework. In addition, organization managers are increasingly aware of the more technical security guidance, such as the ISO/IEC 27000 series, and service delivery guidance, such as the Information Technology Infrastructure Library (ITIL). Although the aforementioned standard and framework emphasize business control and IT security and service management and delivery issues in specific areas of enterprise IT-related activity, only COBIT 5 integrates all functions and processes that establish
GEIT into overall enterprise governance and from a business perspective.

The COBIT governance approach is based on the evaluate, direct and monitor (EDM) model, which is also used in ISO 38500. COBIT 5 is not meant to replace any of these frameworks or standards. It is intended to emphasize what governance and management elements and practices are required to create value from information and technology in support of the organization's business goals.\(^4\)

ISACA has compared COBIT 4.1 to COBIT 5 and documented the illustrative example process reference model within COBIT 5 (see figure 2).\(^5\)

The following represents processes for governance in COBIT 5:
- APO03 Manage enterprise architecture
- APO04 Manage innovation
- APO05 Manage portfolio
- APO06 Manage budget and costs
- APO08 Manage relationships
- APO13 Manage security
- BAI05 Manage organizational change enablement
- BAI08 Manage knowledge
- BAI09 Manage assets
- DSS05 Manage security service
- DSS06 Manage business process controls

---

**Figure 2—Processes for GEIT**

**Evaluate, Direct and Monitor**

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

**Align, Plan and Organise**

- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

**Build, Acquire and Implement**

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

**Deliver, Service and Support**

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

**Monitor, Evaluate and Assess**

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

---

Bridging ISO Standards and ISACA’s Business Framework

A checklist that bridges ISO’s general approach and ISACA’s business-operations approach is in order; this would help users implement the GEIT model. However, several items are readily apparent when attempting to generate such a checklist:

1. While recognizing the aforementioned 11 management-level processes, one observes that a practical checklist or guide does not exist to either bridge the ISO and ISACA model or help the user reach senior management to ensure that the 11 modified processes are successfully implemented.

2. An aid to help the user use COBIT 5 Implementation to implement the GEIT processes on a higher, more holistic level does not readily exist.

In other words, COBIT processes define the required outcomes from their implementation. An assessment against these outcomes—using an assurance approach including ISO 15504 as implemented in the COBIT Assessment Programme—will provide assurance of successful implementation. However, a checklist or mechanism that attempts to provide users with the ability to overlay the ISO and ISACA approaches would be helpful. Such a checklist addressing other areas of governance would include the following general processes (e.g., application controls, training, change standards and procedures):

- Stakeholder engagement and responsibility
- Sponsor responsibilities
- Nature of internal control environment
- Nature of the external environment impacting the controls
- A baseline of the IT system’s control environment

The checklist, provided in Figure 3, is meant to be a living document that can be enhanced over time. The checklist is aimed at helping the reader to crystallize to some degree the ISO standard and overlay the operational approach of COBIT. COBIT’s governance processes do contain metrics for users to consider and refine or extend the governance processes. Governance metrics have been suggested as a starting point in the form of related metrics linked to each of the process goals in each of the COBIT 5 governance processes. However, there are neither examples of these metrics nor uses of these metrics in a business setting. It appears that metrics that do not readily exist should be developed to evaluate whether an IT governance model, provided by ISO or ISACA, has been successfully implemented.

Along with the checklist, guidance is provided to explain how to use the checklist for reviewing GEIT implementation.

---

**Figure 3—Governance Implementation Checklist**

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Description</th>
<th>No.</th>
<th>Question</th>
<th>Response</th>
<th>Guidance on Gaining or Understanding Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Stakeholder engagement</td>
<td>1</td>
<td>Is senior management seeking a governance model?</td>
<td>Yes/No</td>
<td>This information can be obtained from discussions with senior management and a review of governance RACI charts for lines of business. Look for evidence, preferably documentary, which can be in the form of emails from senior management.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Is the interest to implement governance for one line of business or enterprisewide?</td>
<td></td>
<td>Based on the answer to question A-1, the interviewer can tell if the nature and extent of the interest is enterprisewide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Is there an awareness of COBIT 4.1/5 and ISO/IEC 38500?</td>
<td></td>
<td>If not, the reviewer has to further inquire if the organization is using a home-grown model of governance, a model of governance other than COBIT or ISO/IEC 38500, or is not following an overall standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Has management performed an analysis of the existing management reports to:</td>
<td></td>
<td>It is important for the reviewer to identify: What is the operational information senior management uses to measure the value and quality of goods and services to the customer? Are these metrics only operational in nature? Or, are there qualitative factors, such as number of noncompliance issues cited by regulators, or customer complaints of IT services? Has management cataloged the volume of management reports and then reached out to the end user to determine their value and use? Sometimes dashboards or system reports are generated and emailed for review on a consistent basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Identify the additional operational information required for effective GEIT?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>b. Reduce the nature and extent of management reports?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section Number</td>
<td>Description</td>
<td>No.</td>
<td>Question</td>
<td>Response Yes/No</td>
<td>Guidance on Gaining or Understanding Response</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-----</td>
<td>----------</td>
<td>-----------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>B</td>
<td>Sponsor and responsibilities</td>
<td>1</td>
<td>Has a RACI chart been developed for the governance of IT?</td>
<td>Yes/No</td>
<td>There is a need for clear and appropriate assignment of responsibility that coincides with the organization’s strategy. Where more than an organizational unit is assigned responsibility, e.g., to develop a communication plan, overlapping tasks and extended timelines for projects will result.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Has the RACI chart been compared to the existing state, with gaps identified?</td>
<td>Yes/No</td>
<td>If it has been compared and gaps identified, the reviewer should inventory and evaluate the gaps in terms of risk. If it has been compared and no gaps identified, it is time to proceed to step B-3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Have the organization’s risk and management structure and strategy been documented?</td>
<td>Yes/No</td>
<td>Has the organization’s risk management structure been documented? Has its strategy—its inputs, outputs, gaps in the strategy—been documented?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Has the organization’s compliance program been documented?</td>
<td>Yes/No</td>
<td>Is there an overlap between the implementation of risk management and compliance? Is the program consistent domestically and internationally?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Does the strategy synchronize with the organization’s tolerance for risk?</td>
<td>Yes/No</td>
<td>When did the organization last review its IT strategy, compliance program and risk tolerance by portfolio, by system and by line of business, for example? An organization’s risk-tolerance level may change based on customer needs and line-of-business needs. If an organization’s risk tolerance has not been reviewed for more than two to three years, the IT projects currently being discussed and implemented may be inconsistent with stakeholder/sponsor or market requirements or desires. This may affect the long-term profitability of the organization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>Has the organization’s delegation of authority been documented and accepted by senior management?</td>
<td>Yes/No</td>
<td>Where delegation of authority has not been documented, confusion or mistrust of management intentions may occur.</td>
</tr>
<tr>
<td>C</td>
<td>Internal environment</td>
<td>1</td>
<td>Does the organization’s business strategy by line of business or portfolio agree with its risk appetite and history of performance?</td>
<td>Yes/No</td>
<td>This question builds off the answer to question B-3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Does the organization have a mechanism to track change control for its strategic initiatives?</td>
<td>Yes/No</td>
<td>An organization should have means of tracking the change of its strategic initiatives. This mechanism can assist management to perform lessons learned from the various alternatives that may have occurred. It should be noted that Ishikawa diagrams, generally used in quality assurance and control, can be used to evaluate each change and its cause.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Has an evaluation been independently performed to assure that IT services are provided on a level compliant with the accepted service level?</td>
<td>Yes/No</td>
<td>Has management established a service level agreement (SLA)?</td>
</tr>
</tbody>
</table>
### Figure 3—Governance Implementation Checklist (cont.)

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Description</th>
<th>No.</th>
<th>Question</th>
<th>Response Yes/No</th>
<th>Guidance on Gaining or Understanding Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>External environment</td>
<td>1</td>
<td>Has the organization’s governance framework been modified to agree with the regulatory environment?</td>
<td>Yes/No</td>
<td>The organization’s governance framework needs to be consistent with the type of regulatory environment in which the supporting line of business operates. Otherwise, this may expose the organization to unintentional violations or noncompliance of local, federal or international requirements. For example, does the organization need to be concerned with sales to other countries and control requirements?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Does the organization’s governance framework agree with either market technology or technology in place?</td>
<td></td>
<td>Questions D-2 to D-4 are meant to help users understand how the governance framework was designed, implemented and continues to be maintained.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Does the organization’s governance framework agree with stakeholder expectations?</td>
<td></td>
<td>If yes, the user may proceed to D4. If no, an effort should be made to identify and evaluate the gaps in terms of their impact on the organization and IT risk strategy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Does the organization’s governance framework agree with the board of directors’ expectations?</td>
<td></td>
<td>Has the board of directors reviewed the nature of the governance framework to ensure that it provides for timely information and reaction to the board’s issues and concerns? For example, has the board reviewed its methodology for performing independent investigations, such as the Seaboard report, to ensure that it is consistent with the governance framework?</td>
</tr>
<tr>
<td>E</td>
<td>Baseline</td>
<td>1</td>
<td>Has an evaluation been independently performed on the IT systems to ensure that they can meet existing long-term strategy of the business?</td>
<td></td>
<td>Has the organization independently reviewed its IT systems to identify their efficiency and effectiveness? Do they use current hardware and software? Has the organization performed an inventory and explored the possibility of merging, closing or outsourcing these systems, while complying with their long-term strategy of meeting customer satisfaction?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Has an evaluation been independently performed on the IT systems to ensure that they can meet existing short-term strategy of the business?</td>
<td></td>
<td>Same answer as for C-1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Has an evaluation taken place of security and privacy on an enterprisewide level to identify the vectors for data breaches and their remediation?</td>
<td></td>
<td>This is a corollary to B-3 and B-5. Given the organization’s tolerance for risk, has the organization performed an enterprisewide risk assessment of the nature and extent of IT and business data security and privacy vectors? Have the results been reviewed by risk management and business-line management to prioritize the remediation to be consistent with business requirements?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Has an evaluation of security and privacy on an enterprisewide level occurred to identify the vectors for noncompliance with regulatory requirements?</td>
<td></td>
<td>Same answer as for C-3.</td>
</tr>
</tbody>
</table>
This article provides a checklist or mechanism that spans both the ISACA and ISO approaches and identifies common questions that need to be considered during the GEIT implementation process. The checklist is intended to be user friendly and includes suggested responses and tips to help users in their implementation.

### Figure 3—Governance Implementation Checklist (cont.)

<table>
<thead>
<tr>
<th>Section Number</th>
<th>Description</th>
<th>No.</th>
<th>Question</th>
<th>Response</th>
<th>Guidance on Gaining or Understanding Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>Baseline</td>
<td>5</td>
<td>Are formalized charters require to be developed for the following:</td>
<td>Yes/No</td>
<td>The existence of a formal charter approved by management and the board of directors will ensure that IT policy and strategy, systems architecture, sourcing of services, risk, and audit committee structure and roles are consistent with their requirements and shareholder expectations. The existence of these approved charters will also lead users or the reviewer to generate an opinion relating to the nature, extent and quality of the decision-making process (see the question in A-1).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. IT policy and strategy?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>b. Systems architecture?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>c. Sourcing of services?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>d. Risk committees?</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>e. Audit committee?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CONCLUSION

This article provides a checklist or mechanism that spans both the ISACA and ISO approaches and identifies common questions that need to be considered during the GEIT implementation process. The checklist is intended to be user friendly and includes suggested responses and tips to help users in their implementation.

### ENDNOTES

2 Ibid.
3 IT Governance Ltd., “King Code of Governance Principle,” www.itgovernance.co.uk/king_iii_3.aspx
4 ISACA, COBIT 5 Frequently Asked Questions, www.isaca.org/COBIT/Pages/FAQs.aspx
5 ISACA, COBIT 5 Compare With 4.1., PowerPoint, 2012, p. 17
6 American Society for Quality (ASQ), http://asq.org/learn-about-quality/cause-analysis-tools/overview/fishbone.html
Privacy and IT policies have a lot in common: Both are considered important; organizations are concerned about not having them, but not everybody fully understands the implications and consequences if they are wrongly understood.

Privacy and IT policies are concepts that evolve—what is an acceptable policy today (or what is considered a privacy concern) may not be a satisfactory practice tomorrow. Similarly, COBIT® has evolved from an audit framework in 1996 to a governance and management of enterprise IT (GEIT) framework in 2012, presenting, among other aspects, policies as fundamental factors for influencing proper governance and management over IT.

This article presents a modern approach for designing a policy framework using COBIT® 5 principles, which provide a robust and systematic approach to ensure that policies are used as instruments to implement accepted business strategies. A policy framework provides a logical structure for organizing and defining policies. It also establishes additional documentation that supports the policies’ implementation and enforcement.

The objective of this article is to provide a structured methodology for assisting organizations in developing and implementing an effective policy framework.

**EVOLUTION OF IT POLICIES**

IT policies help organizations to properly articulate the organization’s desired behavior, mitigate risk and contribute to achieving the organization’s goals. The evolution of IT policies can be illustrated by comparing the following two documents: *Generally Accepted Principles and Practices for Securing Information Technology Systems*¹ and *Information Security Handbook: A Guide for Managers.*²

The first one, published in September 1996, states that a policy should, among other aspects, define and specify rules for particular systems. The second one, published in October 2006, defines a policy, in the context of information security, as an aggregate of directives, rules and practices that prescribe how an organization manages, protects and distributes information.

