

In This Issue:

- **Case Study: Using COBIT Best Practices for Developing BCP for an Outsourcing Company, by A Rafeq, CISA, CGEIT, CIA, FCA**
- **Integrating ISACA Frameworks Into One Overarching Framework: COBIT 5, by John Lainhart, CISA, CISM, CGEIT, CIPP/G, and Derek Oliver, Ph.D., CISA, CISM**
- **Maturity Models and IT Strategic Planning, by John Petrey**
- **Taking Governance Forward: A Call to Action, by Patrick Stachtchenko, CISA, CGEIT, CA**
- **Key Success Factor: IT Resource Management, by Reinhold Thurner, Ph.D.**

Case Study: Using COBIT Best Practices for Developing BCP for an Outsourcing Company

By A Rafeq, CISA, CGEIT, CIA, FCA

ABC Solutions (ABC) is India's fastest-growing business processing outsourcing (BPO) specialist catering to all corporate business needs. ABC is providing BPO solutions in areas of employer, accounting and financial services. ABC is currently providing integrated payroll services using an Internet platform. A high-end Internet platform architected on multiple Sun Solaris servers and WebLogic Application servers with multiple layers of security has been deployed to enable its customers and employees to have access to the latest payroll information online.

Background

Being proactive about client requirements and considering the criticality of services provided, ABC envisaged the need to develop a business continuity planning (BCP) program and related operational procedures in tune with its policy of providing reliable and continuous services using COBIT® best practices. ABC planned to have a documented BCP system that was process-oriented and comprehensive. To achieve this, ABC engaged a COBIT subject matter expert as an external consultant to study and assess the relevant requirements and to facilitate development of a BCP system. An internal project team with domain knowledge comprising representatives of

Call for Articles

How are you using COBIT, Val IT™, Risk IT, BMIS or ITAF™ at your enterprise?

Submit articles on your experiences with these frameworks.

Deadline to submit copy for volume 3, 2010: 10 June

Submit articles for peer review to:

publication@isaca.org

various functional domains was set up to interface with external consultants and internalize the processes. A series of discussions was held by external consultants with the senior management and executives of ABC to obtain an understanding of the business processes, IT resources and BCP requirements. Based on this, the overall scope, objective, strategy, roles and responsibilities, and methodology for the assignment were finalized.

Objective of Assignment

The primary objective of the assignment was to develop BCP based on COBIT best practices and supplemented with best practices from other frameworks such as ISO 27002 and Business Continuity Institute (BCI) best practices. The BCP system had to be adequate to ensure resumption of computer systems in a timely manner during adverse circumstances, had to be in line with the current/future business requirements, and had to reflect the business operating environment.

Approach for Using COBIT

A detailed project plan was prepared, identifying specific tasks, and roles and responsibilities were agreed upon between the consultant and internal team. The consultant provided support and guidance in the identification and selection of best practices, and these were customized by the internal team based on relevant business processes. The consultant was responsible for preparing the initial BCP system based on inputs from ABC. The BCP system was updated and maintained by ABC.

The key questions for identifying the relevant COBIT components and contents from the relevant stakeholders were:

- What is the objective of COBIT implementation for ABC, and what are the specific deliverables?
- What COBIT components should be used, and why and how should they be used?
- What are the relevant IT processes to be selected from COBIT?
- What level of detail is required, and how is it to be supplemented from other frameworks?
- What is the extent of customization, and how is this to be done?
- What is the extent of integration?
- How can ABC adapt, use and implement relevant best practices for specific IT processes?
- How can ABC monitor/measure success and internalize the processes to ensure sustainability?

Methodology

The step-by-step methodology for using COBIT was as follows:

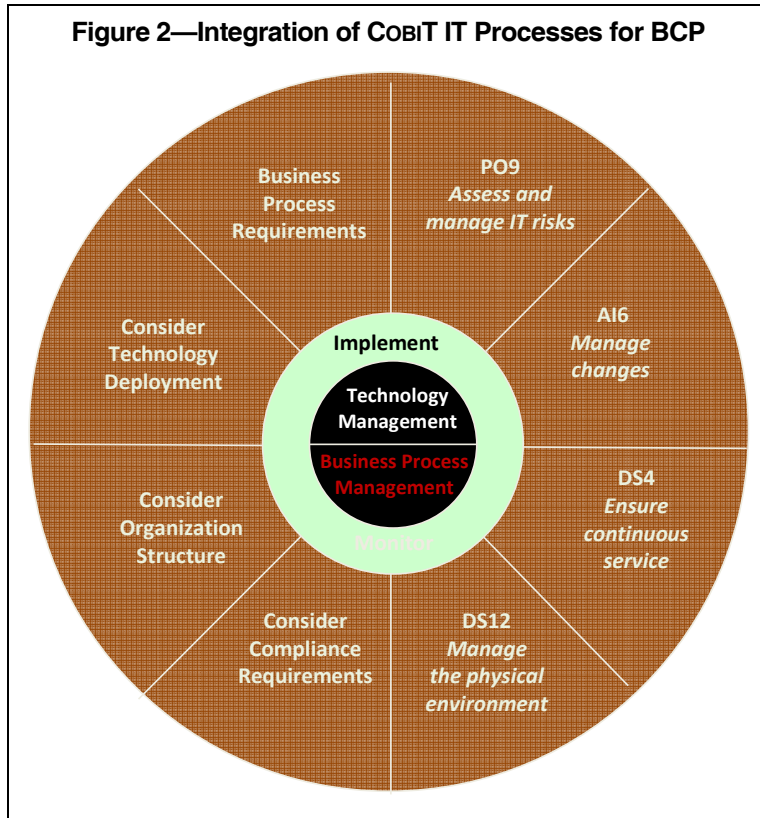
1. A brief presentation on COBIT and the proposed methodology for using it was made to the management and internal team, and this was supplemented with circulation of COBIT documents as relevant.
2. Understanding of the overall business goals and strategy was obtained through interaction with the managing director and executive management.
3. Understanding of the business processes was obtained through interaction with the heads of each of the key departments and review of relevant documentation.
4. Understanding of the technology infrastructure was obtained via a walk-through of the IT infrastructure at the head office and via review of the technology architecture and IT solutions deployed.
5. All documentation relating to business processes/IT policies, procedures and practices, and organization structure, including IT organization structure, was reviewed. This review revealed that the enterprise had good documentation, but it was fragmented and not comprehensive enough to meet the business requirements, especially business continuity requirements.
6. A walk-through of the COBIT summary table (**figure 1**) was done based on the primary information criteria of “availability,” and four key IT processes were initially selected. It was decided to validate these with the internal team.

