

# COBIT®

# Focus

*The newsletter dedicated to the COBIT® user community*

July 2008, Volume 3

## Applying COBIT With Limited Resources

By Matthew Altman

Many midsize and small businesses, IT departments, and organizations in general look at best practices and governance as procedures into which they will grow eventually. Common justifications for not improving include waiting until they have enough people, the department has a larger budget or the current projects are completed.

What is often overlooked is the value of implementing best practices, which can drive goals that help build growth, enhance talent, attract clients, expand services and improve response to problems. There are also those organizations that desire to improve, but do not know how and need a guide.

*Control Objectives for Information and related Technology (COBIT®)* provides a useful framework for recognizing existing strengths and needs, improving processes that will provide noticeable improvements, and creating metrics to gauge the maturity of the business environment. It is possible to do this with existing personnel, and, through incremental implementation, costs can be controlled. The following recommendations are directed at business and IT management with limited budgetary or personnel resources.

### Define Goals and Objectives

To apply COBIT within an organization, goals and objectives must be identified. The best source is a previously defined set of management objectives or a strategy that has long-term goals. Being reasonable is a key element.

With limited resources, two to five foundation goals could be identified. A foundation goal is something that the business, as a whole, can build upon or use for necessary expansion of departments. One that is common is improving communications; another is improving project management and oversight; and a third is reducing costs associated with purchasing and management of systems. With goals identified, partners within the company can be sought.

### In This Issue...

#### Applying COBIT With Limited Resources

By Matthew Altman.....page 1

#### Val IT Framework 2.0: Relationship Between COBIT and Val IT

By John Thorp.....page 3

#### Combining Information Technology Standards to Strengthen Network Security

By Keith Harrell and Taiye Lambo.....page 6

#### New IT Risk Management Framework: How It Relates to COBIT

By Urs Fischer.....page 10

ISACA COBIT Education .....page 13

Continued on page 2

Partners from departments such as internal audit, accounting or perhaps the organization's largest client/vendor, can provide valuable input on objectives that address real needs. The business objectives will guide the organization toward control objectives, which can be mapped to the framework using the current COBIT® 4.1 documentation. There are several mapping tools, available in the appendices of COBIT, that provide control objectives relating to more common goals and objectives for business and IT.

### Resource Constraints

An organization's objectives may map to more control objectives than are wise to implement under existing resource constraints. In this context, the following questions should be asked with respect to the four domains of the COBIT framework (Plan and Organize [PO], Acquire and Implement [AI], Deliver and Support [DS], and Monitor and Evaluate [ME]):

- Does the organization have weaknesses or problems? If the answer is no, then the ME objectives may provide an accurate assessment of the existing structure. Every organization has weaknesses and problems, but they may not be known or self-evident.
- Does the business regularly suffer from low user satisfaction, or significant budget constraints for purchasing new equipment? Low resources available for technology maintenance and replacement can often lead to support problems and higher downtime. To address these issues, control objectives in the DS domain may be appropriate.
- Is there a common concern regarding the security, maintenance and provision of needed tools for

mobile users? This could identify a need for improvement related to objectives in the AI domain.

- Was it difficult to find support materials for goals and objectives? This may identify a need for management to develop guiding documentation, create a strategy and review policies—all of which are done through the PO domain.

These questions do not apply to every organization, so other questions may be necessary to ensure a focused approach that allows for stepwise progress. Limiting the initial approach can provide the recognition and planning of future objectives to meet through new controls.

### Stepwise Improvement and Limited Resources Are Not Free

Unfortunately, governance implementation and process improvement are similar to a New Year's resolution to lose weight. Both require work, time and a willingness to continue, even when it seems overly difficult. Where possible, existing opportunities to improve should be utilized; this could include previously planned implementations of new hardware, purchases of new software or introducing new training materials for computer-security awareness. This can lead to some delays in projects or additional costs in time and materials. The opportunity to familiarize and adapt with an ongoing project can be considerably easier than determining all the necessary changes after implementation, and may reduce the burden on users and administrators to implement control objectives at a later time. Other components to

[Continued on page 3](#)



## Call for Articles

for COBIT® Focus

COBIT® Focus is the  
COBIT-based electronic newsletter.

For more information contact  
Jennifer Hajigeorgiou at [publication@isaca.org](mailto:publication@isaca.org)



consider are the costs of downtime, research, and maintaining compliance with applicable industry and government regulations.

### **Establishing Value**

The expected outcome is an established financial value or recognized improvement for internal or external processes and relationships. Value components for small and midsize businesses include:

- Alignment of business processes
- Faster or more comprehensive response to problems
- Reduction in and reduced impact from catastrophes
- Long-term solution planning
- Improved communication for IT, business managers and employees
- Improved services for clients

### **Conclusion**

Improving processes is an ongoing task that can require significant work. Using a stepwise approach can make the application of COBIT manageable and affordable. Business and IT management can build objectives to implement existing strategies and goals, and overcome known weaknesses.