Configuration and standardization of IT systems and infrastructure were priorities in 1996. After 10 years, organizations realized that taking advantage of IT requires proper management and governance of information resources.

Further, it has become apparent that failure to design and implement robust business processes more quickly renders technology-based controls ineffective. For example, the *Verizon 2011 Payment Card Industry Compliance Report*³ points out that organizations struggling to meet Payment Card Industry Data Security Standard (PCI DSS) requirement 12 (maintain security policies) fail to drive practice and successfully implement other PCI requirements.

**IT POLICY CHALLENGES**

Creating IT policies in a changing environment is not a straightforward task but often a necessary one. Organizations might not fully appreciate advantages, limitations and risk factors of emerging technologies; for instance, choosing a cloud computing solution requires management of the associated risk and empowerment for a route to create business value in an environment full of uncertainties.

IT policies are not an IT-only activity. Incorporating IT principles with end-to-end business processes ensures better coverage and cooperation across the enterprise (i.e., responsibilities and authorities are clearly defined), reduces duplication of controls across different teams, and provides a consistent approach to address business requirements.
Finally, as illustrated in the Information Security Management Handbook, the core of any business is its people—their individual attributes, including integrity, ethical values and competence. Therefore, policies should be communicated, understood, supported and accepted by everybody; otherwise, they are meaningless.

POLICIES AS ENABLERS

COBIT 5 introduces seven enablers (see figure 1) as support tools for the implementation of GEIT. The four dimensions (stakeholders, goals, life cycle and best practices) of the enabler Principles, Policies and Frameworks are discussed in the following sections and suggestions for a systematic method of designing and implementing a policy framework are provided.

Figure 1—COBIT 5 Enterprise Enablers


COBIT 5 ensures that a policy framework meets stakeholders’ needs, covers the end-to-end process (and not only the IT function), and establishes the additional documentation required to ensure that governance and management goals and activities are achieved.

Stakeholders Dimension

There are stakeholders who define and set policy principles, and there are others who follow, adhere to or implement such principles.

The first group of stakeholders defines and sets policy principles, taking into consideration general organizational governance principles and analyzing and identifying internal and external factors (e.g. regulation), business direction, and organizational culture. The organization’s board of directors and executive management belong to this group. They are, in addition, accountable for giving direction about, communicating on and implementing governance objectives, and for defining the core components of a policy framework.

The core components of a policy framework are:

- Appointment of individuals who have the authority to approve policies and their associated responsibilities
- Determination of the consequences for failing to comply with given policies
- Definition of a process for handling exceptions to policies
- Definition of a method for measuring and monitoring compliance with policies
- Definition of the scope of the policy and the group of stakeholders that has to follow the policy

The fear, uncertainty and doubt of the other stakeholders are reduced by following policy principles.

Goals Dimension

Goals are statements, based on the policy principles defined previously, that describe the desired outcome. Examples of goal statements are:

- Provide a tool for staff orientation.
- Document proper delegation and define limits of authority and responsibility.
- Serve as a documentation source for regulatory compliance.
- Protect intellectual property and business continuity.
- Improve clarity and momentum in projects and operations.

As far as policies are concerned, goals and policy principles should be related in order to provide assurance that stakeholders’ requirements are addressed.
Life Cycle Dimension
The policy life cycle combines the policy principles and goals defined previously and includes the following phases:

• **Plan**—This phase establishes the foundation for a policy framework by covering the stakeholders and goals dimensions defined previously. Usually, organizations already have some policies in place; therefore, identifying gaps between the governance principles and current, valid policies helps to redesign and improve the policy framework in use. In this phase, a logical structure of documentation that will support and clarify policy principles is defined. The optimal amount of documentation depends on the organization's culture and management's style; the objective of this activity is to improve clarity of policy principles and support their implementation.

• **Design**—There are two activities in this phase:
  1. Priorities setup—Identification of concrete policies, using a risk-based approach that addresses policy principles, setting deadlines and priorities for their review or creation
  2. Policy structure definition—Writing a policy is not only a writing activity; it needs adequate coordination, including:
     - Policy draft—Identify the individuals responsible for researching and writing policies. A critical success factor is to resolve any potential issue concerning the feasibility for implementing policy principles.
     - Policy review—Identify the individuals responsible for providing an independent review. The objective of this activity is to increase the policy credibility and quality.
     - Approval, communication and distribution—Establish the procedure for obtaining final policy approval from the authorized individuals defined in the stakeholders dimension previously, and determine the policy communication and training strategy.
     - Style—Define writing quality standards, including document format, font type, language style, glossary of terms and document structure. The objective of this activity is to ensure that policies are written, presented and structured in a way that is clear, concrete, complete, consistent and easy to follow.

• **Implement**—This activity corresponds to implementation and enforcement policies, defining activities that will assist the organization in providing a transparent transition from a noncompliant to a compliant state.

• **Operate**—An effective policy should be part of the organization's DNA. Building an accountable culture and using policies in daily operations ensures that the organization's goals are met. In this phase, organizations should “walk the talk” of policy principles.

• **Evaluate/monitor**—This phase has the objective to confirm that policy requirements are properly implemented and the organization operates effectively. The degree of success of policy principles supporting business goals is evaluated, and the overall efficiency of the policy framework is communicated to relevant stakeholders.

• **Update/dispose**—To keep policies aligned with business direction, policies are reviewed for updating or removal. This activity has two objectives: to ensure that organizations have effective policies and to adjust the phases defined previously to maintain or improve the maturity of the policy framework. Good practice would require policies to be reviewed on a regular basis, typically every 12 months.

Good Practices Dimension
The separation of governance and management activities points out the need for more specific guidance on how policy principles are implemented and managed. A good practice is to create additional documentation to support policy effectiveness and efficiency, for example:

• **Standards**—A mandatory action: explicit rules, controls or configuration settings that are designed to support and conform to a policy. A standard should make a policy more meaningful and effective by including accepted specifications for hardware, software or behavior. Standards should always point to the policy to which they relate.

• **Procedures**—A written set of steps to execute policies through specific, prescribed actions; this is the *how* in relation to a policy. Procedures tend to be more detailed than policies. They identify the method and state in a series of steps of exactly how to accomplish an intended task, achieve a desired business or functional outcome, and execute the policy.

• **Guideline**—An outline for a statement of conduct. This is an additional (optional) document in support of policies, standards and procedures—general guidance on issues such as “what to do in particular circumstances.” These are not requirements to be met, but are strongly recommended.

• **Baseline**—A platform-specific rule that is accepted across the industry as providing the most effective approach to a specific implementation.
CONCLUSION

All organizations have policies that guide how decisions are made and how business objectives are achieved. An effective policy framework increases organizational accountability and transparency and is fundamental for helping the organization meet its objectives.

Creating policies is more than typing words on a page; it involves a systematic approach for properly articulating governance and management principles. COBIT 5 principles help to provide a holistic approach to include all the minimum requirements for a policy framework, avoiding reinventing the wheel and ensuring that the complete life cycle of a policy is understood.

ENDNOTES

6 Bacik, Sandy; Building an Effective Information Security Policy Architecture, CRC Press, USA, 2008
7 Op cit. Tipton
For South Africa, a developing country, social, economic, political and cultural transformation is very high on its agenda. Information and communication technology (ICT) is a key enabler to achieve these developmental goals and to position South Africa for sustainable growth. But without appropriate governance, the value of ICT cannot be unlocked.

The King Report on Corporate Governance updated in 2009 (King III), issued by the King Committee on Corporate Governance, explains good governance in the context of effective leadership, as the responsibility of strategic leadership to define strategy, provide direction and ensure sustainability of performance.

Corporate governance of ICT (CGICT), as a subset of corporate governance, is subject to strategic leadership in an organisation. When this leadership is either lacking or poorly executed, it negatively impacts the performance of the organisation.

The King Report on Corporate Governance updated in 2009 (King III), issued by the King Committee on Corporate Governance, explains good governance in the context of effective leadership, as the responsibility of strategic leadership to define strategy, provide direction and ensure sustainability of performance.1

Corporate governance of ICT (CGICT), as a subset of corporate governance, is subject to strategic leadership in an organisation. When this leadership is either lacking or poorly executed, it negatively impacts the performance of the organisation.

The successful implementation of CGICT in an organisation is dependent on the implementation of effective governance and management systems on three levels: the governing body, organisational management, and ICT management and operations. (The last item is not the subject of and, thus, will not be addressed in this article.)

Internationally, much research, literature, best practice and standards are available on CGICT. However, research and case studies on CGICT in the governments of developing countries are lacking. For the purpose of this article, the authors identified the following as international best practices in the field of CGICT:

- ISO/IEC 38500, international standard for corporate governance of information technology2
- King III on governance in South Africa3
- COBIT® 5, business framework for the governance and management of enterprise IT (GEIT)4

The article will further discuss how the Department of Public Service and Administration (DPSA)’s CGICT Policy Framework (CGICTPF)5 was influenced by these international best practices. The scope of this article is the South African Public Service, which is constituted of two levels of government, namely the national and provincial government, excluding local governments.6 Reference to departments includes national and provincial departments and provincial administrations.

DISCUSSION OF THE CGICTPF

The CGICTPF facilitates the institutionalisation of CGICT as an integral part of corporate governance within the South African Public Service in a uniform and coordinated manner.7

It follows a layered approach making provision for Public Service-wide political direction and oversight from Parliament and Cabinet, involving policy and monitoring departments and forums. On a departmental level, it provides an accountability structure for the executive authority, head of department and executive management through a set of principles and practices, and provides a governance model and an implementation approach.8

Guided by the CGICTPF, departments are expected to further develop and implement their own framework to suit their individual environments. The CGICTPF requires departments to follow a three-phased implementation approach:

1. Create an enabling environment.
2. Achieve business and ICT strategic alignment.
3. Ensure continuous improvement through an iterative process.
DISCUSSION OF INTERNATIONAL LEADING BEST PRACTICES

It is acknowledged that there are many related good practices and frameworks in the field of CGICT. However, the Governance Task Team found ISO/IEC 38500, King III and COBIT 5 to be the most relevant to inform the development of the CGICTPF because they discuss the practices and principles required to implement CGICT. In this context, a principle is expressed as a preferred behaviour to guide decision making, and a practice is the activities through which the principles are implemented.9

ISO/IEC 38500 Standard

This advisory standard provides a top-down approach and is comprised of definitions, principles, practices required to implement the principles, and a model for the governance of ICT and its related activities.10 The model describes the tasks of evaluating, directing and monitoring and is used to apply the principles. The principles primarily guide governing bodies, which can, in turn, direct that certain actions be taken by management. ISO/IEC 38500 explains the increasing importance of ICT, as a functional business tool, to the current and future business plans of organisations and the related significant ICT expenditure. It assists governing bodies and management to understand their responsibility for ICT within the organisation.

King III

The King III report dedicates a chapter (Chapter 5) to the governance of ICT. It also follows a top-down approach to address the accountability of the governing body and management regarding “leadership, sustainability and corporate citizenship” responsibilities for corporate governance, fully integrating ICT into an organisation.11 It alludes to the ever-increasing reliance of organisations on ICT as an enabler of business and the resultant escalation in organisational risk. King III creates awareness about the responsibility of the governing body and management for the effective and efficient governance of ICT to ensure that they support the strategic objectives of the organisation. In support of the creation of awareness, King III provides specific principles and practices that should be achieved and executed within a “comply or explain” regime12 by the governing body and management.

COBIT 5

COBIT 5 is a comprehensive business framework that follows a holistic (top-down and bottom-up) approach to assist organisations in achieving their objectives for GEIT.13 It focuses on the pervasiveness of ICT, the increasingly important role ICT plays in improving quality of information and generating value from ICT expenditure. The governing body and executive management need to embrace ICT as they would any other asset/resource of business.

Comprising five principles and seven enablers, COBIT 5 creates awareness of the importance of implementing CGICT in support of strategic goals at all levels of an organisation. It provides a comprehensive and adaptable framework of governance and management processes, allocating responsible, accountable, consulted and informed (RACI) roles as well as a facilitative implementation guide.

COBIT 5 also supports the adoption of ISO/IEC 38500’s principles and implementation approach.14

INFLUENCE OF INTERNATIONAL LEADING BEST PRACTICES IN THE DEVELOPMENT OF CGICTPF

King III and ISO/IEC 38500 provide primarily top-down approaches for the implementation of CGICT. COBIT 5, on the other hand, follows a combined approach. A combination of these best practices guided the holistic approach followed in the CGICTPF.

Layered Governance Model

Although generic, the best practices for CGICT focus primarily on the private sector. They refer to governing bodies as the board of directors and organisational management, implying a two-layer approach. King III, ISO/IEC 38500 and COBIT 5 agree that the ultimate accountability for corporate governance of ICT lies with the board. The equivalent of this had to be defined in the South African Public Service context.
On a Public Service-wide, holistic level, Parliament and Cabinet fulfil the role of the governing body, whilst within the individual departments, each with its own mandates and governance structures, the executive authority (minister) provides political leadership and the head of department and executive management (heads of branches within departments) provide the strategic leadership. This complexity required a three-layer approach in the CGICTPF:

- **Political governance of ICT**—Public Service-wide strategic direction is provided, and monitoring and evaluation are performed.
- **Corporate governance of ICT**—Departmental political and strategic leadership provides contextual strategic direction, monitoring and evaluation.
- **Governance of ICT**—Strategic management and management within the department (business owners, including the government IT officer) govern the delivery of ICT service and monitor its delivery.