Figure 1—COBIT Summary Table Based on Availability								
Legend: Blank = No impact P = Primary impact S = Secondary impact		Information Criteria						
PID	PC Process Controls	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability
PO9	<i>Assess and manage IT risks</i>	S	S	P	P	P	S	S
AI6	<i>Manage changes</i>	P	P		P	P		S
DS4	<i>Ensure continuous service</i>	P	S			P		
DS12	<i>Manage the physical environment</i>				P	P		

7. A presentation was made to the internal team using the one-page framework for all 34 IT processes, and the internal team was asked to identify and select IT processes from COBIT that are relevant to BCP.
8. Process descriptions, which describe what the process owner needs to do, were used for identifying and clarifying specific COBIT IT processes and confirming which processes to select.
9. The internal team used the details in the one-page framework to provide justification and a business case for implementing relevant IT processes within the enterprise. A template was developed for documenting the rationale for selection/nonselection of each of the IT processes.
10. It was decided to use the COBIT maturity models for assessing the current maturity level of IT processes, identifying gaps and preparing a road map for improvement. The contents from the COBIT maturity level for all levels were presented in the format of a questionnaire, and the heads of each of the functional departments were asked to respond to them. The responses were collated, validated and discussed in a joint meeting of all stakeholders. After extensive deliberations, the current maturity level for the selected IT processes was agreed upon. It came as a shock to the stakeholders that the maturity levels were much lower than expected.
11. The next step was to decide the right level of maturity for the selected IT processes. The initial expectation was the highest level of 4 or 5 for all processes, but when a detailed walk-through of the requirements to reach this level was done, it was found that the current business situation and budget did not allow for this. Hence, after detailed deliberation, it was decided to target a minimum level of 3 for all selected IT processes. It was also decided to use COBIT components and contents from other frameworks to bridge this gap.
12. COBIT control objectives show what controls need to be in place and how these controls are to be implemented to ensure performance measurement of IT in line with business requirements and, thus, sustaining or extending business strategy and meeting governance requirements. Control objectives were used as primary documents for assessing the required controls and as a benchmark for effective management of relevant IT processes. The COBIT control objectives were used as a benchmark to validate availability, adequacy and appropriateness of existing IT processes. The identified gaps were implemented by using the relevant control practices. These were supplemented as required with best practices from other frameworks by using the COBIT Mapping series of documents (www.isaca.org/cobitmapping). The COBIT control objectives for each of the identified IT processes/tasks (see **figure 2**) were further supplemented by the following six generic

process controls:

- **Process owner:**
Assign an owner for each COBIT process so that responsibility is clear.
 - **Repeatability:**
Define each COBIT process so that it is repeatable.
 - **Goals and objectives:** Establish clear goals and objectives for each COBIT process for effective execution.
 - **Roles and responsibilities:** Define unambiguous roles, activities and responsibilities for each COBIT process for efficient execution.
 - **Process performance:** Measure the performance of each COBIT process against its goals.
 - **Policy, plans and procedures:** Document, review, keep up-to-date, sign off on and communicate to all involved parties any policy, plan or procedure that drives a COBIT process.
13. The input and output documents matrix was used to map the documentation requirements. Considering that process inputs are what the process owner needs from others and process outputs are what the process owner has to deliver for each of the relevant processes, a mapping was done with existing documentation, and gaps in documentation were identified. Ownership was established for developing appropriate documents as relevant to BCP.
 14. Responsible, Accountable, Consulted and Informed (RACI) charts define what has to be delegated and to whom. Considering that a RACI chart helps clarify the responsibility to be assigned for key activities for ensuring performance measurement to IT process owners, a mapping was done with the existing organization for all key activities relevant to the enterprise. Based on this mapping, gaps in ownership were identified and it was decided to establish an accountability matrix for all key IT processes/activities relevant to BCP for the enterprise.
 15. Goals and metrics show how the process should be measured. Considering that goals and metrics provide transparency about how performance measurement is being implemented, a mapping was done with the relevant key performance indicators in the enterprise. It was noticed that there were many key processes/activities that were not being measured. It was decided to establish goals and metrics for all key activities, and these were integrated as part of the regular reporting requirements and IT balanced scorecard.
 16. Based on the above steps, a detailed report was issued to management highlighting areas of weaknesses in documentation; IT processes; IT policies, procedures and practices; and IT infrastructure requirements. As a result, appropriate recommendations were provided. These were discussed in a presentation to the stakeholders, and a road map for bridging the gaps, which was validated by the consultants, was prepared by the internal team.



Conclusion

The internal team was constituted as a project team and tasked with the implementation. The head of the quality assurance department was named the project leader. The project was successfully completed in 12 months and resulted in additional investment in IT infrastructure, development of detailed documentation, establishment of responsibility for all key processes, and the set up of key performance indicators and key goal indicators for all key activities based on the goals and metrics of COBIT.

The consultants were asked to conduct an external review of the BCP system as implemented. They used the COBIT control objectives to confirm whether the required controls were implemented, and the COBIT maturity model was used to validate whether IT processes were meeting the requirements at a minimum level of 3, which had been the target for the enterprise.

A brief report confirming the successful implementation and reaching of the target level, along with a few areas that required improvements, was issued by the consultants. The project team implemented the recommendations and ensured that all processes were internalized and ownership established to ensure sustainability.

The successful implementation of best practices based on COBIT for relevant IT processes helped ABC build a comprehensive BCP program that met business, client and regulatory requirements. As ABC scaled up its operations, the relevant COBIT components served as a stepping stone for moving up the ladder of the maturity model in a phased manner.

A Rafeq, CISA, CGEIT, CIA, FCA

is an IT governance and assurance professional from Bangalore, India, with more than 25 years of experience in varied roles such as chief financial officer, chief information officer, IT implementer, IT consultant, IT auditor and COBIT trainer. He has been a COBIT user and implementer for more than 14 years and is a well-known COBIT evangelist. Rafeq has made presentations on IT governance, IT assurance and COBIT implementation at international conferences. He was the founding secretary and a past president of the ISACA Bangalore Chapter. He is a member of ISACA's CGEIT Certification Committee and COBIT 5 Task Force.