### **Matthew Altman**

is the information systems internal auditor for Arctic Slope Regional Corp., located in Anchorage, Alaska, USA. He was previously the IT manager for a regional accounting firm, and is a board member and past president of the Alaska Surveying and Mapping Conference Corp. In addition, his consulting firm provides software development services, training and review services to the financial, education and scientific communities.

## **Val IT Framework 2.0: Relationship Between COBIT and Val IT**

### **By John Thorp, CMS, ISP**

Val IT™, from the IT Governance Institute® (ITGI™), provides a governance framework and proven practices to help enterprises manage the challenge of realizing value from investments involving IT. Val IT is applicable to all enterprises and addresses all aspects that should be contained in defining, evaluating, selecting and managing any IT investment.

In a recent Forrester paper, Craig Symons stated, "Organizations struggling to execute IT strategies that deliver business value and to communicate this value to stakeholders should evaluate Val IT as a tool for improved value delivery."<sup>1</sup>

Although primarily targeted at investments involving IT, the practices included in Val IT apply across the board in most, if not all, business-change investments, whether or not they involve IT.

**The Relationship Between Val IT and COBIT**  
COBIT, first released in 1996, provides an IT governance framework from the point of view of the IT function. In recent years, however, it has recorded management practices that straddle the IT and business areas, and began recognizing the need for practices beyond IT. Val IT now provides a framework that responds to that recognition and

need, and is the first comprehensive framework to support the enterprise point of view of IT governance, with a focus on value.

The primary focus of the Val IT domains—Value Governance (VG), Portfolio Management (PM) and Investment Management (IM)—is on delivering business value by:

- Establishing governance practices that provide for a clear and active linkage among the enterprise strategy; the portfolio of IT-enabled investment programs that execute the strategy; and the portfolios of resulting IT services, assets and other resources (VG)
- Managing the overall investment portfolio to optimize value to the enterprise (PM)
- Managing the results of individual investment programs, including business, process, people, technology and organisational change, enabled by the business and IT projects that make up the programs (IM)

The primary focus of the COBIT domains—Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME)—is on delivering the technology capabilities, services, assets and other resources that the business functions need to implement and

---

Continued on page 4

sustain business change through:

- Planning and organizing the enterprise IT processes and IT resources (PO)
- Acquiring and implementing, through a portfolio of technology projects, the technology capabilities, services, assets and other resources that are required to support the business change programs and the ongoing operation of the enterprise (AI)
- Delivering and supporting, on a day-to-day basis, those technology capabilities, along with portfolios of existing services, systems and supporting infrastructure (DS)
- Monitoring and evaluating portfolios of IT services, assets and other resources to ensure that they continue to enable the business to create optimal value and to identify and initiate any improvements in IT that could increase value creation, through further potential investment programs (ME)

The links between COBIT and Val IT are enabled by portfolio mechanisms and investment management, and provided in the IT processes that deal with strategy and portfolios (PO1), investments and budgets (PO5), solution delivery (PO10), service management (DS1), and performance reporting (ME1).

Comparing how COBIT and Val IT focus on governance, processes and portfolios further helps to understand the relationship between the two frameworks, as shown in **figure 1**.

**Original Val IT Framework**

The first edition of Val IT, released in March 2006, represented an important step in the evolution of ISACA, ITGI and COBIT. As the core publication in the Val IT series, *Enterprise Value: Governance of IT Investments, The Val IT™ Framework*, presented processes and key management

practices for three domains: VG, PM and IM.

The original Val IT framework publication was primarily targeted at new IT-enabled business investments—significant business investments in sustaining, growing or transforming the business with a critical IT component, where IT is a means to an end—the end being to contribute to the process of value creation in the enterprise.

**The Val IT Framework 2.0**

The latest edition, *Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0*, extends Val IT beyond new investments to include IT services, assets and other resources. It does this by identifying a broader range of operational IT portfolios that might be added as a result of investments managed by Val IT, but which would be managed by COBIT, and by providing “hooks” for the performance of those portfolios to be reported back to Val IT. It also aligns terminology more closely with COBIT and adds management guidelines, similar to the COBIT management guidelines. These include inputs and outputs to illustrate what processes (including COBIT processes) need from others and what the processes typically deliver; activities and associated roles and responsibilities; and goals and metrics, which are based on a consistent cascade of Val IT domain goals, process goals and activity goals. Version 2.0 of the framework also includes maturity models for the three Val IT domains.