Currently, most departments treat the ICT function as a technical entity and do not govern it as an asset to add value to service delivery. Its governance is not embedded in the corporate governance systems within the three levels. The CGICTPF facilitates the institutionalisation of CGICT on these three levels.

**Governance and Management Model**
ISO/IEC 38500 establishes a model for the governance of ICT, which describes the evaluating, directing and monitoring tasks of the governing body. This model was adapted to reflect CGICT from an external, Public Service-wide political, prescriptive and oversight environment to a departmental, internal context, depicting the total value chain.

**Accountability Framework**
Due to the history of the apparent disconnect between political and strategic leadership and the ICT function in departments, it was concluded that King III should comply with or explain the system of governance with no significant results in departments. King III, however, alludes to the allocation of accountability and responsibility to both the board and organisational management. The required results in the South African Public Service can be achieved only in a compulsory compliance regime within the ambit of the Public Service Act and Regulation; therefore, an accountability framework was created that allocates specific principles, with their related practices, to the political and strategic leadership of departments.

**Principles and Practices**
ISO/IEC 38500, King III and COBIT 5 demonstrate the concept of governance principles to achieve a specific outcome. ISO/IEC 38500 provides principles and describes practices as necessary for successful implementation of CGICT, whilst King III allocates specific accountability to the board through specific principles and related practices.

COBIT 5 is based on principles and incorporating enablers, and also provides comprehensive governance and management processes and related practices, which provide guidance for the implementation of CGICT. The CGICTPF principles and practices were derived from these best practices, with the political and strategic leadership of a department being accountable for their implementation.

The principles address political and strategic mandate, CGICT, business and ICT strategic alignment, ICT expenditure, risk management and assurance, and organisational behaviour. The practices provide for the execution of the principles by allocating specific accountability, roles and responsibilities to the political and strategic management. The practices also allude to vertical sector mandates in which the mandate of executive authorities transcends into relevant business, provincial and local government.

**Governance and Management Systems**
ISO/IEC 38500 and principle five of COBIT 5 require separate governance and management systems for CGICT. The CGICTPF is a governance framework and does not create context for a management system. The latter will be addressed in the pursuant implementation guideline, which will be derived from the COBIT 5 management processes.

**Implementation Approach**
The generic implementation guidance of ISO/IEC 38500 and COBIT 5 confirmed the importance of developing an implementation guideline for the CGICTPF. Therefore, the CGICTPF provides specific implementation guidance on how departments should create an enabling environment through a CGICT policy and charter, developing and implementing
related policies and coordinating governance functions. Departments are further expected to perform business and ICT strategic alignment and achieve continuous improvement. The CGICTPF contains specific timelines within which each of these must be achieved.

STRENGTHS AND OPPORTUNITIES
No other case studies could be found where these international best practices were collectively and selectively adapted to a public service/federal government context. Thus, the DPSA had to develop a tailor-made CGICTPF. However the CGICTPF does not re-invent the wheel. Where applicable, it draws on the strengths of each of the leading international best practices. It spells out what should happen, how, when and by whom, thus providing specific guidance.

Extensive knowledge of the organisational environment is required for the development of a framework of this magnitude. In the South African Public Service, this knowledge base was available internally.

The CGICTPF is a flexible, holistic approach and creates a governance regime that spans all three levels of governance of ICT required in the South African Public Service. The CGICTPF follows a top-down approach from Cabinet and Parliament, the political governance of ICT, to political and executive leadership, at which point the executive authority for a department is accountable.

A principle-based accountability structure according to which the political and strategic leadership of departments must integrate the CGICT into their unique governance systems is provided. Furthermore, the policy framework provides practices to cascade the implementation of the governance principles, a timeline for their implementation, as well as context for a standard against which conformance and performance are measured.

As research/case studies on the CGICT in the governance regimes of governments of developing countries are lacking, it is anticipated that South Africa is the first public service to implement holistic CGICT. The CGICTPF could easily be adapted for governments of other developing countries.

WEAKNESSES AND THREATS
Political support of the CGICTPF has not been tested as it is not yet approved by Cabinet. A lack of political will and drive would seriously impact the Public Service-wide implementation of CGICT.

The acceptance of and commitment to the implementation of the CGICTPF at the political and strategic leadership level in a department may place obstacles in the department’s road to conformance.

The political and strategic awareness of and buy-in to the CGICTPF and its related change management may delay the implementation process and may cause departments to miss implementation timelines.

The CGICTPF does not contain governance and management processes for implementation. It does, however, indicate that the implementation guideline provides guidance to the departments on the minimum set of COBIT 5 processes that should be implemented. The implementation guideline is still in development, thus the processes to be focused on have yet to be finalized.

CONCLUSION
CGICT is not a new subject and is addressed by international best practices such as King III, ISO/IEC 38500 and COBIT 5. Individually these best practices did not sufficiently address the context of CGICT for the South African Public Service; however, collectively they provided a holistic approach and strong foundation for the development of the CGICTPF. The CGICTPF creates Public Service-wide and departmental context for the political and strategic leadership of ICT through principles, practices, a governance model and an implementation approach.

ENDNOTES
1 Institute of Directors Southern Africa, King Report on Governance for South Africa, South Africa, 1 September 2009
3 Op cit, Institute of Directors Southern Africa, 2009
5 Department of Public Service and Administration (DPSA), Draft Public Service Corporate Governance of Information and Communication Technology Policy Framework, internal document, South Africa, 1 March 2012
6 Department of Public Service and Administration, Public Service Act 103 of 1994, South Africa, 1994
The DPSA is the policy department for inter alia ICT in the South African Public Service (all national/provincial departments).

8 *Op cit*, DPSA, 2012


10 *Ibid*.


12 *Ibid*.

13 *Op cit*, ISACA, COBIT 5

14 *Ibid*.

15 The Auditor General of South Africa, ‘Status of the governance of information technology in government’, Letter from the Auditor General to the Department of Public Service and Administration regarding the information systems review of the governance of information technology in government, unpublished, 28 May 2010


17 Department of Public Service and Administration, *Electronic Government Regulations* (as amended), South Africa, 5 January 2001


22 ISACA, *COBIT 5: Implementation*, USA, 2012, p. 10

---

**Simplify your search with ISACA’s newly enhanced Career Centre.**

**Don’t get lost** in your quest for a job.

Explore the ISACA Career Centre Today:

[www.isaca.org/careercentre](http://www.isaca.org/careercentre)
Creating the Business Case for ERP System Acquisitions Using GEIT

Many organizations choose to acquire an enterprise resource planning (ERP) system to serve as a common system for their wide range of daily operations.

Various business benefits can be realized from ERP investments due to operational performance improvements. For instance, ERP systems embed industry best practice processes, which enterprises can leverage to achieve a discontinuous improvement in performance.

However, many ERP investments fail to deliver on their promised benefits due to deficient ERP investment appraisals caused by inflated expected benefits and underestimated cost and risk. Therefore, improved governance of enterprise IT (GEIT) in general, and governance of ERP system acquisitions in particular, are crucial for success. One of GEIT’s key practices is the development, maintenance and utilization of a proper business case throughout an investment’s economic life cycle.1

What are the key elements of an ERP investment business case, and which GEIT best practices are relevant? Furthermore, do such practices resonate with management and finance best practices, which are expected by executive business leaders who control access to funds?

The business case is a core concept in successful GEIT practices. It is intended as a tool for decision making on investment matters, both prior to and after initiating an investment. It is often captured as a document or presentation, and it is heavily promoted in Val IT®, COBIT® 53 and the Certified in the Governance of Enterprise IT® (CGEIT®)4 certification.

For example, Val IT’s Investment Management domain and processes require an enterprise to develop and evaluate the initial program concept business case (practice IM1) and to update the business case (practice IM8).5, 6 Furthermore, COBIT 5 continues to promote business cases to ensure benefits delivery (process EDM02), to manage enterprise architecture (process APO03) and to manage portfolio of investments (process APO05).7 Finally, domain three of CGEIT confirms that business cases are part of the GEIT practice.8

What is important to include in a business case? One answer is offered in ISACA’s eight-step approach for business case development (figure 1).9 In particular, steps three, four and five require the analysis of an investment’s expected benefits, resource and cost requirements, and associated risk. While nonfinancial benefits might be difficult to quantify, better developed business cases include well-quantified benefits, costs and risk, hence enabling superior ERP investment appraisals.

Therefore, the key elements of a business case are the benefits, costs and risk. Once established, the investment can be appraised (figure 2).
The Benefits

Various benefits can be expected from a successful investment in an ERP system. Ultimately, however, it is the investing organization that must determine which business benefits it can realize from such investments based on its own strategy and objectives. The following is a summary of common benefits.

Many organizations that do not have a proper ERP system are structured functionally, which leads to the proliferation of functional and silo IT systems. Others follow an organizational design that focuses on end-to-end business processes spanning across functions. In the latter, ERP systems can improve information exchange across functional systems. They are designed with an end-to-end perspective to significantly increase efficiency over silo-functional applications, thus removing manual coordination requirements for exchanging information across functional systems. The promised business benefit is optimized enterprise performance.

Consequently, an ERP system’s database integrates and unifies information from various functional capabilities. For example, a master list of vendor names would be created, as opposed to duplicate lists in purchasing, logistics and finance. This integration and unification of information allows an organization to have a single source of truth, which is the foundation for business intelligence (BI) and analytics. A McKinsey Global Institute report pronounced analytics as “the next frontier for innovation, competition and productivity,” and Thomas H. Davenport, a BI and analytics pioneer, emphasized that applying analytics on business processes, such as those provided by an ERP system, is one of the last remaining ways for organizations to achieve differentiation and competitive advantage.

Another common business benefit of ERP systems is the enforcement of standard processes across the organization and its geographically dispersed sites. Process standardization is a prerequisite for continuously improving process performance and organizational efficiency, on both IT and the business sides, as advocated by Shewhart’s Plan-Do-Check-Act cycle and frameworks such as COBIT 5, IT Infrastructure Library (ITIL) and Capability Maturity Model Integration (CMMI). Furthermore, the standardized processes can be provided by the ERP system out of the box; these standardized processes are designed based on best practices obtained from many successful organizations. The organization acquiring an ERP system should adopt such best practices through business process reengineering (BPR) for all of its processes, except those that provide it with a competitive advantage.

The Costs

Despite the many potential benefits that ERP systems promise, they come at a significant acquisition cost. ERP system licenses are generally more expensive relative to other systems, the corresponding ERP acquisition project includes many diverse activities, and ERP system deployment by itself is costly due to the large user base and likely resistance to change.

A consequence of adopting best practice processes in ERP systems is that ERP investments almost always require existing business processes to be reengineered. This can disrupt operations and, therefore, requires effective organizational change management. Conversely, customizing the ERP system, instead of performing organizational BPR, is also a costly activity due to the system complexity and impact on future software upgrades.

Migration from multiple functional systems also comes at a cost. It is likely that information duplication will exist due to the proliferation of silo-functional systems. As the inconsistency of data models across these systems increases, more effort will be required to cleanse the data and then migrate it to the new ERP system. The paradox here is that the larger the organization, the more likely it is to acquire an ERP system. However, larger and more complex organizations are also more likely to have a larger number of ERP systems and higher data fragmentation across them due
to decentralization and localization needs and to maintain specific competitive advantages by seeking a best-of-breed approach. Therefore, the cost of ERP system acquisition increases at a nonlinear rate.

Additionally, ERP deployments may require newer and/or more capable IT assets, such as new servers and software. Such supporting hardware and software infrastructure can be expensive, and it increases architecture work and acquisition cost.

THE RISK

Activities such as BPR, customization and data migration can be complex and risky. For example, BPR can result in resistance to change, as discussed previously. Resistance to change continues to introduce risk areas for ERP acquisitions.

Risk must be appropriately identified and managed, and a business case should not be completed until there is a proper understanding of the investment’s risk. There is risk associated with different IT service and system life cycle stages (e.g., planning, implementation, project closure, transition to operations, operations, retirement). Risk associated with all of these life cycle stages is relevant and should be considered when preparing the business case and determining the risk-adjusted required return. In essence, as finance theory advocates, investors must demand higher investment returns for increased investment risk.

Risk must always be defined from a business perspective. Thus, an organization looking to acquire an ERP system should define the specific risk relevant to it. Furthermore, Risk IT’s Risk Evaluation (RE) process activity 1.4 requires the identification of risk contributing factors, which are drivers of the frequency and magnitude of risk events. These are important for root-cause analysis of risk, which is also emphasized by other frameworks and models such as the Committee of Sponsoring Organizations (COSO) Enterprise Risk Management—Integrated Framework and CMMI’s Causal Analysis and Resolution (CAR) process area. Furthermore, not only does understanding risk factors help better mitigate risk due to improved root-cause analysis, but it also helps quantify any necessary contingency funds required for residual risk, and to quantify the required return or discount rate for projected cash flows.