Research Update

Recently released COBIT publication:

- ***SharePoint Deployment and Governance Using COBIT® 4.1***

Recently released Val IT publication:

- ***Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0***

Upcoming COBIT publications:

- ***COBIT® Mapping: Mapping of BS25999 With COBIT® 4.1***
- ***COBIT® Mapping: Mapping of CMMI With COBIT® 4.1***
- ***COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1***
- ***COBIT® Mapping: Mapping of ISO 20000 With COBIT® 4.1***
- ***COBIT® Mapping: Overview of International IT Guidance, 3rd Edition***

Upcoming Val IT publication:

- ***Business Case Guide: Using Val IT™ 2.0***

Upcoming BMIS publication:

- ***Business Model for Information Security***

Integrating ISACA Frameworks Into One Overarching Framework: COBIT 5

By John Lainhart, CISA, CISM, CGEIT, CIPP/G, and
Derek Oliver, Ph.D., CISA, CISM

For many years, ISACA® has researched the key area of enterprise governance to advance international thinking and provide guidance in evaluating, directing and monitoring an enterprise's use of IT. ISACA has developed groundbreaking frameworks—COBIT, Val IT, Risk IT, the Business Model for Information Security (BMIS) and the IT Assurance Framework™ (ITAF)—to help enterprises implement sound governance mechanisms and address specific areas such as information security and assurance. In addition, ISACA has established the Taking Governance Forward (TGF) initiative to provide a structured, high-level overview of enterprise governance, including its definition, components, objectives, participants and views. COBIT® 5 will be designed and developed in alignment with these frameworks and the initiative.

The primary improvements that will be found in COBIT 5 include that it will:

- Align with ISACA's TGF initiative as well as recent global governmental and market-driven enterprise and IT governance initiatives, such as sustainability and green IT
- Be consolidated into a single overarching framework providing one consistent and integrated source of guidance
- Be described in a high-level framework publication, providing an explanation of the objectives, scope, format and usage of COBIT 5 and enabling enterprises to strategically plan adoption of COBIT 5 and how to migrate to the new framework
- Consist of a set of publications providing the content of COBIT 5 required for enterprise implementation and assurance activities, and the focused guidance publications on functional, responsibility and organisational views to help provide COBIT 5 users who have a specific area of interest with a better understanding of how COBIT 5 can support their role in governance and management
- Clarify the distinction between governance and management through a revised process model that distinguishes between these domains while also showing how they relate to each other
- Align with the latest management practices and strengthen areas such as decision making, organisational structures, skill requirements, human factors, culture and change enablement

New Online COBIT Training

The online COBIT®
Foundation Exam is now
available on the **ISACA
e-Learning Campus**.

COBIT Training at Training Week

2010 dates and locations:

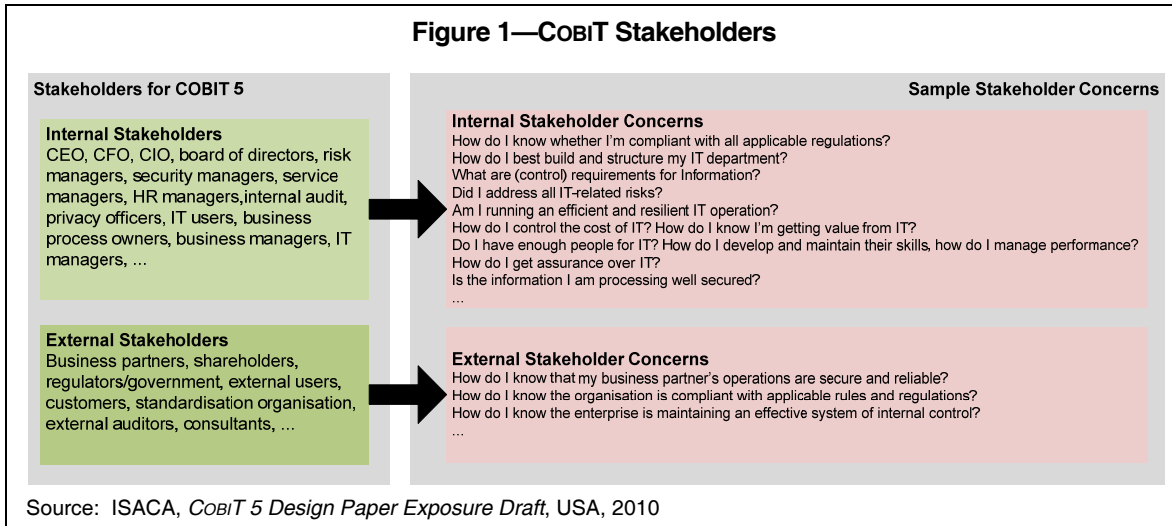
- **24-28 May 2010,
Charlotte, North
Carolina, USA**
- **13-17 September 2010,
Orlando, Florida, USA**
- **11-15 October 2010,
Indianapolis, Indiana,
USA**
- **6-10 December 2010,
Las Vegas, Nevada,
USA**

[Click here to register.](#)

ISACA On-site Training

**Groups of 10 or more
requiring COBIT training
can maximize their
organization's training
opportunities while
minimizing costs by
eliminating the need for
staff travel.**

[Click here for more
information.](#)



Stakeholder Requirements

The COBIT 5 development will be based on the best possible understanding of stakeholder needs. Stakeholders are all those who have an interest in the enterprise governance of IT; this covers a wide range of potential COBIT users and role players who either sponsor/support the use of COBIT or who are affected by its use and may be internal or external to the enterprise. These various COBIT 5 stakeholders have concerns and requirements related to the enterprise governance of IT, which are summarised in **figure 1**.

Recognition that these diverse stakeholders have some unique requirements and the need for digestible and practically usable guidance are driving forces for the future direction of COBIT.