The high-level interrelationships between *The Val IT Framework 2.0* domains and processes are illustrated in **figure 2**.

*The Val IT Framework 2.0* is available in two forms: an extract and a full version. The extract is intended for the reader who wants an overview of

Continued on page 5

**Figure 1—Comparison of COBIT and Val IT to Governance, Processes and Portfolios**

Comparison of Val IT With COBIT			
	Governance Focus	Process Focus	Portfolio Focus
Val IT	Enterprise governance of IT	<ul style="list-style-type: none"> <li>• Programme design and initiation</li> <li>• Benefit realisation</li> <li>• Investment and ongoing value management aspects of all processes</li> </ul>	<ul style="list-style-type: none"> <li>• Manage the investment portfolio</li> <li>• Provide the overall view of portfolio performance</li> </ul>
COBIT	IT governance	<ul style="list-style-type: none"> <li>• IT solution delivery</li> <li>• IT operational implementation</li> <li>• IT service delivery</li> </ul>	<ul style="list-style-type: none"> <li>• Manage the IT project portfolio in support of investment programmes</li> <li>• Manage the IT service, asset and other resource portfolios</li> <li>• Provide information on the performance of the IT service, asset and other resource portfolios</li> </ul>

Source: IT Governance Institute, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008

Val IT without the detail, and includes the first four chapters of the full document, which provide:

- An introduction to the challenge of value, and the need for a comprehensive and structured governance framework
- An introduction to Val IT
- Key Val IT terms, principles and domains
- An overview of Val IT processes, including high-level management guidelines, maturity models, and the relationship between Val IT and COBIT

The full document is intended for the reader who needs a detailed understanding of Val IT. It includes two additional chapters that provide:

- Detailed Val IT process and key management practice descriptions, including detailed management guidelines and maturity models
- A breakdown of accountabilities and responsibilities for Val IT activities by function

**Future Direction**

ITGI is moving toward having a comprehensive, complete, coherent and consistent suite of frameworks and supporting products that will be consistent with an overall architecture and aligned with the needs of different constituencies. To that end, work is currently underway on a risk framework, which will complement and be consistent with Val IT and COBIT (see the article on

page 10). The changes included in *The Val IT Framework 2.0* are intended to move in this direction. It is anticipated that the next releases of these three frameworks will take the next steps in this direction.