Fortunately, risk factors are common across ERP system acquisitions, as determined by examining successful and failed ERP acquisition cases. These risk factors were identified by examining actual ERP acquisition cases, for example, as reported in quantitative case studies, qualitative case studies and expert opinions. Figure 3 provides a summary of the top 10 risk factors for ERP investments.

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Factor</th>
<th>Corresponding Areas of Concern</th>
</tr>
</thead>
</table>
# Risk Factor | Corresponding Areas of Concern
---|---
5 Independent consultants | Involvement of external experts. Their involvement throughout the life cycle. Their ERP and BPR project experience. Their soft skills, e.g., communication, professionalism. Their value-added expertise in relation to in-house experts. Their managerial support. Their technical support.
6 Healthy returns (including cost control and postimplementation performance measurement) | Validating the business case throughout the ERP life cycle. Establishing key performance indicators (KPIs), including benefits realization KPIs. Calculation of return. Proper user awareness and training on ERP system. Close tracking of implementation costs. Consideration of all project risk factors. Early establishment of an ERP vision.
7 Level of customization | Limiting customization to must-have advantages. Leveraging best practices from standard processes in the ERP system.
8 Human resources (HR) development (IT staff and users) | User training and documentation on ERP system. IT staff training on ERP system maintenance and support. Including all employees in ERP implementation. Refraining from using the ERP system to reduce employee headcounts.
9 Managing expectations | Establishing realistic expectations. Managing stakeholder expectations. Alerting top management to ERP system complexity, associated risk and possible complications.
10 IT infrastructure | Consideration of existing IT infrastructure. Proper IT infrastructure with a proper budget. Integrity of existing databases.

### Figure 4—Relative Importance of Various ERP Risk Factors

![Relative Importance of Various ERP Risk Factors](image)

**Figure 4** illustrates the relative importance of these risk factors.

Understanding these risk factors should significantly aid the governance of ERP system acquisitions and the development of relevant business cases, including the allocation of contingencies for residual risk.

**THE APPRAISAL**

Once benefits, costs and risk are quantified and analyzed, an ERP investment can then be appraised.

The net present value (NPV) is considered by many as the most appropriate investment appraisal method. It is advocated by corporate finance gurus and is illustrated in step three of the business case development approach from ISACA. ING, for instance, has used NPV in appraising IT-enabled investments. NPV’s advantages are a result of utilizing discounted incremental cash flows rather than forecast profits, which are used in the book rate of return and payback period methods. Discounted incremental cash flows are more realistic because forecast profits are dependent on the company’s accounting methods. Furthermore, the payback period is biased against long-term investments.

Identifying incremental cash flows is about identifying the difference in cash flows for the organization when accepting the investment and rejecting it. In accordance with Val IT’s principles and its investment management processes, such as IM4 (Develop full life-cycle costs and benefits), incremental cash flows should be those incurred during the investment’s full economic life cycle, thus including system acquisition, operation and retirement costs. Costs correspond to cash outflows whereas benefits correspond to cash inflows. Therefore, quantifying benefits and costs is required to perform an appraisal using NPV.
Cash flows must include the full scope of activities required to achieve business value, and these may come in many forms. Figure 5 identifies and explains rules\(^33\) for identifying cash flows when applying the NPV investment appraisal method. These rules should be used as a checklist whenever the NPV method is used. For instance, an unused server capacity or idle IT operations staff that will be utilized to operate an ERP system will have an opportunity cost, which must be reflected as a cash outflow. Just because they are currently available does not mean that they should be ignored.

Each cash flow is then discounted from the future period in which it will be realized back to the present date of the decision (e.g., year zero or today). The factor by which those future cash flows are divided to achieve present value is a function of the “discount rate.” It reflects the cost of capital and uncertainty in future cash flows as reflected in the investment’s risks. In essence, a higher discount rate is used for riskier investments because contingency is built into the discount rate. This can be viewed from the perspective that higher returns are required from riskier investments and, therefore, is consistent with the concept described as risk-adjusted return in the CGEIT Review Manual.\(^34\)

Finally, the discounted cash flows (DCFs) in present values at year zero are then summed to arrive at the investment’s NPV. With other strategic and nonfinancial factors being constant, a firm should accept an investment if it has a positive NPV and reject it if it has a negative NPV. In practice, however, numbers do not tell a complete story, and the NPV value is not the sole determinant of decision making over investments. Step four in ISACA’s business case development method clearly states that nonfinancial benefits must be identified and considered as part of an investment’s appraisal.\(^35\) Managerial judgment is necessary.

**CONCLUSION**

It is a reality, IT must be run and, therefore, governed and managed as a business.\(^36\) Management is running out of excuses for accepting investments that do not deliver on promised

<table>
<thead>
<tr>
<th>Rule</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Do not confuse average with incremental payoffs.</strong></td>
<td>Any cash flows assigned to the investment should be calculated on an incremental basis. This equals the difference between cash flows if the firm accepts or rejects the investment.</td>
</tr>
<tr>
<td><strong>Include all incidental effects.</strong></td>
<td>Many investments are related; therefore, accepting an investment may increase or decrease cash flows for other investments. In such a case, the differences must be accounted for in the cash flows. This is particularly important as an ERP investment often aims to retire several fragmented legacy systems, thus contributing to a cash inflow by reducing cash outflows, such as maintenance costs, for the legacy systems.</td>
</tr>
<tr>
<td><strong>Forecast sales today, and recognize after-sales cash flows to come later.</strong></td>
<td>An organization should recognize that it normally would sell items and later provide paid support. For example, an IT department may sell ERP services to the business and follow it with a pay-per-use support model. Cash flows resulting from both should be included in the analysis.</td>
</tr>
<tr>
<td><strong>Do not forget working capital requirements.</strong></td>
<td>Working capital is the difference between current assets and current liabilities. In other words, it equals the cash necessary for the firm to prepay its bills until it actually receives revenue for the services it provides.</td>
</tr>
<tr>
<td><strong>Include opportunity costs.</strong></td>
<td>Sometimes an organization may already have resources that can be used for the investment. For example, an IT organization may already have IT operations staff members who can operate and maintain the ERP system. Nevertheless, their cost is not free; it is equal to the NPV that they provide if they were put to their other best alternative use. As a second example, unutilized IT infrastructure, such as server capacity, has an opportunity cost if used on a particular investment. The opportunity cost relates to the cost of utilizing it at its best alternative use.</td>
</tr>
<tr>
<td><strong>Forget sunk costs.</strong></td>
<td>Sunk costs are any costs already spent by the organization. For example, if an investment failed once and is restarted, past costs are considered sunk and are not included in the investment appraisal the second time. However, be careful not to ignore opportunity costs because assets from a previous failed investment might be utilized for other investments if not used in the restarted investment. The decision to accept or reject the investment does not change sunk costs.</td>
</tr>
<tr>
<td><strong>Beware of allocated overhead costs.</strong></td>
<td>Carefully consider overhead costs, such as HR support to IT. Only the difference in overhead costs should be assigned to the investment. Often, accepting or rejecting an investment does not change overhead costs, which means that they should not be assigned to the investment.</td>
</tr>
<tr>
<td><strong>Remember salvage value.</strong></td>
<td>Salvage value is the terminal value once the system terminates. For example, when the ERP system is retired, the company may be able to sell the software secondhand to another firm or department. If this is indeed a possibility, the salvage value would equal this value.</td>
</tr>
</tbody>
</table>
business benefits, require costs and require reactions to multiple unplanned risk incidents. Fortunately, the abundance of GEIT best practices can help.

In particular, the business case is an instrumental tool for appraising investments and managing them throughout their life cycles. An effective business case may be based on the NPV investment appraisal method, thus considering expected benefits, costs and risk. For ERP investments, general benefits and costs are understood, and there exist common risk factors. Understanding these common risk factors can guide an organization to better understand and manage ERP investment risk. Applying the NPV method, including an understanding of the expected benefits, costs and risk, is a common practice in the business and finance community. Not only can this approach aid IT professionals in performing better informed appraisals, but it will also help them better communicate with the business and finance community, which often controls access to funds. The end result, therefore, includes improved communication, business-IT alignment and benefits realization.

ENDNOTES
2 Ibid.
3 ISACA, COBIT 5, USA 2012, www.isaca.org/cobit5
5 Op cit, ISACA, 2008
7 Op cit, ISACA, COBIT 5, 2012
13 Shewhart, W. A., Statistical Method From the Viewpoint of Quality Control, Dover, USA, 1939
14 Op cit, COBIT 5, 2012
15 UK Cabinet Office, Information Technology Infrastructure Library (ITIL), UK, 2011
16 Software Engineering Institute (SEI), Capability Maturity Model Integration version 1.3, 2010
17 Kimberling, E.; The Case for and Against Using Multiple ERP Systems Across Your Organization, Panorama Consulting, 2012
20 ISACA, Risk IT, USA, 2009, www.isaca.org/riskit
22 Op cit, ISACA, 2009
23 Committee of Sponsoring Organizations (COSO), Enterprise Risk Management—Integrated Framework, 2004
24 Op cit, Software Engineering Institute
25 The author identified these risk factors as part of his wider practical case study research on GEIT and ERP system acquisitions, which also included risk management strategies for ERP system acquisitions.
27 Wong, A.; H. Scarbrough; P. Y. K. Chau; R. Davison; Critical Failure Factors in ERP Implementation, 2005
28 Kimberling, E.; Nightmare Continues, Panorama Consulting, 2010
29 Op cit, Brealey, 2008
30 Op cit, ISACA, 2006
32 Op cit, Brealey, 2008
33 Ibid.
35 ISACA, 2006
36 Innovation Value Institute (IVI), Information Technology Capability Maturity Framework (IT-CMF), 2012
William Emmanuel Yu, Ph.D., CISSP, CRISC, CSSLP, is the technology vice president at Novare Technologies and a consultant at SMART Communications. Yu is working on next generation telecommunications services, valued-added systems integration and consulting projects focused on fixed mobile convergence and enterprise mobility applications with mobile network operators and technology providers. He is actively involved in Internet engineering, mobile platforms and information security research. Yu is also a faculty member at the Ateneo de Manila University, Philippines, and Asian Institute of Management, Manila, Philippines.

BYOD Security Considerations of Full Mobility and Third-party Cloud Computing

Bring your own device (BYOD) is a growing trend. According to International Data Corporation (IDC), 40 percent of devices at work are personally owned. Understandably, there has been some push back, with a great deal coming from IT administrators particularly in terms of security and cost impact. For example, IBM defined policies blocking applications such as Siri and Dropbox because of potential information leakage and privacy concerns. But when IT managers restrict BYOD liberties, usage is driven underground. In a study by SkyDox in 2012, 60 percent of users use free file-sharing applications and 55 percent of these do not report such usage to their IT departments. VisionCritical also states that 66 percent of young employees (20 to 29-year-olds) will circumvent anti-BYOD rules and 50 percent will install and use their own applications—whether for work or play, users want to use their own devices and their own applications—whether an organization allows it or not. Thus, it is better for organizations to address this in a structured manner within their overall IT governance context.

In an earlier BYOD era, some organizations allowed employees to bring their own laptops and notebooks to the workplace and/or supported teleworking—allowing employees to bring corporate laptops and notebooks outside the office. Today, with the advent of smartphones (full mobility as opposed to nomadic laptops and notebooks) and cloud computing, additional concerns have emerged that need to be considered.

IT departments and professionals must reassess current actual usage and find a new balance between user preferences, organizational needs and information security requirements. With respect to BYOD, this should be no different. This article details additional BYOD security concerns that emerge when considering greater mobility and third-party cloud computing.

MOBILITY CONSIDERATIONS

Smartphones and other full-mobility devices, such as tablets, are becoming more and more pervasive. Due to the wide range of choices, greater functionality and potential for improved productivity, users increasingly feel it is their right to use their personal mobile devices at work. However, this usage raises a number of additional concerns that are not usually considered when dealing with BYOD in the context of laptops and notebooks:

- **Clearly defined platform support**—Unlike notebooks and laptops, full-mobility devices are much more diverse in terms of operating systems, chipsets and platforms. This fragmentation makes it more difficult to craft rules that cover this broader range of devices. Fortunately, the industry is converging on a few common platforms—Android, iOS, RIM and Windows Phone. Compared to feature phones, these common platforms present IT managers with a smaller set on which to target BYOD support. IT departments need not certify each and every device, but they do need to cover certain representative sets. With a fixed set of platforms, employers can now design programs to ensure that information security risk is managed. The first step is to be aware that today’s full-mobility devices have much more fragmentation than laptops and notebooks. Next, administrators should profile commonly used full-mobility device platforms to roll out their BYOD programs. They cannot and do not have to support all platforms on day one.

- **Stolen, misplaced and disposed devices**—There have been numerous cases where devices containing confidential information (such as customer and credit card data) have been misplaced or stolen, resulting in potential data loss. When employees use their personal devices for work, there will certainly be work-related information on those devices. Access to these devices by unknown or unauthorized...
Recipients will give those recipients access to potentially sensitive and confidential information and infrastructure. Mobile devices tend to be more readily misplaced or stolen, compared to larger laptops and notebooks or bolted-down desktops. The replacement cycles of mobile devices also tend to be shorter—from every two years to every six months in certain markets, as opposed to the usual three-to-five-year cycle for notebooks and laptops (raising the issue of proper wiping and deactivation prior to disposal). The following measures may be considered: real-time remote locking, data wiping and device tracking. Application and service access revocation should also be considered, as mobile access to corporate resources typically has stored and cached credentials. This functionality is possible since even lost devices can still be connected to the corporate network. Additionally, device bricking* should be considered because mobile devices, even with their data wiped, might still have access to sensitive corporate resources.