Future Direction of COBIT

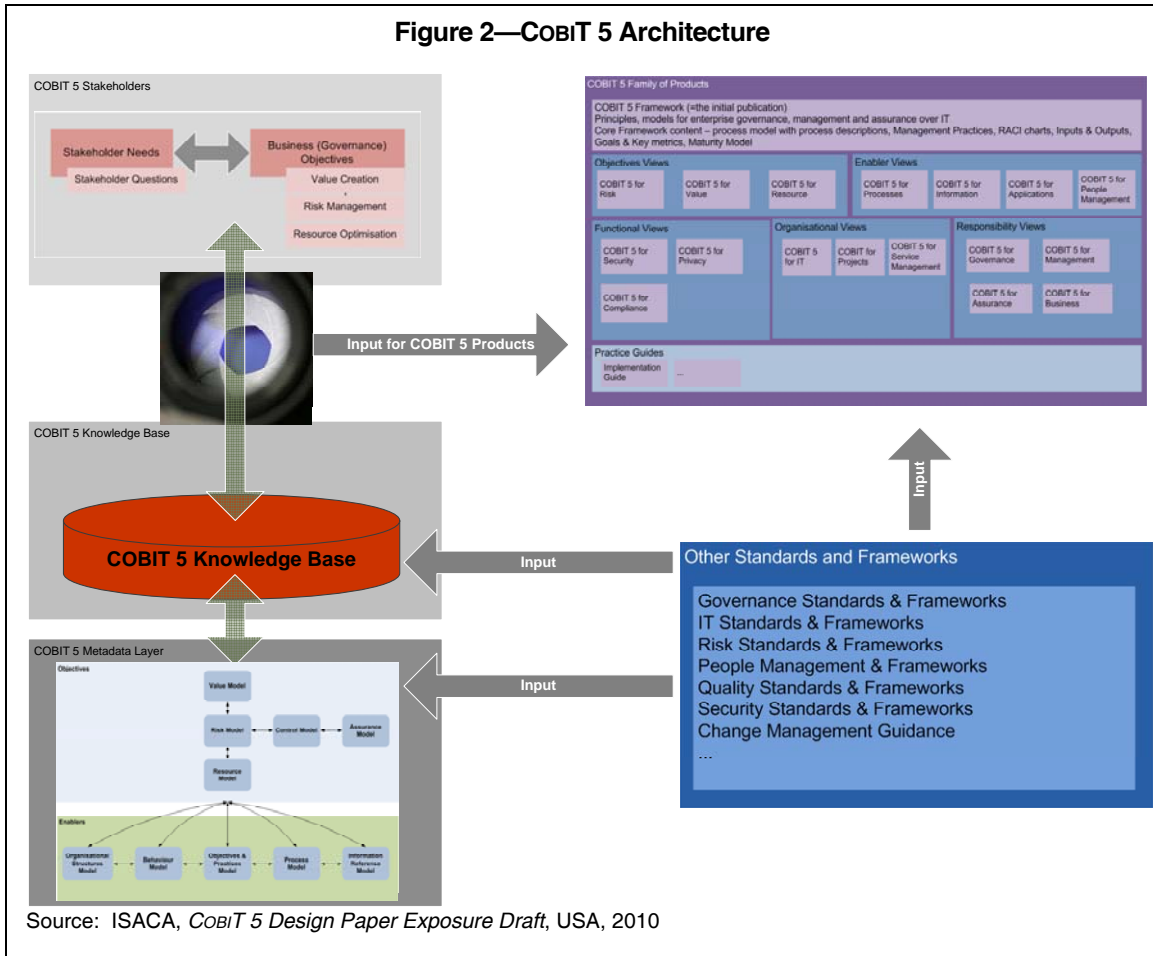
COBIT 5 will be a major strategic improvement, providing the next generation of guidance on the enterprise governance of IT. Building on the more than 15 years of practical usage and application of COBIT by many global enterprises and users from the business, IT, security and assurance communities, COBIT 5 will be designed to meet the current needs of stakeholders and will align with the most up-to-date thinking in enterprise governance and IT management techniques.

COBIT 5 will provide for an easy migration for current users of COBIT 4.1, Val IT, Risk IT, BMIS and ITAF, with guidance on how to migrate to the new framework. It will be more complete and easier to navigate, bringing together, under one integrated framework, all of ISACA's guidance relating to the enterprise governance of IT (see **figure 2**) and providing a logical path through them, depending on the stakeholder's needs. As a result, a new product set will be developed to support users, recognising that the content of COBIT 5 will need to be presented in several separate but inter-related publications to enable the guidance to be navigable, digestible, readable and usable in practice for a diverse range of stakeholder needs.

The updated framework will continue to align and support the approach provided in the most recent ISACA guidance on implementation, *Implementing and Continually Improving IT Governance*, released December 2009, in which the emphasis is on continual improvement, presented as a life cycle.

The process model of COBIT 5 will clarify the distinction between governance and management, distinguishing between these domains while also showing how they relate to each other. In the new COBIT 5 framework, the current four-domain format of COBIT 4.1 will be retained, but used to focus on management processes. Some simplification and consolidation of existing processes, as

Figure 2—COBIT 5 Architecture



well as the expansion and introduction of new areas of activity, are also proposed. Overall, the scope and content of these processes will aim to cover the full end-to-end scope within the business and IT specialist functions of management activities, continuing a trend that has evolved over several years but now truly recognises that IT is pervasive and, in almost all cases, involves activities across the enterprise.

A new focus on governance will be organised into three new governance process domains—Evaluate, Direct and Monitor—aligned with ISO 38500. Other models will also be used to support the use of the COBIT framework, covering aspects such as resources and information.

The underlying content of COBIT 5 will be created and maintained in a database repository, ensuring that the material is complete, consistent, properly organised and more easily maintained in the future. This approach will also improve the integrity and accuracy of the COBIT 5 components, with clearer links to external standards and best practice sources.

Going Forward

An initial exposure draft containing the proposals summarised here will be used to obtain input and comment regarding the assumptions of stakeholder requirements, the proposed strategic approach and the high-level design. The initial exposure draft was distributed to a significant number of volunteer reviewers and the COBIT development groups located in several countries around the world. There has also been a global survey of key COBIT contacts, and a copy of the exposure draft was posted on the ISACA web site for public feedback.

Key stakeholders in the outcome of this initiative are invited to provide any feedback regarding the requirements or any concerns they may have in relation to the enterprise governance of IT

that should be considered in designing COBIT 5. Feedback should be e-mailed to Brian Selby at bselby@isaca.org.

Based upon the comments received on the initial exposure draft and other feedback, the design for COBIT 5 will be finalised. Upon completion of the design, content development will begin.

Development activities will involve extensive input from many sources and people and will result in a draft version of the overarching COBIT 5 framework, which will be widely distributed for feedback. This review activity is currently planned for March 2011.

To learn more about COBIT 5, please visit www.isaca.org/cobit5. There will be regular communications in *COBIT Focus* and other ISACA publications and on the ISACA web site regarding the status of this initiative as it progresses.