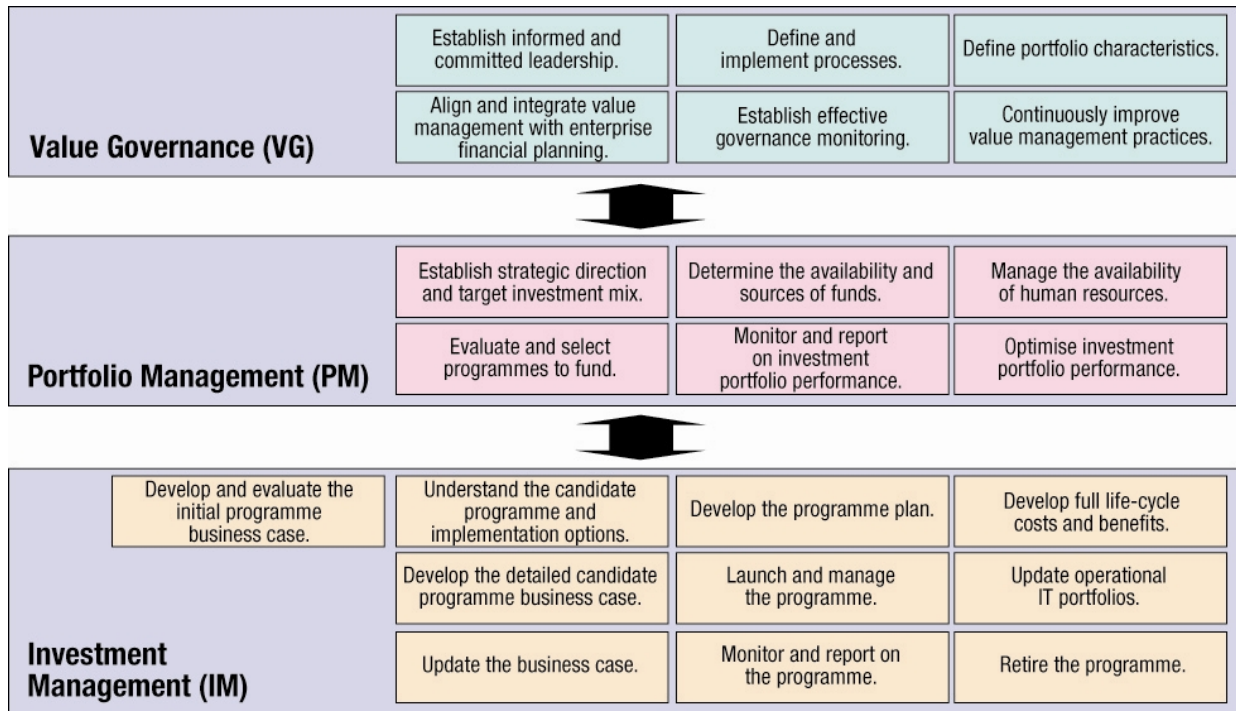
**Conclusion**

Executives may not recognize that many of the day-to-day business issues they face involve issues of value management, even if they relate to the need for more effective governance and management of IT. Val IT provides proven value management principles, processes and practices to enable enterprises to maximize the delivery of business value from investments in IT. COBIT complements Val IT by providing the framework for the execution of the IT-related aspects of investments, including IT solution delivery, IT operational implementation and IT service delivery. The risk management framework mentioned earlier will make the picture even more complete.

Together, these frameworks will provide the most comprehensive overall guidance to enterprises for the effective governance and management of the delivery and use of IT, and will enable enterprises to maximize value by optimizing benefits at an

[Continued on page 6](#)

**Figure 2—High-level Interrelationships Among Val IT Framework 2.0 Domains and Processes**



Source: IT Governance Institute, *Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0*, USA, 2008

affordable cost with a known and acceptable level of risk.

**John Thorp, CMC, ISP**

is president of The Thorp Network Inc. and a consulting fellow with Fujitsu Consulting. He is an internationally sought-after management consultant with 45 years of experience in the information management field. Author of *The Information Paradox*, Thorp’s focus is on helping organizations realize the benefits of IT-enabled change. Over the last five years, his work has extended beyond IT to the broader issues of enterprise value management and strategic governance. Working with ITGI, he has been a lead developer of Val IT, and is currently chair of the Val IT Steering Committee and a member of the IT Governance Committee.

**Editor’s Note:**

*Enterprise Value: Governance of IT Investments*, *The Val IT Framework 2.0* and *Enterprise Value: Governance of IT Investments, Getting Started With Value Management* are the two latest releases in the Val IT series. They are available along with *Enterprise Value: Governance of IT Investments, The Business Case* and *Enterprise Value: Governance of IT Investments, The ING Case Study* at [www.itgi.org/valid](http://www.itgi.org/valid) and [www.isaca.org/bookstore](http://www.isaca.org/bookstore).

© 2008 John Thorp. All rights reserved.

**Endnote**

<sup>1</sup> Symons, Craig; *From IT Governance to Value Delivery*, Forrester Research, 22 June 2007

## Combining Information Technology Standards to Strengthen Network Security

**By Keith Harrell, CISA, and Taiye Lambo, CISA, CISM, CISSP, BS 7799 LA, HISP**

The recent wave of high-profile security breaches has indicated to a number of corporations that they need to have a Statement on Auditing Standards (SAS) No. 70 audit and/or an International Organization for Standardization (ISO) certification to strengthen network security. The US continues to lead other nations in the occurrences of loss of critical data. The number of records lost or stolen has steadily increased each year (see **figure 1**).<sup>1</sup> When an organization suffers a data breach, it costs approximately US \$197 per lost record. That means if a company loses 100,000 records, it would cost close to US \$20 million.

Fees to correct data breaches continue to be excessive when losses occur, as organizations must strengthen internal controls, educate the consumer on the impact of data loss and pay

legal retainer fees. As a result, enterprises should integrate the implementation of COBIT and ISO standards to achieve a holistic standard that substantially strengthens network security.

**COBIT Framework**

COBIT is used by many companies to provide a framework for corporate governance and implementation of internal controls. COBIT includes the essential business and IT process controls and objectives needed to achieve corporate objectives. COBIT is written at the management level and driven by business requirements, and identifies what should be managed and measured to achieve effective network security. Standards are most appropriate when used as a starting point, and specific practices can be mapped to the COBIT network security framework.

**Figure 1—Increase in Lost/Stolen Data 2002-07**

Year	Records Lost/Stolen
2007	162,563,703
2006	49,679,333
2005	55,986,942
2004	31,895,900
2003	6,405,000
2002	4,960

COBIT is divided into four high-level domains of logically grouped processes—Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME)—that cover the essential IT operational areas. The domains consist of a number of IT processes, 34 in total, that are defined to provide a structure within which to implement policies and procedures and to reduce the risk that undesired results are not

Continued on page 7

detected. For each process, a description and related control objectives, management guidelines and a maturity model are provided in the framework. Assurance guidelines are also available separately, in the *IT Assurance Guide*, to provide operations advice on how to monitor processes and make improvements.