- **Mind the transport**—With any deployment that provides remote access to corporate resources, there is a need to ensure that the transport layer is secured. It is not sufficient to rely on interface security. Transport layer security (TLS) is best end to end. People tend to use applications such as Short Message Service (SMS) that may not provide the necessary level of security. Corporate access via mobile sites may not have the necessary TLS/Secure Sockets Layer (SSL) security. In laptops and notebooks, there is a tendency to look at virtual private networks (VPNs) as the catch-all security solution for providing secure transport to remote corporate resources. However, while VPNs may also be used in the mobile context, these are less popular and may not cover all applications. The comfortable familiarity of VPN use can potentially give users a false sense of security. This is particularly true in mobile VPNs, in which all traffic is not automatically routed into the VPN tunnel. Users may assume that they have logged on to their mobile VPN client and may not realize that their SMS traffic is not subject to that (their organization’s) security. Another set of concerns includes home routing* and legal intercept capabilities of network operators. This means that all the user’s data traffic is visible to his/her home provider. Unlike with the Internet, traffic is generally routed to the user’s network provider. It is necessary, therefore, to ensure that the applications that allow users to store and process corporate information on mobile devices secure their own transport.

- **Implicit authentication**—Most common remote applications today are designed with explicit identification and authentication mechanisms (e.g., user name/password, on-time password (OTP) tokens, biometrics). These make access to corporate information explicit. In the case of mobile devices, some applications use implicit security such as SIM-based Extensive Authentication Protocol (EAP) authentication and Generic Bootstrap Architecture (GBA) methods. Implicit authentication is typically used by most mobile phone services. A consideration is that users may allow other people to use their mobile devices without thinking that this also provides access to applications that use implicit authentication. Explicit authentication can succeed in becoming implicit authentication by saving explicit authentication tokens in mobile devices. This makes succeeding authentications implicit. It is likewise important to recommend the use of device locks and pass phrases because of the large amount of implicitly authenticated applications and services used in mobile devices.
• **Always on and always online**—Full mobility devices are typically always connected to a network and always powered on. Therefore, these devices are always reachable and additional security controls can be introduced. Some of the features mentioned previously, such as remote wiping and management, are possible. It is also possible to track these devices in real time, allowing organizations better visibility of devices and allowable zones of operation.

**THIRD-PARTY CLOUD SERVICES CONSIDERATIONS**

The earlier generation of BYOD rules already considered network-based services when they were drafted for laptops and notebooks. In addition, organizations have put in place teleworking rules for employees to bring their equipment home and use these to access network-based assets. However, there are additional considerations when these network services are hosted and controlled by third parties:

• **Choose applications wisely**—It is clear that certain applications can be used to potentially leak corporate information. For example, a mobile phone with a location-based service (LBS) application may be used to track the comings and goings of a key employee. This information might then be used to gain corporate insight. Another case is photo-sharing applications, which may accidentally leak information within photos that are shared. Some applications leak more data than others. Each organization must make a customized assessment regarding the interaction of leak-prone mobile applications within their specific corporate environment.

• **Determine tolerance for keeping data in the cloud**—An organization may want to determine its tolerance for having data stored in the cloud. For plain storage requirements (e.g., Dropbox), it is possible to use security measures (such as encryption and digital signatures) at the organization’s end to keep data secure while stored in third-party locations. For services such as cloud-based office productivity applications and electronic mail services, the data are clearly available to the cloud provider. If the organization does not want corporate information to be stored and potentially available to a cloud provider, these types of services should not be used. Putting data into a third-party facility always introduces a potential for confidentiality violations—whether intentional (e.g., theft or cracks) or unintentional (e.g., leakage). The organization should review the regulatory environment (e.g., Payment Card Industry Data Security Standard [PCI DSS], the US Health Insurance Portability and Accountability Act [HIPAA]) to ensure that using these types of services is allowed and compliance with any special regulatory requirements is maintained. Organizations must review the regulatory environment in which the cloud provider operates, as it may have requirements or restrictions of its own (e.g., legal intercept). Organizations must then determine if the cloud provider provides appropriate controls to ensure that data are appropriately secure.

• **Ensure service opt out**—An organization may eventually wish to discontinue its service with a third-party cloud-based provider. The organization would then want to remove its data from the system and ensure that the service provider clears the system (including any backups) of its data. Some providers do not offer automated or bulk data withdrawal mechanisms, which the organization needs to migrate its data. These aspects should be clarified prior to using a third-party provider.

• **Read the fine print**—Organizations must carefully review their contracts with third-party cloud providers. Specifically, considerations such as service level agreements (SLA), data ownership, third-party access, withdrawal, backup/archiving/restore and management should be reviewed. Organizations may find that some of the terms are not favorable to them. In the case of data ownership, some service providers reserve rights to access customer information in order to perform certain transactions and provide certain services. It is also good to determine if backup, archiving and restoration services are available. An organization may need to plan its own data recovery processes and procedures if the service provider does not make this available or it has doubts about the service provider’s processes (see figure 1).
Figure 1—Recovery Processes

<table>
<thead>
<tr>
<th>Processes</th>
<th>Old BYOD</th>
<th>New BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms targeted</td>
<td>Laptops and notebooks</td>
<td>Mobile devices, e.g., smartphones, tablets</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Nomadic (on-demand connectivity)</td>
<td>Full mobility (always on/always online)</td>
</tr>
<tr>
<td>Network used in services</td>
<td>Own network</td>
<td>Third party/cloud</td>
</tr>
<tr>
<td>Data storage</td>
<td>Own infrastructure</td>
<td>Third party/cloud</td>
</tr>
<tr>
<td>Authentication</td>
<td>Explicit</td>
<td>Implicit</td>
</tr>
<tr>
<td>Common security mechanism</td>
<td>VPN</td>
<td>Case-to-case, per application</td>
</tr>
<tr>
<td>Range of operating systems</td>
<td>MS Windows, Linux, Mac OS</td>
<td>Google Android, Apple iOS, RIM BlackBerry, Microsoft Windows Phone, HP PalmOS, Tizen, Samsung Bada, Nokia Symbian</td>
</tr>
</tbody>
</table>

CONCLUSION
The key solution here is to find a balance between what the user wants and what the organization needs. Both users and organizations stand to benefit from BYOD. In many cases, organizations do not even have rules for BYOD. For those who do have BYOD or teleworking rules, many of these rules may be dated, as they were designed for laptops and notebooks. These rules must be updated to apply to mobile and third-party, cloud-specific considerations. Nevertheless, BYOD, in this era of full mobility and cloud computing, can bring benefits to organizations, but they need to establish appropriate security mechanisms based on IT governance and manage them well.

ENDNOTES


7 Messmer, Ellen; “Young Employees Say BYOD a ‘Right’ Not ‘Privilege’,” Comm Solutions, 19 June 2012, www.commsolutions.com/blog/2012/06/young-employees-say-byod-a-right-not-privilege/

8 Occurs when the firmware or BIOS has been corrupted or when hardware has been improperly installed; it will render the device unable to boot. Urban Dictionary, www.urbandictionary.com/define.php?term=Brick&defid=2189251

9 Home routing refers to the act of sending the message to an element in the network instead of the message going directly to the subscriber. The concept expands beyond SMS to voice and data traffic. 3GPP, TR 23.840, www.3gpp.org/ftp/Specs/html-info/23840.htm

10 Op cit, Darrow

Effective implementation of IT governance in the business units of an enterprise involves the process of institutionalization (e.g., changes in culture and behaviors of people), to use the processes, tools and metrics. Many times, IT governance implementation fails due to ineffective institutionalization. Quite often, the root cause can be traced to lack of business-unit executive buy-in. Therefore, a critical success factor is earning buy-in from business-unit executives. This article discusses the essential process of formulating and presenting practical business cases to executives to increase chances of earning buy-in from business-unit executives.

Implementation of IT governance in an enterprise’s business units is no easy task. There are many strategies and tactics necessary to change the culture and behaviors of people for the usage of processes, tools and metrics. Most of the time, IT prepares business cases using a standard company template and converts them to slides for presentation. It is no wonder that the end result is a failure of the business-unit executives to understand the scope of the effort and a negative response.

Business case presentations need to clearly communicate the scope, be easily understood by business executives and be presented in an hour-long meeting. As such, the presentation needs to focus on the following points:1

- Organization or business-unit goals
- Pain points of the business units in meeting these goals
- Implementation strategies and tactics
- Cost and schedule
- Benefits
- Metrics
- Success stories
- Presentation technique

The following steps outline a process to determine the strategies, tactics, benefits and metrics to formulate and present effective business cases:

1. **Develop initial strategies and tactics**—Similar to any transformational change or process-improvement initiative, business-unit strategies and tactics should be developed along the three dimensions of the people, processes and tools (PPT) triangle.2 Developing the strategies and tactics along the three dimensions ensures an adequate balance in the system (e.g., people need to be trained to use processes that are enabled by tools). The reason is that if any one dimension is not in alignment with the others, the system as a whole becomes unbalanced and fails. Along with developing the people, processes and tools related to strategies and tactics, developing metrics such as key performance indicators (KPIs) and key goal indicators (KGIs) to measure, monitor and validate the achievement of strategies and tactics is also a must.

   People-related strategies can include training, communication and awareness sessions; capability levels; mentoring; and quality support. Process-related strategies can include process training, process compliance audits, tailoring and augmenting processes, building process repositories, and providing process support. Tool-related strategies can include tool deployments, tool training and tool usage audits. Appropriate metrics (KPIs and KGIs) should be selected to measure and monitor the progress and critical success factors (CSFs).

2. **Implement Hoshin Kanri planning**—After the initial PPT strategies and tactics are developed, they need to be refined and aligned with the organization’s strategies and communicated to all business-unit staff. Hoshin Kanri planning is a useful process in carrying this out. Also called Policy Deployment,3 this is a strategic planning/strategic management/strategic control methodology based on Deming’s Plan-Do-Check-Act (PDCA) cycle. The purpose is to communicate and spread awareness of the organization’s vision, goals, KPIs and CSFs to

---

**Rajesh Bhatia, CISA, CGEIT, PMP, MDP,** is currently the supply chain business process owner at Safeway Inc. in Pleasanton, California, USA. Previously, Bhatia worked as senior manager of strategic demand management at CSC, where he was involved in institutionalizing demand management processes, tools and metrics in the health care accounts.
all levels to ensure that the business units and staff at all levels do the following:

- Plan, develop and align tactics based on the strategic intent of the organization as well as other business units.
- Act on and validate the achievement of goals, KPIs and CSFs.
- Provide feedback for continual improvement.

The Policy Deployment X Matrix tool can be used to implement the Hoshin Kanri Planning technique. Use of this tool ensures the alignment of business-unit strategies, tactics and metrics to the organization’s goals or objectives. The tool is a spreadsheet with objectives, action programs (or strategies), action items (or tactics), and measures and targets along the four sides of a square and a RACI chart on the right. There are grids in the four quadrants where “X” can be entered to show correlation between the following:

- Objectives and measures and targets
- Objectives and action items (tactics)
- Measures and targets and action programs (strategies)
- Action programs (strategies) and action items (tactics)
- Action items (tactics) and RACI charts

The tool has been found to be extremely useful for ensuring that the strategies cover all objectives, there are adequate and correct tactics for the strategies/action programs, and sufficient metrics are present to measure the objectives and progress of strategies/action programs.

4. **Summarize the cost and schedule**—A question that is always asked when business cases are presented is the cost and schedule of institutionalization activities. It is critical to provide the summarized cost and schedule with milestones, because executives frequently base their decisions on this information. A very high cost and lengthy schedule is more likely to result in a negative response due to business-unit funding and budget issues. Therefore, it is important to appropriately plan the IT governance implementation activities and tailor them to the business-unit needs so that a realistic and achievable cost and milestone schedule is presented to the business-unit executives.

5. **Present the business benefits**—While presenting business cases, questions frequently surround the benefits: What are the benefits? When will they be realized? How will they be measured and reported? Presenting benefits using a results chain model can be useful. A results chain model is a comprehensive and accurate model of an organization’s or business unit’s benefits realization process. Results chain diagrams map out a series of causal statements that link short-, medium- and long-term results in an if-then fashion. Using this model, the strategies, tactics and any assumptions can be linked to the intermediate and long-term benefits and goals in a visual manner. The model can
also visually depict the achievement of business benefits at that point in time. Thus, a results chain model is a great presentation tool and its usage greatly enhances the presentation.

6. **Present the measurement and reporting plan**—Executives also want to know how the business benefits will be monitored, measured and reported. Presenting the metrics and the measurement and reporting plan is important. It is critical to select the correct metrics, those that will demonstrate the progress of meeting the goals. Planning using the Policy Deployment X Matrix certainly helps in arriving at metrics that are aligned to the business-unit goals, strategies and tactics. It is also important to stress metrics analysis, development of an improvement plan and tracking of corrective actions for continual improvement.