John W. Lainhart IV, CISA, CISM, CGEIT, CIPP/G

is the service area leader for Security, Privacy, Wireless & IT Governance with the public sector of IBM Global Business Services (GBS). He was most recently the project executive responsible for IBM consulting projects, which led to the implementation of IT governance, COBIT and Val IT at the US Department of Veterans Affairs, Freddie Mac and Fannie Mae. He has held numerous positions at ISACA/IT Governance Institute® (ITGI®), including 1984-1985 international president, and currently is a member of the Framework Committee and serves as co-chair of the COBIT 5 Task Force. He has been a key member in the development of COBIT since its inception.

Derek J. Oliver, Ph.D., CISA, CISM

is the founder and CEO of UK-based Ravenswood Consultants Ltd., an information security and audit consultancy, and has more than 26 years of experience as a specialist in that field. He is a chartered fellow of the British Computer Society, a fellow of the Institute of IT Service Management and a member of the Institute of Information Security Professionals. Following two years as president of the ISACA London Chapter, he was appointed to the CISA Test Enhancement Committee (TEC) and was subsequently a member of the CISA Certification Board. After working on the Credentialing Task Force, he was appointed founding chairman of the CISM TEC. He was chairman of the BMIS development committee and is currently co-chair of the COBIT 5 Task Force and a member of ISACA's Framework Committee.

Maturity Models and IT Strategic Planning

By John Petrey

It is striking what is not part of most IT strategic plans.¹ They always cover the textbook strategic planning topics of documentation of the business strategy, assessment of the current environment, business application needs, IT infrastructure strategy, architecture strategy, sourcing strategy, alignment of IT strategies with the business strategy, etc., and are replete with tactical objectives to execute the strategy. What they seem to consistently miss is the IT organizational maturity required to successfully execute the strategy, the current state of maturity, and the strategy and tactics to address the maturity gap.

Without this, no IT strategic plan is complete, and its likelihood of success may be in doubt. In an IT organization, particularly one supporting a growing or turnaround company, is it realistic for IT to think it will be able to execute well against the IT strategic plan without ensuring that it is at the appropriate maturity level and, if not, is consciously raising its maturity level? Part of the problem is that IT often does not focus on maturity and, as a result, assumes that the way IT does business today is sufficient for it to be successful in the future, including as the company grows. Could this be part of the reason that there is more chief information officer (CIO) turnover than there should be?

Fortunately, there are a variety of maturity models available for collections of IT processes as well as IT specialty areas such as project management, architecture and software engineering. A few of the sources include the Capability Maturity Model (CMM) from Carnegie Mellon University, Gartner and COBIT. Generic maturity models are not as helpful in developing an IT strategic plan because they tend to lack specificity, which assists with developing the actions required to raise the capability maturity needed to support the business objectives. To be helpful for planning purposes, the maturity model must contain specific, objective criteria that are relevant to the goals of the plan and easily discernable by the planners. It must clearly illustrate different states of maturity that the planners can use to determine the current state and desired target state and to derive the steps needed to move the IT organization to the target state.

The maturity models of each of the COBIT processes can be a great resource for building the part of a comprehensive IT strategic plan that deals with IT capabilities, because it is one source that covers all of IT and has the characteristics noted previously. Other specialty maturity models can certainly be used, either separately or in conjunction with COBIT.

As part of developing any IT strategic plan, the IT management team—the entire IT management team, if practical—should perform a self-assessment of its maturity level based on the chosen maturity models. In doing so, it is important to be honest, challenge each other, and only claim to be at a maturity level for which consistent documentary evidence showing adherence to all aspects of maturity for that level can be provided. Next, the IT management team should determine, based on the business strategy and aspirations, the appropriate target maturity level for IT. Then, the gap should be reviewed; the strategy for each area developed; and the specific tactical objectives to move from the current state to the target state, including target dates and individual responsibilities, identified. And, of course, progress against the plan should be tracked.

This can be both enlightening and inspiring for the IT management team. It may be surprising, but frequently the management team will rally around making themselves best-in-class. In addition, the business will know how mature the IT organization is, and if it is not addressed and the maturity assessment and plans are not known and transparent, the IT strategic plan may lack some measure of credibility with the business and within IT.

Maturity models are a valuable resource and using them can make the IT strategic plan a great vehicle to garner additional support from the business to help raise IT maturity, help ensure successful execution of the plan, improve IT employee job satisfaction, and increase the success of the IT management team and CIO.

John Petrey

is CIO at First Niagara Bank. Previously, Petrey was CIO at Guaranty Bank and Banknorth and an executive with Fidelity Information Services. Named a top 100 CIO by *Insight Magazine*, Petrey is an IT executive with extensive experience in banking and technology and a proven track record of IT performance improvement, business-IT alignment and strategic planning. Throughout his career, he has repeatedly been tapped to turn around troubled areas and start up new business units.

Endnote

¹ This statement is based on the author's experiences in three tours as a chief information officer with growth and turnaround organizations.

Taking Governance Forward: A Call to Action

By Patrick Stachtchenko, CISA, CGEIT, CA

Enterprises exist to deliver value to their stakeholders. Delivering value is achieved by operating within a value and risk atmosphere that is acceptable and advantageous and by using resources responsibly. In a rapidly changing environment, speedy direction setting and a quick reaction to change are essential. Decision-making accountabilities must be shared among many people—and when accountability must be shared, governance comes into play. Successful enterprises ensure that they have implemented an overarching system of governance that facilitates the achievement of their desired outcomes, both at the enterprise level and at each level within the enterprise.