### ISO Information Technology Standards

ISO standards contain more detailed instructions on implementation of network security for operational management and can be mapped to the COBIT framework.<sup>2</sup> Essential parts of ISO 17799:2005 (now renamed ISO 27002:2005), *Information Technology—Security Techniques—Code of Practice for Information Security Management*, were developed and published by BSI British Standards. The ISO Technical Committee publishes the international standards. These standards can provide a basis for developing reliable and detailed security standards and management practices within an organization.

These best practices provide detailed instructions relating to protection and nondisclosure of personal data, protection of internal information, protection of intellectual property rights, information security policy, assignment of responsibility for information

security, problem escalation, and business continuity management. A framework for development of an organization-specific network security system is presented and consists of:

- A security policy
- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Information security incident management
- Business continuity management
- Compliance

### Combining Standards and COBIT

To achieve a holistic solution leveraging COBIT and ISO, management must first align IT strategy with business objectives. In many companies, IT strategy is not considered a true partner, but is a service provider only. As a partner, IT will be challenged to increase business revenue and will be required to focus on the most critical network security internal controls. For example, a company highly dependent on wireless networks should have the following internal controls in place:

[Continued on page 8](#)

## COBIT Research Update

COBIT-related publications scheduled for availability in the third quarter of 2008 include:

- *Aligning COBIT® 4.1, ITILv3 and ISO/IEC 27002 for Business Benefit*
- *COBIT® Mapping: Mapping of COSO Enterprise Risk Management 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: Mapping of ITILv3 With COBIT® 4.1*
- *COBIT® Mapping: Mapping to NIST SP800-53 With COBIT® 4.1, 2<sup>nd</sup> Edition*
- *COBIT® User Guide for Service Managers*
- *Guide to Managing and Controlling Applications Using COBIT®*
- *IT Governance and Process Maturity*
- *Identifying and Aligning Business Goals and IT Goals: Full Research Report*
- *Understanding How Business Goals Drive IT Goals*

COBIT initiatives scheduled to start development in 2008:

- *COBIT® Mapping: Mapping of PMBOK 2 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of CMMI With COBIT® 4.1*
- *COBIT® Mapping: Mapping of BS 25999 With COBIT® 4.1*
- *COBIT® Quickstart—Tools and Support*

An updated version of the Val IT framework, *Enterprise Value: Governance of IT Investments*, *The Val IT Framework 2.0*, and a new publication in the Val IT series, *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*, will be available in the ISACA Bookstore in the third quarter of 2008.

- Enable available security features to reap their benefit, because embedded security features are often disabled by default.
- Change the default settings for the service set identifier (SSID), and define a complex name for the wireless network.
- Disable the Dynamic Host Configuration Protocol (DHCP), and instead use static IP addresses to prevent unauthorized access.
- Move or encrypt the SSID password and the Wired Equivalent Privacy (WEP) key, which are typically stored in the Windows registry file, to make it more difficult for a hacker to acquire privileged information.
- Do not broadcast the SSID; use a closed network instead of an open network, so the SSID is not broadcast. In addition, periodically changing the name is a good practice.

If alignment of priorities is not performed, IT may be concentrating on disaster recovery or application support and not on these essential wireless network controls. IT priorities should be aligned with those of the business strategy, to effectively mitigate the most relevant risks. This will also increase return on investment.

Next, one should understand how network security standards tie together. To derive the benefits from ISO standards and the COBIT framework, a risk-based approach to information security management should be taken. The risks within the organization that are more likely to occur and affect the computing networks should be identified. The organization should concentrate on the incidents that are more likely