7. **Relay success stories**—Relaying success stories, if available, reinforces the business case authenticity and practicality. If the business-unit executives agree with the contents but do not want to move ahead due to questions on practicality, relaying success stories can be a game changer.

8. **Choose the appropriate presentation technique**—It is very important to match the delivery with the personality types of the executives. People are mainly of three personality types: visual, auditory or kinesthetic. Most executives tend to be visual, which means the business case needs to be delivered at a good pace, while focusing on the big picture. But sometimes, it may be necessary to deliver the presentation to people who are of auditory or kinesthetic personalities. In these cases, it is necessary to deliver the business case at the pace and level that is easily understood by the audience. Not following this guideline can either lead to the business-unit executives getting frustrated (e.g., this would be the case if presenting at a slow pace or with a lot of detail to visual types) or not understanding the message (e.g., this would be the case if presenting at a fast pace and big picture to auditory or kinesthetic types).

**CONCLUSION**

IT governance implementation and institutionalization in enterprise business units is dependent on buy-in from the business-unit executives. Formulating strong and effective business cases is the most important factor in gaining buy-in. But it is not enough. Business case presentations should be done in a manner that clearly communicates the scope, is easily understood by business executives and can be presented in an hour-long meeting. Following the aforementioned steps ensures effective formulation and presentation of business cases, which, in turn, increases the chances of gaining buy-in for IT governance implementation.

**ENDNOTES**

1. This is based on the successful experience of the author in presenting business cases for IT governance.
3. Jackson, Thomas L.; Hoshin Kanri for the Lean Enterprise: Developing Competitive Capabilities and Managing Profit, Productivity Press, 2006
5. Thorp, John; DMR Center for Strategic Leadership; The Information Paradox: Realizing the Business Benefits of Information Technology, McGraw Hill, Canada, 1998
6. Ibid.
Today’s IT business environment requires regulatory compliance, cost control, availability, risk management, business alignment, timely project delivery, change and continuous innovation to deliver stakeholder value. Fulfilling these demands heightens pressure on boards and executives to ensure effective oversight of IT, making IT governance integral to overall corporate governance.

IT governance allows organizations to encourage desirable behavior when using IT. There are three key aspects:

• **What** are the essential decisions that must be made for effective management and IT usage (IT domains)?

• **By whom** should they be made (governance styles)?

• **How** will they be monitored to ensure control (mechanisms)?

Well-designed, well-understood and transparent governance mechanisms are critical. Building and maintaining these mechanisms forms a continuum (see figure 1) that requires desire for change, identification and accountability for required changes, and ongoing monitoring to ensure that the desired results are achieved.

**IMPLEMENTING IT GOVERNANCE**

Top-down IT governance addresses *what, who* and *how* IT decisions are made and acted upon.

---

**Figure 1—Integrated GEIT Implementation Life Cycle**

![Integrated GEIT Implementation Life Cycle Diagram](image)

- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

Source: ISACA, COBIT 5, USA, 2012, p. 37
Conceiving the governance model (the what, who and how) is the first step. Implementing it is the second step, and this can be accomplished with a seven-phased approach:

• **Phase 1: Initiate program**—What are the drivers? The impetus for IT governance is a desire for change that stems from the strategic plan of the business, from which the IT strategic plan is derived. This requires obtaining ownership at the board and executive level, establishing initial awareness and involvement of business and IT management, and establishing an IT governance project organization.

• **Phase 2: Define problems and opportunities**—Where are we now? The next step is to assess existing IT governance processes (as-is situation assessment) and identify problems and opportunities. At this point, a team should be identified and charged with detecting problems and opportunities in later phases.

• **Phase 3: Define road map**—Where do we want to be? Based on the results of the as-is assessment, the focus moves to defining what an ideal IT governance model should look like (e.g., IT is an essential part of strategy, IT’s business impact is measured and monitored, IT is viewed as a strategic business asset and managed as a portfolio, IT participates in technology investment decisions, and IT has board-level oversight and executive leadership). The outcomes of the definition process should be communicated to business and IT leaders, and an implementation road map established.

• **Phase 4: Plan program**—What needs to be done? The IT project work commences in this phase by establishing effective governance. This includes identifying people and groups to be involved (and their level of involvement), such as the IT steering committee, the IT project steering committee and the chief information officer (CIO). In addition, an IT project governance methodology, IT portfolio management, budget control and reporting standards are established.

• **Phase 5: Execute plan**—How do we get there? Obtaining the participation of the business is paramount, and can often be greeted with resistance. Accordingly, it is critical to focus on relational and change management mechanisms. Parties can be brought on board through alignment processes (e.g., IT investment approval process, architecture exception process, service level agreements, formal tracking of business-IT value) and effective communication (e.g., executive announcements; formal/ad hoc committee work; IT governance education delivered by the CIO; working with managers who stray from desirable behaviours; increasing transparency by housing policies, standards and performance on web-based portals).

• **Phase 6: Realize benefits**—Did we get there? In this phase, the effectiveness of IT governance implementation is determined by considering a number of factors, including a comprehensive model for managing all IT resources, improved executive participation, strategies and business objectives for IT investment, alignment between the business and the IT department, decision making and communication, perception of IT value, IT risk management, return on assets, lower IT costs, transparency of IT, IT performance tracking, and IT innovation.

• **Phase 7: Review effectiveness**—How do we keep the momentum going? The final phase of the continuum entails monitoring and reviewing IT governance, planning for its sustainment, and assessing its effectiveness. This should include shifting focus from relational mechanisms to improving structures/processes once the governance framework is embedded. In addition, a performance management system (balanced scorecard) should be introduced to facilitate continuous monitoring of IT governance effectiveness and ongoing framework enhancement.

**Building and Maintaining Effective IT Governance: Pitfalls and Key Success Principles**

The journey to effective IT governance is fraught with many challenges. Common pitfalls that may hinder the success of IT governance include:
CONCLUSION
The outcomes of a successful implementation are worth the challenge, producing both shorter-term, tangible benefits (such as reduced cost) and long-term benefits (such as enhanced management of IT-related risk, improved relationships between business and IT, and increased business competitiveness). Leveraging the leading practices that have been outlined will assist the board and C-suite executives on their journey to IT governance effectiveness.

REFERENCES
IT Governance Institute and PricewaterhouseCoopers, An Executive View of IT Governance, USA, 2009, www.isaca.org/bookstore


Van Grembergen, Wim; Steven De Haes, Guidelines for the Implementation of Enterprise Governance of IT, Springer Science, USA, 2009


The Modernization Problem, Part 1

Informally, a legacy system may be defined as technology or software application environments that may be replaced by newer or more modern technology, but because of prohibitive cost, lack of detailed knowledge and, in some instances, effectiveness within the current context, the system continues to function and provide services to the organization. The intellectual capital stored up in legacy systems often represents a significant organizational asset; therefore, the management of these long-term systems is critical to organizations as they are not easily replaced.

The concept of software evolution has been in existence for many years. For example, J.I. Schwartz said the following at the second North Atlantic Treaty Organization (NATO) Software Engineering Conference in 1969:

Managers must be willing to adapt as situations arise requiring changes in scope or technique. The basic system must, through such means as data description divorced from procedures, centralized data maintenance, and data-independent programming languages, be flexible enough to permit change and evolution without reprogramming. People must be flexible enough to tolerate rather drastic changes in direction.

DRIVERS OF CHANGE
Organizations have made significant capital investments in their underlying software systems, and the expectation is that they will see a return on these investments and, consequently, that software will be usable for a good number of years. The life span of software is variable, but there are numerous examples of large systems remaining in use for more than 10 years. In fact, many large software installations remain in use for more than 20 years (e.g., systems at insurance companies and banks).

The business drivers for legacy modernization are numerous and provide good incentive for organizations to embark on these projects. Business drivers include:

- The risk associated with running potentially unsupported software
- Graying of the labor pool as experts on the legacy system age (e.g., shortage of Cobol programmers. Cobol is more than 50 years old, yet a large portion of legacy systems have been written in Cobol.)
- Low levels of legacy systems integration capability and inflexibility with respect to responding to changing business demands

The reality is that although legacy systems possess numerous limitations, such as greenscreen interfaces that lack the conveniences of modern applications (i.e., drop-down menus, instant help files, intuitive navigation), approximately 70 percent of today’s organizations’ core business systems are legacy applications that are still heavily relied on to provide mission-critical business functionality.

ADDRESSING THE PROBLEM—RIP AND REPLACE
It is common knowledge that organizations regularly replace outdated equipment and machinery with newer and more modern systems. This is not generally the case with software systems and, in particular, legacy systems. These types of projects may lead to significant risk, including:

- Incomplete legacy system specification
- Business processes and legacy systems codependency
- Undocumented and embedded business rules
- New software development risk

Incomplete Legacy System Specification
In most instances the original documentation of the system has been lost or is not representative of the current version of the system. The implication of this lack of adequate documentation is manifested as:

- Increased risk to the organization when implementing changes to the system in response to external or internal forces
- Higher maintenance costs
- Increased cycle times for introduction of new products and/or services that rely on underlying system changes

Kirk Henry is head of the information and communications technology (ICT) department at the Trinidad & Tobago Unit Trust Corporation, the largest mutual fund provider in the Caribbean region. Henry has extensive experience in ICT governance, strategic planning and application systems development. He is currently spearheading a legacy modernization program that is based on his postgraduate work at the University of the West Indies, St. Augustine campus. Henry can be reached at khenry@ttutc.com.

Go directly to the article: [Go to article](https://www.isaca.org/journal/article/2013/1/Modernization-Problem-Part-1)
Business Processes and Legacy Systems Codependency

In most instances, the organizations’ business processes have evolved around the underlying legacy system implementation and would have been designed to work around or avoid any software weaknesses. The importance of the relationship between the business process and the system often becomes clear when projects are undertaken in an attempt to change a process without touching the supporting legacy system module. In these circumstances, the codependency condition has the potential for disruptions in production operations.

Undocumented and Embedded Business Rules

Important business rules may be embedded or hard-coded into the software and may not be documented elsewhere. A business rule is a constraint that applies to some business function; the implementation of new systems that break these constraints can result in unpredictable consequences for the business. Programmers come and go and business rules that have been codified over the years by multiple programmers are difficult to understand by an individual or group new to the system. In these circumstances even routine programming changes may expose organizations to unintended consequences that may give rise to financial impacts (third-party claims), reputational damage and even regulatory breaches.

New Software Development Risk

Software development is an activity that has a significant amount of uncertainty that is usually manifested as possible risk materialization.3 The well-known Chaos Report by the Standish Group in 1994 indicated that 16 percent of software projects were successful; 53 percent were challenged as a result of cost overruns, budget overruns or content deficiencies; and 31 percent were cancelled. This risk is magnified for new software developments involving interaction with legacy systems. The absence of a fully documented environment, aging infrastructure and a lack of standards contribute to an increased possibility of project failure. While keeping such legacy systems in production avoids replacement risk, this has to be balanced against the rising costs of maintaining the aging system.

ADOPTING MODERNIZATION AS A STRATEGY

While recognizing the value of existing systems and the risk involved in their replacement, organizations are realizing the value of adopting a modernization strategy as opposed to replacement. A 2010 survey conducted by NASCIO identified legacy modernization as one of the top 10 activities that organizations were planning to carry out in 2011.5

Modernization involves more extensive system changes than regular maintenance and results in the preservation of significant portions of the legacy investment while at the same time executing activities such as:

• System restructuring
• Enhancing core system functionality
• Modifying software attributes

Organizations recognize that a modernization of programs represents a viable approach to upgrading legacy environments when risky and pervasive changes are needed to address changing business requirements.5

Modernization is the preferred approach to system evolution when the legacy system provides significant business benefit, but the growing complexities associated with system maintenance results in overall increased risk for the organization. In the main, there are two broad approaches to legacy system modernization:

1. White-box modernization—This approach is largely predicated on an understanding of the existing system, facilitated through the use of existing documentation or, in most instances, the execution of a reverse-engineering process. This is often a labor-intensive exercise, and vendors are continuously coming out with new tools to facilitate automated system information discovery.

2. Black-box modernization—In contrast, black-box modernization is not concerned with the inner workings of the system to be modernized. The main focus of this approach lies in understanding the interfacing elements of the operations of the system. The fundamental idea is to wrap a layer of code around the legacy system to hide the complexity and expose a modern interface for interaction with other systems.

The decision to replace a system as opposed to ongoing maintenance or modernization is usually predicated on the inability to justify the cost of maintenance or modernization efforts against the cost of acquiring a new system. The decision to utilize replacement as the route to system evolution must be evaluated against the inherent implementation risk associated with new system developments, since the system being introduced typically is not as stable as the old system. Additionally, consideration must be given to risk associated
with the implementation of a new technology unfamiliar to supporting personnel. Therefore, when deciding upon a plan of action, organizations must gain an appreciation of the potential risk and develop mitigating plans through the application of an appropriate risk framework (e.g., COBIT® 5 or Risk IT®) to feed into the final decision.

NEXT STEPS
The question facing organizations that have decided to embark on a modernization program is how to achieve the necessary agility while maintaining operating effectiveness, especially in those circumstances where the legacy system resides on either a mainframe, AS/400/IBM i, OpenVMS/Unix or Windows client server-type platform.