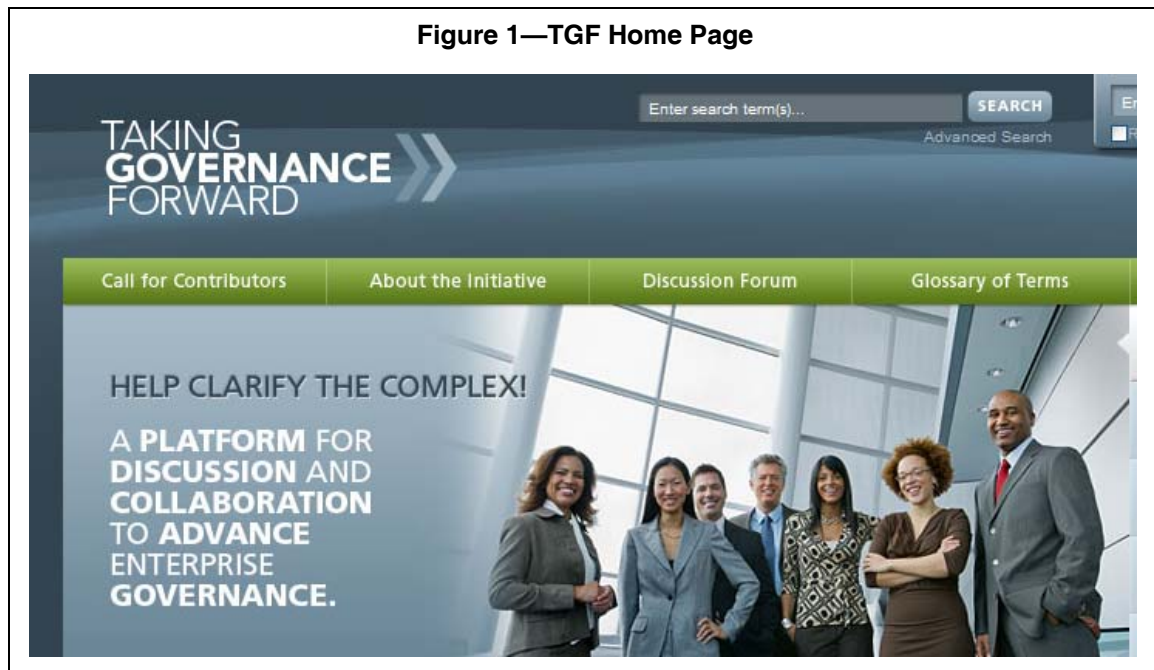
The Taking Governance Forward (TGF) site (see **figure 1**), which will be available beginning in May 2010, is the outcome of an initiative led by ISACA to provide a high-level overview of governance: its definition, objectives, components, participants and views. It is designed to be brief, simple, straightforward and practical, with a minimum use of theory.

The TGF initial content has been through several rounds of review by groups of individuals representing various job titles, years of experience, types of expertise and levels of engagement with governance issues. Now it is nearly time for others to provide input.

With its launch, both individuals and enterprises will be invited to build on and improve the contents of the TGF site. For example, individuals may wish to add to the list of standards and frameworks currently represented in the map, especially if a certain guidance document has been of particular use to them. Also, it is hoped that for areas of asset governance other than IT governance (e.g., human resources), enterprises serving those constituencies may wish to build a map of their own, specific to their professional discipline.

To facilitate and encourage this involvement, community interaction with the diagram maps and term definitions is supported through discussion forums and wikis. The contributions of the masses will help shape future releases of related material while providing a collaborative

Figure 1—TGF Home Page



understanding and acceptance of these concepts and frameworks.

To review the TGF materials and to collaborate in the discussions about the approach, please visit www.takinggovernanceforward.org following the web site launch in May, and share your enterprise governance experience, opinions and questions with other interested professionals.

Patrick Stachtchenko, CISA, CGEIT, CA

is a past international president of ISACA. He is a partner at Stachtchenko & Associés, a business consulting firm specializing in governance and performance improvement. Previously, he was responsible for Management Solutions, the management consulting practice of Deloitte France, and for the computer audit and risk management and IT consulting practices for Coopers & Lybrand France. He is also the chair of ISACA's Framework Committee and serves on ISACA's Knowledge Board, Strategy Advisory Council and Governance Advisory Council.

Key Success Factor: IT Resource Management

By Reinhold Thurner, Ph.D.

Information and the information processing infrastructure are enterprise resources like money, goods and labor. Therefore, IT resources need to be professionally structured, controlled and managed just as any other resource. The responsible action is to make sure that adequate IT resource management is in place. Organizations with a higher maturity level achieve substantial gains in cost, time and quality.

ERP4IT—Management of IT Resources

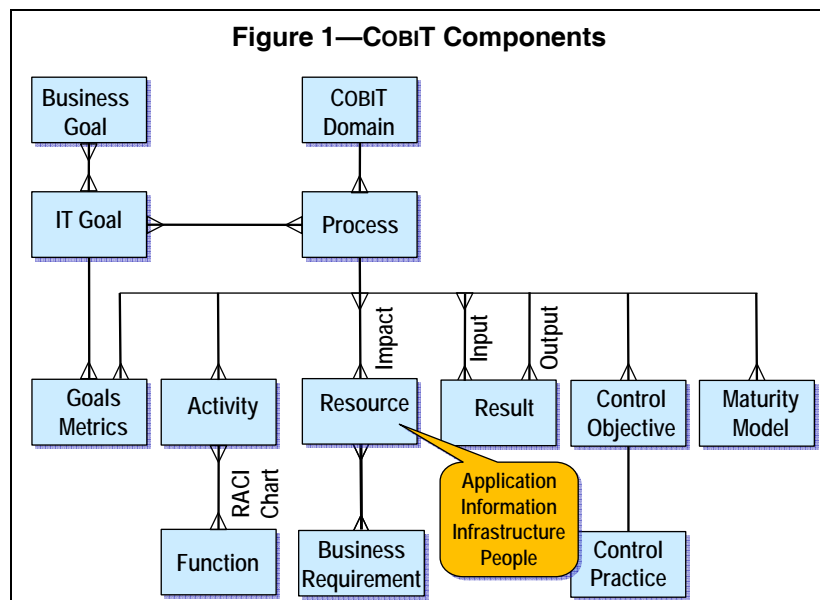
Professional management of resources is one of the key success factors for any medium to large organization. Enterprise resource planning (ERP) systems are used to control the processes, maintain proper records about the status and optimize performance. Such a system is the prerequisite to provide the information infrastructure not only for the control of ongoing operations, but also for business governance and strategic decisions.

Similar principles are also applicable to IT resources and IT resource management. Efecte Corp. (www.efecte.com) uses the term “ERP4IT” (enterprise resource planning for information technology) to describe automation of IT. ERP4IT focuses on automated IT and not on the automation of business processes by IT.

COBIT: The Definition of IT Resources

COBIT provides a generic framework for the control objectives of an ERP4IT system and defines people, information, applications and infrastructure as key resources for IT.