Continued on page 9

Figure 2—Cross-referencing COBIT

COBIT v4 Mapping to ITIL, COSO and ISO 27002	ITIL V2										COSO (Original)				ISO 27002:2005																							
	Business Perspective	Application Management	Infrastructure Management	Security Management	Service Support					Service Delivery					Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring	Information Security Policy	Organization of Information Security	Asset Management	Human Resources Security	Physical and Environmental Security	Communications and Operations Management	Access Control	Information Systems Acquisition, Development and Maintenance	Information Security Incident Management	Business Continuity Management	Compliance								
					Incident Management	Problem Management	Configuration Management	Change Management	Release Management	Service Level Management	Capacity Management	Availability Management	IT Service Continuity Management	Financial Management for IT Services																								
<b>PO—Plan and Organize</b>																																						
P01	Define a strategic IT plan	x	x																																			
P02	Define the information architecture		x																																			
P03	Determine technological direction		x																																			
P04	Define the IT processes, organization and relationships	x																																				
P05	Manage the IT investment																																					
P06	Communicate management aims and direction	x																																				
P07	Manage IT human resources	x																																				
P08	Manage quality	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
P09	Assess and manage IT risks	x																																				
P10	Manage projects		x																																			
<b>AI—Acquisition and Implementation</b>																																						
A11	Identify automated solutions		x	x																																		
A12	Acquire and maintain application software		x																																			
A13	Acquire and maintain technology infrastructure			x																																		
A14	Enable operation and use			x																																		
A15	Procure IT resources																																					
A16	Manage changes																																					
A17	Install and accredit solutions and changes																																					
<b>DS—Delivery and Support</b>																																						
DS1	Define and manage service levels																																					
DS2	Manage third-party services																																					
DS3	Manage performance and capacity																																					
DS4	Ensure continuous service																																					
DS5	Ensure systems security																																					
DS6	Identify and allocate costs																																					
DS7	Educate and train users	x																																				
DS8	Manage service desk and incidents																																					
DS9	Manage the configuration																																					
DS10	Manage problems																																					
DS11	Manage data																																					
DS12	Manage the physical environment																																					
DS13	Manage operations																																					
<b>ME—Monitor and Evaluate</b>																																						
ME1	Monitor and evaluate IT performance	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
ME2	Monitor and evaluate internal control																																					
ME3	Ensure regulatory compliance																																					
ME4	Provide IT governance	x																																				

to occur and result in damages, and identify and prioritize the implementation of countermeasures to strengthen the security posture.

**Figure 2<sup>3</sup>** demonstrates how internationally accepted best practice standards/frameworks of ISO and COBIT cross-reference to one another at the control objectives and controls levels.

The hybrid approach probably makes more sense for most enterprises to strengthen network security controls. The obvious benefit of this integrated approach is that enterprises are able to demonstrate that they have good internal controls over financial processes and, even more important, that they will mitigate potential network security risks. By implementing this holistic approach, internal controls will be comprehensive. Management will then have ongoing measurements to maintain and monitor network security and identify possible data security breaches sooner.

A holistic approach will also assist in meeting industry, legal, contractual and regulatory requirements imposed on an enterprise. As a result, a sustainable and effective network security management program will be adopted, managed and monitored by combining implementation of standards.

### Help Others Learn About COBIT

COBIT is benefiting enterprises internationally, and there is a great demand for case studies that describe different implementations.

The experiences described in a COBIT case study are effective ways to share what is working well and what challenges enterprises have faced. Submitting material for a case study is easy. Simply contact [news@isaca.org](mailto:news@isaca.org) or +1.847.660.5566 to receive details and a list of questions. Examples of full implementations are not necessary. Many enterprises use only portions of COBIT or use it in only very specific areas; all kinds of uses make good case studies.

ISACA staff members will draft the case study based on the information supplied and send it back for the submitter's review and approval. Once the case study is approved, it will be included on the COBIT case study sections of the ISACA and ITGI web sites and possibly in internal and external publications and marketing materials.

Forward-thinking enterprises that take this integrated approach will also be able to meet Sarbanes-Oxley, SAS 70 and ISO requirements. In addition, there are efficiencies and cost savings that result from taking a hybrid approach. Ultimately, enterprises will end up with a strong and robust network security management system, based on international best practices. This approach will increase shareholder value, strengthen competitive advantage, and ensure customer and business partner information assurance.

#### **Keith Harrell, CISA**

is president of SAS70ExPERT.biz and the former senior manager with the Global SAS70 Practice of the Reznick Group P.C. Harrell has 12 years of financial, operational and IT audit experience with private and *Fortune* 500 companies. In addition to being a subject matter expert in SAS 70 audits, he is also COBIT trained. He has expertise in performing risk assessments in numerous industries and determining compliance with COBIT and many national and international standards, to provide a holistic approach and cost-efficiencies to corporations.

#### **Taiye Lambo, CISA, CISM, CISSP, BS 7799 LA, HISP**

is the founder and chief technology officer of eFortresses Inc. He has expertise as a hybrid technical and business information security expert with a pragmatic holistic approach to the management of information security and regulatory compliance, and is a subject matter expert on information security governance and compliance relating to regulatory requirements. He founded the UK HoneyNet project, [www.honeynet.org.uk](http://www.honeynet.org.uk), and the Holistic Information Security Practitioner (HISP) Institute, [www.hispi.org](http://www.hispi.org). He can be reached at [tlambo@eFortresses.com](mailto:tlambo@eFortresses.com).

#### Endnotes

- <sup>1</sup> Etiolated Consumer/Citizen, <http://etiolated.org>
- <sup>2</sup> The *Aligning COBIT<sup>®</sup>, ITIL and ISO 17799:2005 for Business Benefit* publication is being updated to reflect ISO 27002:2007. *Aligning COBIT<sup>®</sup> 4.1, ITILv3 and ISO/IEC 27002 for Business Benefit* is expected to be available shortly. For more information on this and other COBIT mappings, please visit [www.isaca.org/cobitmapping](http://www.isaca.org/cobitmapping).
- <sup>3</sup> The mapping in **figure 2** was developed by the authors and it does not necessarily match the official COBIT mappings, published by ITGI.