Part two of this article, to be published in volume 2, 2013, will examine some of the techniques available to organizations as they embark on modernization projects and will discuss the questions surrounding:
1. Writing a new application from the beginning
2. Application migration and the use of service-oriented architecture (SOA)
3. Application reengineering, through the execution of functional transformations to generate either a more modern representation on the existing platform or multiple instantiations on multiple platforms
4. Application revamping, via updating the presentation layer of the legacy system without touching the underlying application code

ENDNOTES
3 Boban, M. Pozgaj; H. Sertic; Strategies for Successful Software Development Risk Management, vol. 8, 2003, p. 77-91

Get noticed...
Advertise in the ISACA® Journal
For more information, contact media@isaca.org.
ACROSS
1. The G in GEIT
6. URL ending
9. For each, in statistics (2 words)
13. Wipe clean
14. Audio visual, briefly
15. Common ending to family business names
16. Often the biggest risk in any security policy or framework (the end user can be the weakest link)
17. Leave out
19. Consult
21. Logical volume, for short
22. Drop back
24. Very exact (2 words)
25. Section of history
28. Range
29. Functions
31. ___FR coverage
33. Wise man
35. Benefit
36. Factor often underestimated as influencing success in governance and management activities
39. Service organization for short
41. Before

DOWN
1. Tool that helps a company compare its actual performance with its potential performance
2. Reseller, for short
5. Genetic initials, for short
4. Crops up
5. Risk and possibilities term
6. ____ restore, a data recovery and restoration technique (2 words)
7. Kind of file
10. Time before
11. Author of “IT Governance: A Pocket Guide,” Alan ___
12. HP product
18. Fine ____ (perfects)
20. “Walk the talk” in applying company principles
23. Platform-specific rule providing the most effective approach to a specific implementation, ____ line
26. Central points
27. ____ reputation, service to improve Internet security for a company
30. Forerunner to the European Union
32. ____ flow
34. Statements that describe desired outcomes
36. Completely remove data
37. Verifying who the customer is
38. Stings
40. Opponent
42. Board action
43. URL ending
44. Close to, for short
45. Economic group of advisors who advise the US president on economic matters, abbr.
48. Stumbling expression

(Answers on page 54)
Quiz #146
Based on Volume 5, 2012—Privacy and the Cloud
Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

BARRASSO AND WALLACE ARTICLE
1. Forrester Research estimated that the cloud computing market will reach US $200 billion by 2020, while IDC reports that spending on equipment for both public and private cloud storage systems will hit US $241 billion by 2015.

2. In this case study, the team sent gigabytes of highly sensitive encrypted data to the cloud using deduplication and compression to keep costs down.

RAVAL ARTICLE
3. In COBIT®, 5, the practices noted in enabler 5, Culture, Ethics and Behavior, are communications, enforcement, incentives and rewards, awareness, rules and norms, and champions.

4. Key success factors for broad implementation guidance in COBIT 5 include top management direction and mandate, and visible ongoing commitment and support.

5. ISACA’s Business Model for Information SecurityTM (BMIS™) does not provide any reference to ethics, so it cannot be used as a supplement to COBIT 5 in this area.

SINGLETON ARTICLE
6. Social media risk areas are similar to those brought about by other IT, such as inefficiency, wasted investment, insufficient effectiveness and lost opportunity. But, social media also has some unique risk areas, including damage to public image as a result of negative comments and postings in social media venues.

7. In auditing social media, auditing proactively for image and public relations is impossible because of risk velocity.

8. The audit of the IT (social media) itself is not much different from the approach used in other IT audits, but the risk assessment component has some special considerations (e.g., risk velocity, employee abuse).

NDIANDUKUE ARTICLE
9. The motivations of employers and recruiters of social networks include profiling and targeting potential markets, deepening customer relationships, online promotion and sales, and online surveys and studies.

10. Social networks’ conditions of use are in no way capable of guaranteeing the safety of Internet users and are purposely written in such a way that will discourage users from browsing them properly. Sites basically have no interest in users finding certain clauses that give them full control over all the information published.

AHMED ARTICLE
11. The only way a customer could become automatically compliant is if a PCI-compliant cloud provider actually managed all the way up the application stack and had a Software as a Service (SaaS) offering that is specific around one application that does a specific function. The cloud service provider (CSP) would have to ensure that every single customer, whether on physical or virtual servers, has the same level of security and separation.

12. For Infrastructure as a Service (IaaS), the consumer manages or controls the underlying cloud infrastructure, but has no control over the operating systems, storage and deployed applications, and unlimited control over select networking components (e.g., host firewalls).

13. Cloud providers should make management and maintenance more transparent and auditable by customers. This should include recording logs and complete administrative sessions that affect the part of the cloud infrastructure used by customers and, if requested, making these records accessible to customers.

VOHRADSKY ARTICLE
14. The management of the relevant business unit must own the risk associated with its use of cloud services, and must establish, direct, monitor and evaluate commensurate risk management on an ongoing basis.

15. The guiding principle of accountability for cloud computing risk is related to all necessary staff knowledge of the cloud, management’s knowledge of who is using the cloud and management authorization of what is put in the cloud.
ISACA Journal
CPE Quiz
Based on Volume 5, 2012—Privacy and the Cloud
Quiz #146 Answer Form
(Please print or type)
Name ________________________________________________
_____________________________________________________
Address ______________________________________________
_____________________________________________________
CISA, CISM, CGEIT or CRISC #___________________________

Quiz #146

True or False

BARRASSO AND WALLACE ARTICLE
1. ________
2. ________

AHMED ARTICLE
9. ________
10. ________

RAVAL ARTICLE
3. ________
4. ________
5. ________

Singleton Article
6. ________
7. ________
8. ________

VOHRA DSKY ARTICLE
11. ________
12. ________
13. ________
14. ________
15. ________

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current Journal subscribers. An electronic version of the quiz is available at www.isaca.org/cpequiz; it is graded online and is available to all interested parties. If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information by email to info@isaca.org or by fax to +1.847.253.1443. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA.

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

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

A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.
ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of IT audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards are a cornerstone of the ISACA professional contribution to the audit and assurance community. The framework for the IT Audit and Assurance Standards provides multiple levels of guidance:

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

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

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

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

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

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

Links to current guidance are posted on the standards page, www.isaca.org/standards. Please note that the standards are being updated for integration into the ITAF™ IS audit and assurance framework, www.isaca.org/itaf. The updated standards are scheduled to be issued in March 2013.

The titles of issued standards documents are:

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

**IT Audit and Assurance Guidelines**
- G1 Using the Work of Other Experts Effective 1 March 2008
- G2 Audit Evidence Requirement Effective 1 May 2008
- G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
- G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
- G5 Audit Charter Effective 1 February 2008
- G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
- G7 Due Professional Care Effective 1 March 2008
- G8 Audit Documentation Effective 1 March 2008
- G9 Audit Considerations for Irregularities Effective 1 September 2008
- G10 Audit Sampling Effective 1 August 2008
- G11 Effect of Pervasive IS Controls Effective 1 August 2008
- G12 Organisational Relationship and Independence Effective 1 August 2008
- G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
- G14 Application Systems Review Effective 1 October 2008
- G15 Audit Planning Revised Effective 1 May 2010
- 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 May 2010
- G18 IT Governance Effective 1 May 2010
- G19 Withhold Information Effective 1 September 2010
- G20 Reporting Effective 16 September 2010
- G21 Enterprise Resource Planning (ERP) Systems Review Effective 16 September 2010
- G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
- G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2005
- G24 Internet Banking Effective 1 August 2003
- G25 Review of Virtual Private Networks Effective 1 July 2004
- G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
- G27 Mobile Computing Effective 1 September 2004
- G28 Computer Forensics Effective 1 September 2004
- G29 Post-implementation Review Effective 1 January 2005
- G30 Competence Effective 1 June 2005
- G31 Privacy Effective 1 June 2005
- G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
- G33 General Considerations for the Use of the Internet Effective 1 March 2006
- G34 Responsibility, Authority and Accountability Effective 1 March 2006
- G35 Follow-up Activities Effective 1 March 2006
- G36 Biometric Controls Effective 1 February 2007
- G37 Configuration and Release Management Effective 1 November 2007
- G38 Access Controls Effective 1 February 2008
- G39 IT Organisation Effective 1 May 2008
- G41 Return on Security Investment (ROSI) Effective 1 May 2010
- G42 Continuous Assurance Effective 1 May 2010

**Code of Professional Ethics** Effective 1 January 2011
### 2013 CISA® EXAM REFERENCE MATERIALS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRM-13</td>
<td>English Edition</td>
<td>$135.00</td>
<td>$105.00</td>
</tr>
<tr>
<td>CRM-13C</td>
<td>Chinese Simplified Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CRM-13F</td>
<td>French Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CRM-13J</td>
<td>Japanese Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CRM-13S</td>
<td>Spanish Edition</td>
<td>135.00</td>
<td>105.00</td>
</tr>
<tr>
<td>CISA Review Questions, Answers &amp; Explanations Manual 2013*</td>
<td>QAE-13</td>
<td>100.00</td>
<td>80.00</td>
</tr>
<tr>
<td>QAE-13C</td>
<td>Chinese Simplified Edition</td>
<td>100.00</td>
<td>80.00</td>
</tr>
<tr>
<td>QAE-13F</td>
<td>French Edition</td>
<td>100.00</td>
<td>80.00</td>
</tr>
<tr>
<td>QAE-13J</td>
<td>Japanese Edition</td>
<td>100.00</td>
<td>80.00</td>
</tr>
<tr>
<td>QAE-13S</td>
<td>Spanish Edition</td>
<td>100.00</td>
<td>80.00</td>
</tr>
<tr>
<td>CISA Review Questions, Answers &amp; Explanations Manual 2013 Supplement*</td>
<td>QAE-13C5</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QAE-13F5</td>
<td>French Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QAE-13J5</td>
<td>Japanese Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>QAE-13S5</td>
<td>Spanish Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CISA Practice Question Database v13 (1,050 Questions)*</td>
<td>CBQ-13</td>
<td>225.00</td>
<td>185.00</td>
</tr>
<tr>
<td>CBQ-13W</td>
<td>Download—English Edition</td>
<td>225.00</td>
<td>185.00</td>
</tr>
<tr>
<td>CBQ-13S</td>
<td>Download—Spanish Edition</td>
<td>225.00</td>
<td>185.00</td>
</tr>
<tr>
<td>CAN*</td>
<td>Candidate’s Guide to the CISA Exam and Certification</td>
<td>15.00</td>
<td>10.00</td>
</tr>
</tbody>
</table>

### 2013 CISM® EXAM REFERENCE MATERIALS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM-13</td>
<td>English Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CM-13J</td>
<td>Japanese Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CM-13S</td>
<td>Spanish Edition</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CISM Review Questions, Answers &amp; Explanations Manual 2012*</td>
<td>CQA-12</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>CQA-12J</td>
<td>Japanese Edition</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>CQA-12S</td>
<td>Spanish Edition</td>
<td>90.00</td>
<td>70.00</td>
</tr>
<tr>
<td>CISM Review Questions, Answers &amp; Explanations Manual 2012 Supplement*</td>
<td>CQA-12C5</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CQA-12J5</td>
<td>Japanese Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CQA-12S5</td>
<td>Spanish Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CISM Review Questions, Answers &amp; Explanations Manual 2013 Supplement*</td>
<td>CQA-13</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CQA-13J</td>
<td>Japanese Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CQA-13S</td>
<td>Spanish Edition</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CISM Practice Question Database v13 (1,050 Questions)*</td>
<td>MBQ-13</td>
<td>160.00</td>
<td>120.00</td>
</tr>
<tr>
<td>MBQ-13W</td>
<td>Download—English Edition</td>
<td>160.00</td>
<td>120.00</td>
</tr>
<tr>
<td>CQC*</td>
<td>Candidate’s Guide to the CISM Exam and Certification</td>
<td>15.00</td>
<td>10.00</td>
</tr>
</tbody>
</table>

### 2013 CITO® EXAM REFERENCE MATERIALS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIG-13</td>
<td>CITO Review Manual 2013</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CIGD-13</td>
<td>CITO Review Questions, Answers &amp; Explanations Manual 2013 (60 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CIG-13ES*</td>
<td>CITO Review Questions, Answers &amp; Explanations Manual 2013 Supplement (60 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CACO*</td>
<td>Candidate’s Guide to the CITO Exam and Certification</td>
<td>15.00</td>
<td>10.00</td>
</tr>
</tbody>
</table>

### 2013 CRISC EXAM REFERENCE MATERIALS

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRP-13</td>
<td>CRISC Review Manual 2013</td>
<td>115.00</td>
<td>85.00</td>
</tr>
<tr>
<td>CRQ-13</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2013 (200 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>CRQ-13ES*</td>
<td>CRISC Review Questions, Answers &amp; Explanations Manual 2013 Supplement (100 Questions)</td>
<td>60.00</td>
<td>40.00</td>
</tr>
<tr>
<td>XMKR13-6M*</td>
<td>CRISC Exam Self-Study Subscription—6 Months</td>
<td>225.00</td>
<td>185.00</td>
</tr>
<tr>
<td>CACR*</td>
<td>Candidate’s Guide to the CRISC Exam and Certification</td>
<td>15.00</td>
<td>10.00</td>
</tr>
</tbody>
</table>