The (simplified) unified modeling language (UML) diagram (figure 1) shows the semantic structure of



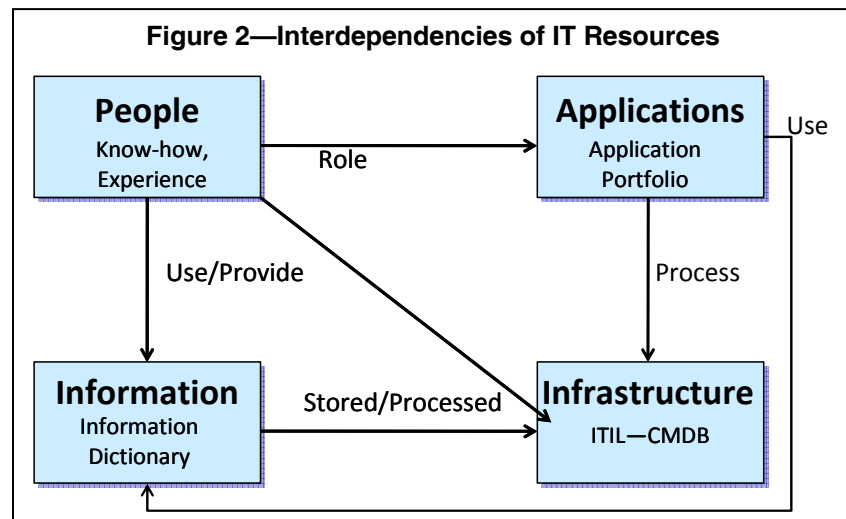
the components of COBIT and, among them, the role of IT resources. This kind of diagram is commonly used to describe the meaning (semantics) of the elements of a system in a graphical manner. It provides a quick, inside look into the basic structural principles of complex systems.

The line between “process” and “resource” with the “crowfoot” sign signifies that each resource is used by several processes and each process affects several resources, thereby creating a complex *m-by-n* network of interdependencies. PO3 shows that IT resources are used to fulfill business requirements; new business requirements drive investments to acquire new IT resources. That is, COBIT process PO3 *Define technological direction* requires accurate information about the existing status of the IT resources and the pending business requirements to plan new investments in applications, infrastructure and human resources.

The Structure of IT Resources

The introductions of new technologies (e.g., new applications) must be coordinated with the acquisition of the necessary infrastructure and also of the know-how to develop and maintain the new applications. Managing IT resources, therefore, requires also managing the dependencies among these resources. Examples for these dependencies are (see **figure 2**):

- People are responsible for the maintenance and the development of applications.
- Applications manage information.
- Applications use/are responsible for system components.
- System components use other system components.
- Information is stored and managed using an IT infrastructure.
- IT infrastructure is operated by people.



Managing Information About IT Resources

It is important for management to have precise information about the IT resources and their dependencies. When a problem arises, quick action is required; the source of the problem must be identified and the correct resource must be assigned to solve the problem. Planning and further development of applications is based on information about available resources, pending requirements and so forth.

Taking a more detailed look at one resource—the applications—there are normally a large number of applications in operation. They are sorted into application domains (or groups). Information about applications is maintained in an application portfolio. This includes not only descriptions and attributes of the applications, but also the Responsible, Accountable, Consulted and Informed (RACI) charts—the relationship of people in charge of the support and development of the applications.

Applications are constructed from technical components, where each component may be used in several applications and may use other components. Applications process business information. Without precise information about these interdependencies, problem support, development and

change management can be time-consuming and costly, and dangerous errors can also occur. COBIT rightly requests that a configuration management system be in place to keep track of these interdependencies and to maintain an information dictionary as a basis for data management.

From the business point of view, the focus is less on applications than on services provided to support the business processes within the organization. These services are generally described by service level agreements (SLAs) in a *service portfolio* detailing which services are provided and at what quality level and costs.

The services detailed in the SLAs can again use multiple components stemming oftentimes from different applications or application groups. Transparent and accurate information about these relationships is required to optimize the cost and the quality of IT services.

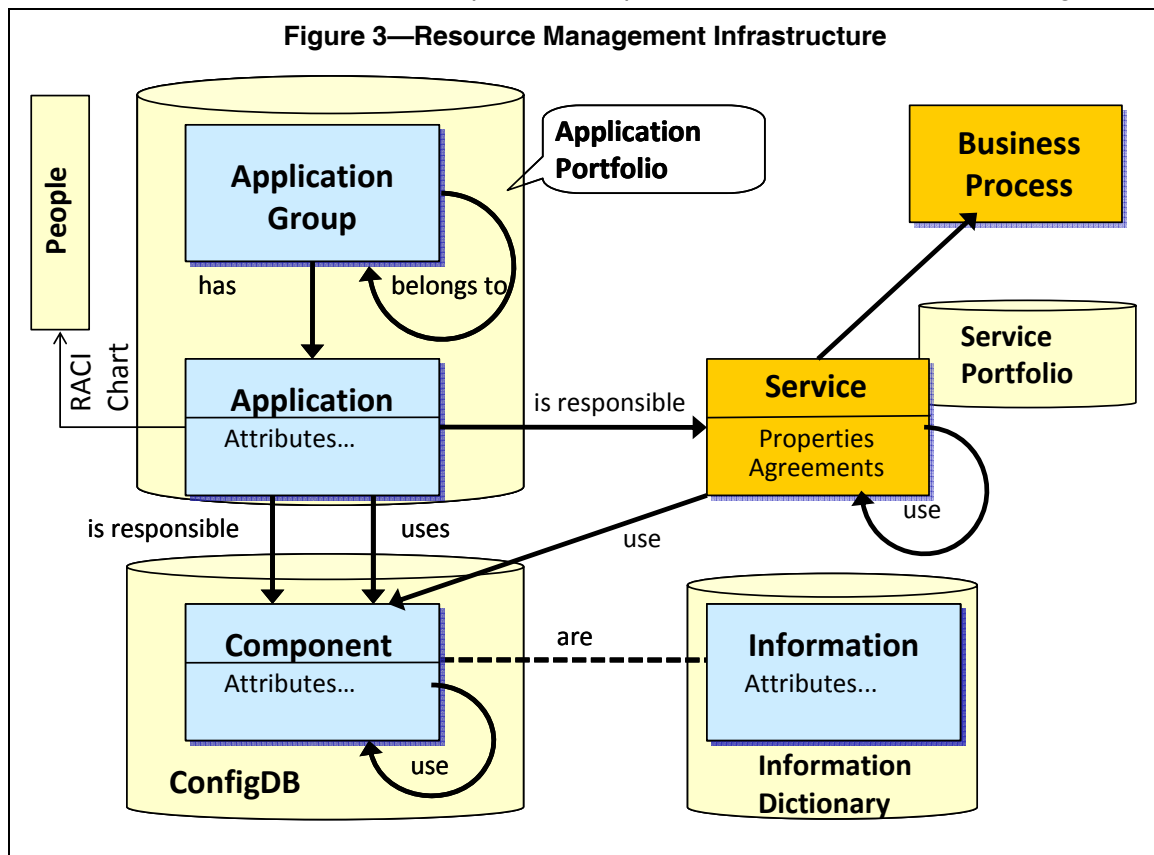
Maturity of IT Resource Management

A quick check of the maturity level reveals how well IT resources can be managed and what must be done to improve the performance, reduce cost, and monitor and improve quality (see **figure 3**):