## New IT Risk Management Framework: How It Relates to COBIT

By Urs Fischer, CISA, CIA, CPA Swiss

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

### Why Is It Important?

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

Therefore, the new risk-oriented framework, expected to be available by the end of 2008, will round out ITGI's full coverage of IT governance by

covering the risk management component. The other four focus areas of IT governance—strategic alignment, value delivery, resource management and performance measurement—are addressed by ITGI's other two internationally tested and globally adopted frameworks: COBIT and Val IT.

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

### What Will It Cover?

The framework aims to fill the gap between

Continued on page 11



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

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

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

Further detail about these principles can be found in *Enterprise Value: Governance of IT Investments, The Val IT Framework*, available from [www.isaca.org/valit](http://www.isaca.org/valit).

generic risk management frameworks and standards such as the Committee of Sponsoring Organizations of the Treadway Commission’s *Enterprise Risk Management (COSO ERM)* and the Australian/New Zealand standard AS/NZS4360 on one hand, and detailed (mostly security-related) IT risk management frameworks and standards on the other. Indeed, the goal of this framework is to enable enterprises to understand and manage all IT-related risks (beyond security), and to address all aspects (beyond operational management of IT) when managing risk.

The current ITGI frameworks, material and concepts, contained therein, are used and capitalised to the maximum possible extent. Indeed, ITGI wants to create a coherent set of frameworks all aimed at providing the user with the best possible guidance on IT governance.

ITGI’s IT-ERM Task Force has analysed a large number of already-established and existing standards and frameworks for concepts and components that could be re-used—it made no sense to reinvent already-existing and good material. The use and benefit of ITGI’s new framework lies in the fact that it will not be cast in stone, but that it will evolve over time, taking into account new ideas, evolving technologies and organisational theories. It will also be complemented with additional guidance to help the risk management practitioner to the maximum extent possible. Many of the existing frameworks have a focused view on risk, e.g., addressing security risk. This framework will address all IT-

related risks at all levels throughout the enterprise, i.e., starting from strategic risk and going down to very operational risk.

**Benefits and Outcomes**

The new framework will cover the following requirements of the intended audiences:

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

**How It Relates to COBIT**

The COBIT framework provides a generally accepted control framework (amongst many other things), but it does not provide the full detail required for comprehensive risk management. COBIT’s applicability in terms of risk management is shown in **figure 1**.

Since the new IT Risk Management Framework

Continued on page 12

**Figure 1—COBIT’s Applicability to Risk Management**

		COBIT 4.1 Product Suite	Comment
		Full	
		Partial	
		Not Applicable	
<b>A</b>	Comprehensive view on risk management, not only mechanical/technical	Partial	The risk dimension is mentioned throughout the framework.
<b>B</b>	Specific for the subject matter, i.e., IT-related	Full	COBIT is all about IT controls.
<b>C</b>	End-to-end view on the subject matter, i.e., complete view on IT-related risks	Partial	COBIT does not describe IT-related risk in any explicit form, although the risk management dimension is present implicitly throughout the framework. COBIT also goes beyond pure security risk.
<b>D</b>	Business-oriented	Partial	COBIT provides a link to business goals and IT goals, thus providing a business orientation.
<b>E</b>	Provide a continuous process, from risk identification to continuous monitoring and feedback	Not Applicable	COBIT is a process model, but is not specific to risk, or risk management is not made explicit; it is also not an end-to-end model for risk management.
<b>F</b>	Cover all risk treatment options	Not Applicable	COBIT specifies IT controls, but without linking them back to specific risks; it also does not describe other risk treatment options in detail.
<b>G</b>	Availability/accessibility of the framework	Full	COBIT is publicly and freely available.

deals with risk management, which is an integral part of good enterprise governance, it has been decided to (re-)use and reference all relevant components in other frameworks. In essence, the new framework will extend COBIT (and Val IT) coverage by providing ERM guidance and support, adapted to focus on IT-related aspects of IT governance and management.

The new framework can be used and understood as a stand-alone framework, but a basic understanding of COBIT and Val IT's most important definitions will result in a better understanding of the new IT Risk Management Framework. Indeed, the new framework considers both the upside and downside views of risk, i.e., risk as a threat/hazard on one hand, and as an opportunity on the other. From there, it is a logical step to COBIT, with its control focus, and to Val IT, with its focus on value generation.