---

**NON-ENGLISH RESOURCES** for additional CBT material.
**RISK RELATED TOPICS**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>78-WRM</td>
<td>The Failure of Risk Management: Why It’s Broken and How to Fix It</td>
<td>70.00</td>
<td>50.00</td>
</tr>
<tr>
<td>70-WFR</td>
<td>Fraud Risk Assessment: Building a Fraud Audit Program</td>
<td>84.00</td>
<td>74.00</td>
</tr>
<tr>
<td>11-CRC8</td>
<td>How to Complete a Risk Assessment in 5 Days or Less</td>
<td>98.00</td>
<td>88.00</td>
</tr>
<tr>
<td>84-WRM</td>
<td>Information Technology Risk Management in Enterprise Environments</td>
<td>110.00</td>
<td>100.00</td>
</tr>
<tr>
<td>2-HBS</td>
<td>IT Risk: Turning Business Threats Into Competitive Advantage</td>
<td>45.00</td>
<td>35.00</td>
</tr>
<tr>
<td>1-HHP</td>
<td>The Operational Risk Handbook for Financial Companies</td>
<td>63.00</td>
<td>53.00</td>
</tr>
<tr>
<td>5-PL</td>
<td>Risk Management &amp; Risk Assessment</td>
<td>105.00</td>
<td>95.00</td>
</tr>
</tbody>
</table>

**AUDIT, CONTROL AND SECURITY—ESSENTIALS**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>48-CRC</td>
<td>Access Control, Security, and Trust: A Logical Approach</td>
<td>105.00</td>
<td>95.00</td>
</tr>
<tr>
<td>1-IT9</td>
<td>Accounting Information Systems, 9th Edition</td>
<td>324.00</td>
<td>314.00</td>
</tr>
<tr>
<td>93-WAAS</td>
<td>Auditing and Assurance Services: Understanding the Integrated Audit</td>
<td>235.00</td>
<td>225.00</td>
</tr>
<tr>
<td>6-PL</td>
<td>IT Assurance IT Infrastructures</td>
<td>105.00</td>
<td>95.00</td>
</tr>
<tr>
<td>76-WSL</td>
<td>Build Your Own Security Lab: A Field Guide for Network Testing</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>43-CRC</td>
<td>Building an Effective Information Security Policy Architecture</td>
<td>94.00</td>
<td>84.00</td>
</tr>
<tr>
<td>31-CRC</td>
<td>Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI</td>
<td>140.00</td>
<td>130.00</td>
</tr>
<tr>
<td>79-CAW</td>
<td>Computer Aided Fraud Prevention and Detection: A Step by Step Guide</td>
<td>74.00</td>
<td>64.00</td>
</tr>
<tr>
<td>51-CRC</td>
<td>Data Protection: Governance, Risk Management, and Compliance</td>
<td>86.00</td>
<td>76.00</td>
</tr>
<tr>
<td>13-ITCAT</td>
<td>The Definitive Guide to the ISO 27001 Transformation</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>50-WPM5</td>
<td>Effective Project Management: Traditional, Agile, Extreme, 6th Edition</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-ABE5</td>
<td>Enterprise Security for the Executive: Setting the Tone from the Top</td>
<td>45.00</td>
<td>35.00</td>
</tr>
<tr>
<td>92-WA</td>
<td>The Essential Guide to Internet Auditing, 2nd Edition</td>
<td>65.00</td>
<td>55.00</td>
</tr>
<tr>
<td>71-WCP</td>
<td>Essentials of Corporate Fraud</td>
<td>58.00</td>
<td>48.00</td>
</tr>
<tr>
<td>82-WACL</td>
<td>Fraud Analysis Techniques Using ACL</td>
<td>221.00</td>
<td>211.00</td>
</tr>
<tr>
<td>11-IT</td>
<td>Guide to Firewalls and VPNs, 3rd Edition</td>
<td>180.00</td>
<td>170.00</td>
</tr>
<tr>
<td>7-ART</td>
<td>Implementing the ISO/IEC 27001 Information Security Management System Standard</td>
<td>105.00</td>
<td>95.00</td>
</tr>
<tr>
<td>2-ABA</td>
<td>Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists</td>
<td>130.00</td>
<td>120.00</td>
</tr>
<tr>
<td>4-CRC3</td>
<td>Information Technology Control and Audit, 3rd Edition</td>
<td>100.00</td>
<td>90.00</td>
</tr>
<tr>
<td>95-WAAS</td>
<td>Interpretation and Application of International Standards on Auditing</td>
<td>115.00</td>
<td>105.00</td>
</tr>
<tr>
<td>8-PL</td>
<td>IT Auditing: The Process</td>
<td>105.00</td>
<td>95.00</td>
</tr>
<tr>
<td>90-WACS</td>
<td>IT Audit, Control, and Security</td>
<td>100.00</td>
<td>90.00</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITOC0C</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>50.00</td>
<td>FREE</td>
</tr>
<tr>
<td>WITOC0C</td>
<td>Print Format</td>
<td>60.00</td>
<td>35.00</td>
</tr>
<tr>
<td>STOPKN</td>
<td>IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals</td>
<td>20.00</td>
<td>15.00</td>
</tr>
<tr>
<td>WITAP</td>
<td>ITAC: A Professional Practices Framework for IT Assurance e-book—PDF format (purchase online only)</td>
<td>45.00</td>
<td>FREE</td>
</tr>
<tr>
<td>15-MT2</td>
<td>IT Auditing Using Controls to Protect Information Assets, 2nd Edition</td>
<td>80.00</td>
<td>70.00</td>
</tr>
</tbody>
</table>

**IT Control Objectives for Basel II**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>WITCOB0</td>
<td>E-book—PDF Format (purchase online only)</td>
<td>35.00</td>
<td>FREE</td>
</tr>
<tr>
<td>WITCOB0</td>
<td>Print Format</td>
<td>50.00</td>
<td>20.00</td>
</tr>
<tr>
<td>FS0X</td>
<td>IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition</td>
<td>7.00</td>
<td>7.00</td>
</tr>
<tr>
<td>22-MSM</td>
<td>IT Security Metrics: A Practical Framework for Measuring Security &amp; Protecting Data</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>6-ITDSO</td>
<td>IT Strategic and Operational Controls</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-IA</td>
<td>A New Auditor’s Guide to Planning, Performing, and Presenting IT Audits</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>7-SYN10</td>
<td>PCI Compliance, Third Edition</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-RIA</td>
<td>Practical IT Auditing with current Supplement</td>
<td>470.00</td>
<td>460.00</td>
</tr>
<tr>
<td>12-IT</td>
<td>Principles of Information Security, 4th Edition</td>
<td>166.00</td>
<td>150.00</td>
</tr>
<tr>
<td>2-SAPP</td>
<td>SAP Security and Risk Management, 2nd Edition</td>
<td>80.00</td>
<td>70.00</td>
</tr>
<tr>
<td>28-MSM</td>
<td>Security Metrics: A Beginner’s Guide</td>
<td>50.00</td>
<td>40.00</td>
</tr>
</tbody>
</table>

**INTERNET AND RELATED SECURITY TOPICS**

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Nonmember</th>
<th>Member</th>
</tr>
</thead>
<tbody>
<tr>
<td>45-CRC</td>
<td>Cloud Computing: Implementation, Management, and Security</td>
<td>90.00</td>
<td>80.00</td>
</tr>
<tr>
<td>11-EL</td>
<td>Cyber Attacks: Protecting National Infrastructure</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>1-CR03</td>
<td>Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 3rd Edition</td>
<td>48.00</td>
<td>38.00</td>
</tr>
<tr>
<td>10-IT</td>
<td>Cybersecurity: The Essential Body of Knowledge</td>
<td>107.00</td>
<td>97.00</td>
</tr>
<tr>
<td>4-MG08</td>
<td>Gray Hat Hacking: The Ethical Hackers Handbook, 3rd Edition</td>
<td>70.00</td>
<td>60.00</td>
</tr>
<tr>
<td>23-MHE</td>
<td>Hacking Exposed Web Applications, 3rd Edition</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>2-MC07</td>
<td>Hacking Exposed 7: Network Security Secrets &amp; Solutions, 7th Edition</td>
<td>60.00</td>
<td>50.00</td>
</tr>
<tr>
<td>17-MHE2</td>
<td>Hacking Exposed Wireless: Wireless Security Secrets &amp; Solutions, 2nd Edition</td>
<td>60.00</td>
<td>50.00</td>
</tr>
</tbody>
</table>
www.isaca.org/bookstore

Order online at www.isaca.org/bookstore

M all completed form with payment:
ISA CA / ITG I
1055 Paysphere Circle
Chicago, IL 60674-1055 USA

Fax completed order form with credit card number and expiration date to +1.847.253.1443

Phone: +1.847.660.5650

Monday-Friday, 8:00 am-5:00 pm Central Time (Chicago, Illinois, USA) Personal service—please have credit card number available. We will confirm availability and expected delivery date.

Send electronic payments in US dollars to: Bank of America, ABA #0260-0959-3
ISA CA Account #22-71578
S.W.I.F.T code B0FAUS3N

Returns Policy

All purchases are final. No refunds or exchanges.

Publication Quantity Discounts

A academic and bulk discounts are available on books published by the ISA CA and IT Governance Institute. Please call +1.847.660.5501 or +1.847.660.5578 for pricing information.

Delivery

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

Customs

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

Customer Information

Name ____________________________

FIRST  MIDDLE  LAST/FAMILY

ISACA Member:  ☐ No  ☐ Yes  Member Number ____________________________

Company Name ____________________________

Address:  ☐ Home  ☐ Company

City ____________________________ State/Province ____________________________

Country ____________________________ Zip/Mail Code ____________________________

Phone Number ( ) ____________________________ Fax Number ( ) ____________________________

E-mail Address ____________________________

Code ____________________________ Title/Item ____________________________ Quantity ____________________________ Unit Price US $ ____________________________ Total US $ ____________________________

Shipping Information  (If different from customer information)
If shipping to a P.O. Box, please include street address to ensure proper delivery.

Name ____________________________

FIRST  MIDDLE  LAST/FAMILY

Company Name ____________________________

Address:  (If Part of Shipping Address) ____________________________

City ____________________________ State/Province ____________________________

Country ____________________________ Zip/Mail Code ____________________________

Phone Number ( ) ____________________________ E-mail Address ____________________________

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

Payment Information—Prepayment Required

☐ Payment enclosed.  Check payable to “ISACA” in US dollars, drawn on US bank.
☐ Bank wire transfer in US dollars.  Date of transfer ____________________________
☐ Charge to  ☐ Visa  ☐ MasterCard  ☐ American Express  ☐ Olivers Club  ☐ Discover

Credit Card # ____________________________

Exp. Date ____________________________

Print Cardholder Name ____________________________

Signature of Cardholder ____________________________

Shipping & Handling Rates for Orders
All orders outside the US are shipped Federal Express Priority.

For Orders Totaling Outside US US $ Within US US $ In Total
Up to US $30.00 US $10.00 US $5.00 17% of Total
US $30.01 to US $50.00 US $15.00 US $7.00 10% of Total
US $50.01 to US $80.00 US $20.00 US $8.00
US $80.01 to US $150.00 US $26.00 US $10.00
Over US $150.00

No shipping charges apply to Mycsor C200T.
No shipping charges apply to CSA Practice Question Database v1.3—download.
No shipping charges apply to CISM Practice Question Database v1.3—download.

Subtotal

Sales Tax:  Add sales tax if shipping to:

Louisiana (LA), Oklahoma (OK)—4%
Wisconsin (WI)—5%
Florida (FL), Minnesota (MN), Pennsylvania (PA), South Carolina (SC), Texas (TX), Washington (WA)—6%
California (CA), New Jersey (NJ), Puerto Rico (PR), Tennessee (TN)—7%
Illinois (IL)—9%

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

TOTAL

Shipping details www.isaca.org/shipping
International customers are solely responsible for paying all duties, service charges, and taxes levied by their country.

All purchases are final.  Pricing, shipping and handling, and tax are subject to change without notice.
In a sea of IT professionals, ISACA members get noticed.

No matter where you are on your career path, ISACA® equips you with the resources you need to enhance your skills, expand your professional knowledge and experience a vibrant local and global community of peers. Be sure to utilize all of the benefits offered through your ISACA membership.

Visit www.isaca.org/benefits for a full list of member benefits.

Renew now!

If you aren’t currently a member, visit www.isaca.org/join and join today!
Regis University offers a graduate certificate as well as a master’s degree in Information Assurance. With both programs, you have the option to take classes online or on campus. Regis University is also designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

**INFORMATION ASSURANCE PROGRAMS**

**GRADUATE CERTIFICATE**
- Can be completed in less than a year
- Four classes (12 credit hours)

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

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

Classes can be taken on campus or completely online.

Regis University is an accredited, 130-year-old Jesuit institution in Denver, CO. Regis has been recognized as a national leader in education for adults and is committed to programs that are accessible and affordable. *U.S. News & World Report* has ranked Regis University as a Top University in the West for 17 consecutive years.

**REGIS UNIVERSITY**

School of Computer & Information Sciences

LEARN MORE

www.regisdegrees.com/ISACA | 855.508.8454