- Are the applications and their interdependencies documented by an integrated application portfolio?
- Is business information managed in an information dictionary?
- Are the configuration management processes operational and is a configuration database in place?
- Is a services portfolio properly connected with the business processes and the system components?
- Do these systems logically fit together?
- Is all IT-related information that is required by the other domains of IT governance available?

IT Resource Management and IT Governance

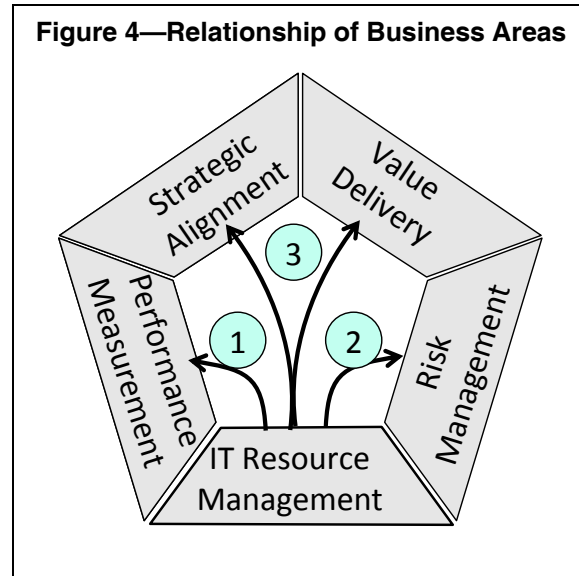
Management of IT resources is a prerequisite to run the business on the operational level in a secure and reliable manner. But it also provides the platform, structures and data to change the



business (see **figure 4**).

Performance measurement collects the key performance figures and consolidates them along the reporting lines of the organizational structure. The basic data for this process are provided by the resource management processes.

Risk management, as described in ISACA's Risk IT framework, provides guidance on handling risks related to items. The majority of these items are managed and cataloged by IT resource management, which can provide the necessary information to risk management, relieving risk management from needing to build up its own, and necessarily redundant, catalogs of risk items.



IT resource management deals with the existing resources and the processes to provide services as contracted in SLAs. The processes for continuous strategic alignment and improvement of value delivery reach beyond the current status. The application portfolio is supplemented by the portfolios of pending investment requests and in-flight projects to control the change process and renew, replace, reengineer or improve the status of the resources and operational processes.

This creates a strong relationship between IT resource management and the processes of value delivery, as described in ISACA's Val IT framework. IT resource management handles the current status and provides for the planning processes of value delivery, providing all necessary consolidated information. Portfolio management and investment management use this information to plan ahead and control the change processes to create the next version of operational resources.

Infrastructure for IT Resource Management

An ERP system is highly dependent on the availability of IT services to maintain proper records, provide information for decision makers and control the processes. The same is also true for the management of IT resources. The data volumes in ERP4IT are certainly smaller than in the ERP systems of the business. The volatility and complexity of ERP4IT systems are at least as complex. They include hundreds of different information types and relationships. Information about thousands of instances of each type must be managed.

One would expect that infrastructures to manage these data are generally established. In practice such a complete infrastructure is rarely in place. More often than not there are large collections of Excel spreadsheets, local databases and point-to-point data exchanges. This leads to unreliable information about IT resources with adverse effects on quality, security and cost.

The technical solutions to build a reliable infrastructure are available today. The new breed of federated repositories takes advantage of new technologies, such as the Internet and Java, and various frameworks and provides the necessary flexibility to maintain information about IT resources and manage the processes.

Responsibility for Planned Organizational Change

Installing new software, as usual, does not solve the problem on its own. Such fundamental changes must be properly planned, resources must be allocated, and clear goals must be set and controlled. One cannot expect that such a process is initiated from within IT itself—day-to-day duties and the obligation to keep the lights on leave little room for substantial organizational improvement. Investments in such infrastructures are “invisible” to the business. They are

postponed often to the end of the investment list and are the first victims of cost-cutting programs.

It is the responsibility of IT governance to keep the big picture in mind, to monitor the performance, and to initiate and control improvement processes. It is the responsibility of IT auditors to assess the situation, report deficits and, thereby, contribute to the necessary process of organizational change. By doing so, an organization will not only decrease cost, but also increase quality, reliability and effectiveness and reduce risks.

Reinhold Thurner, Ph.D.

is chief executive officer and founder of Metasafe GmbH (Switzerland). The main areas of his work comprise compilers, application generators, metasystems, repositories and information modeling.

COBIT Focus is published by ISACA. Opinions expressed in *COBIT Focus* represent the views of the authors. They may differ from policies and official statements of ISACA and its committees, and from opinions endorsed by authors, employers or the editors of *COBIT Focus*. *COBIT Focus* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Please contact Joann Skiba at jskiba@isaca.org.

Framework Committee

Patrick Stachtchenko, CISA, CGEIT, CA, France, chair
John W. Lainhart, IV, CISA, CISM, CGEIT, USA
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
George Ataya, CISA, CGEIT, CISM, Belgium
Robert G. Parker, CISA, CA, CMC, FCA, Canada
Derek J. Oliver, CISA, CISM, CFE, FBCS, UK
Sergio Fleginsky, CISA, Uruguay
Rolf M. von Roessing, CISA, CISM, CGEIT, Germany
Jo Stewart-Rattray, CISA, CISM, CGEIT, Australia
Robert E. Stroud, CGEIT, USA
Steven Babb, CGEIT, UK

Editorial Staff

Jane Seago, Chief Communications Officer
Jennifer Hajigeorgiou, Senior Editorial Manager

Comments regarding the editorial content may be directed to Jennifer Hajigeorgiou, senior editorial manager, at jhajigeorgiou@isaca.org.



©2010 ISACA. All rights reserved.