The new framework defines a number of guiding principles of effective risk management of IT-related business risk; these principles are based on generally accepted risk management principles and have been applied to the domain of IT. Built upon these principles are, amongst others, a number of processes (grouped in three domains) that build upon the core components to identify all activities required—from executive to operational management—for proper risk management. The process model is familiar to COBIT and Val IT users, i.e., substantial guidance is provided on the key activities within the process, who is responsible, which information flows between processes and how one can measure the performance of the process.

So far, the general relationship of the new framework to COBIT has been described; however, there is also a close relationship when it comes to internal control. A major risk factor, confirmed by some studies as the most important one, is the presence or absence of good control measures. Indeed, good control measures can have a positive influence on:

- Reducing the business impact when events happen
- Reducing the likelihood that events will happen
- Reducing the likelihood that, when events happen, a business impact will occur
- Increasing the likelihood that correct investments are made and projects are successfully completed

There are many ways to classify and structure controls, and in the new framework the COBIT control objectives and related control practice statements have been maintained as the major reference source. The COBIT framework provides several levels of detail on control, starting at the process level, through control objectives down to the control practice steps.

### Summary

Like COBIT and Val IT, the new IT Risk Management Framework will be vendor-, application- and platform-neutral. It will not be focused on any particular legislation or regulation, but will instead consist of internationally accepted good practices for the identification, assessment and mitigation of IT risk across an enterprise. For all IT professionals, the new framework will be a valuable addition to the already existing material from ITGI and ISACA®.

### Urs Fischer, CISA, CIA, CPA Swiss

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

### Editor's Note:

The new framework is expected to be available before the end of 2008. More information on the IT Risk Management Framework will be posted at [www.itgi.org](http://www.itgi.org) as it becomes available.

### 2008 Calendar of ISACA COBIT Events

- |                      |                                                                                                                                                                                                         |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 15-19 September..... | ISACA® Training Week<br>(including COBIT-specific training)<br>Edinburgh, Scotland, UK<br><a href="http://www.isaca.org/trainingweek">www.isaca.org/trainingweek</a>                                    |
| 6-7 October.....     | IT Governance Using COBIT®<br>and Val IT™ course at the IT<br>Governance, Risk and<br>Compliance Conference in<br>Orlando, Florida, USA<br><a href="http://www.isaca.org/itgrc">www.isaca.org/itgrc</a> |

## ISACA COBIT Education

Looking for ways to build the internal competencies that support the adoption of COBIT and IT governance?

ISACA provides COBIT training in several formats. All ISACA classroom-based courses are delivered by ISACA-accredited trainers. The following are some highlighted COBIT training opportunities available through ISACA.

### COBIT User Convention

The COBIT® User Convention was designed to facilitate discussion and debate among experienced COBIT users and to focus on discussion around applications, solutions and approaches.

Each convention is two days in length and features case studies and facilitated discussion groups that address how COBIT is used from governance and assurance perspectives. Conventions are offered through ISACA chapters to serve COBIT users in the geographic areas.

To learn more about these events, please visit [www.isaca.org/cobituserconvention](http://www.isaca.org/cobituserconvention).

### COBIT Steering Committee

Robert E. Stroud, USA, chair  
Gary S. Baker, CA, Canada  
Rafael Eduardo Fabius, CISA, Uruguay  
Urs Fischer, CISA, CIA, CPA (Swiss), Switzerland  
Erik Guldentops, CISA, CISM, Belgium  
Jimmy Heschl, CISA, CISM, Austria  
Debbie A. Lew, CISA, USA  
Maxwell J. Shanahan, CISA, FCPA, Australia  
Dirk E. Steuperaert, CISA, Belgium

### 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](mailto:jhajigeorgiou@isaca.org).

### COBIT Campus

The COBIT® Campus, [www.isaca.org/cobitcampus](http://www.isaca.org/cobitcampus), provides access to a number of online COBIT and related courses and exams.

### COBIT Training Week

ISACA is proud to be offering a new and unique Training Week course in 2008. The COBIT Training Week integrates ITGI's research and ISACA's current COBIT educational courses into a single, comprehensive, COBIT training program.

The course begins with an emphasis on IT issues, governance concepts, control and risk management, and how COBIT provides the framework and tool set to meet the challenge of managing IT resources, to make available the best information assets for business success. It follows with a thorough explanation of how to implement an IT governance process using the *IT Governance Implementation Guide, 2<sup>nd</sup> Edition*, and Val IT. During the course, the *IT Assurance Guide*, based on COBIT 4.1, will also be presented and illustrated.

Lecture, discussion, case studies and exercises are used to help the participant understand proper implementation techniques to achieve optimum results for managing IT resources and properly documenting controls for compliance.

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

© 2008 ISACA and IT Governance Institute. 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](mailto:jskiba@isaca.org).