

In This Issue:

- **Toward Better IT Governance With COBIT 5**
- **Introducing the New COBIT Assessment Programme: Why and How It Is Replacing the COBIT Maturity Model**
- **Why Do IT Process Improvement Initiatives Struggle?**
- **Updated COBIT Mapping Overview Publication Released**
- **Using COBIT to Support IT Risk Management**



Come join the discussion! Alpaslan Menevse will be responding to questions in the **discussion area of the COBIT—Use It Effectively** topic beginning 24 October 2011.

Toward Better IT Governance With COBIT 5

By Alpaslan Menevse, CISA, CRISC

As an advisory and regulatory body, the Basel Committee plays a very important role in structuring the global banking sector. The latest guidance publications from Basel have one common viewpoint: the need for sound governance practices for all banks around the world. Today, from banking to all lines of business, so much is dependent on IT, and it is almost impossible to separate IT governance from enterprise governance. This dependency raises a need for an integrated framework to satisfy the needs of business and fulfill the demands of good governance practices.

The upcoming **COBIT 5**, an exposure draft of which was released earlier this year, with the final document expected in early 2012, strikes with important changes in governance processes, proving that COBIT is not intended for IT audit only, which is a common misconception. One of the most important changes with COBIT 5 is the precise definitions of “governance” and “management” and their respective responsibilities, which help to define clear roles and responsibilities for all stakeholders. The COBIT 5 Evaluate, Direct and Monitor (EDM) process set is designed to govern and encapsulate the processes of all other management processes. This major upgrade in COBIT 5 is intended to increase awareness of the need for a structured governance framework for all organizations at an enterprisewide level, from operations to the strategic board.

In general, governance practices are considered at their best when they are linked and embedded as continuous management life cycles, such as enterprise risk management, in all processes within an organization. COBIT 5 will enable organizations to implement auditable, dedicated IT governance processes and measurable performance metrics, which are among the biggest and most valuable changes in COBIT 5.

COBIT 5, like COBIT 4.1, offers an easy-to-implement mapping tool to map the strategic objectives of an organization to related IT objectives in order to achieve the required governance model.

Call for Articles

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

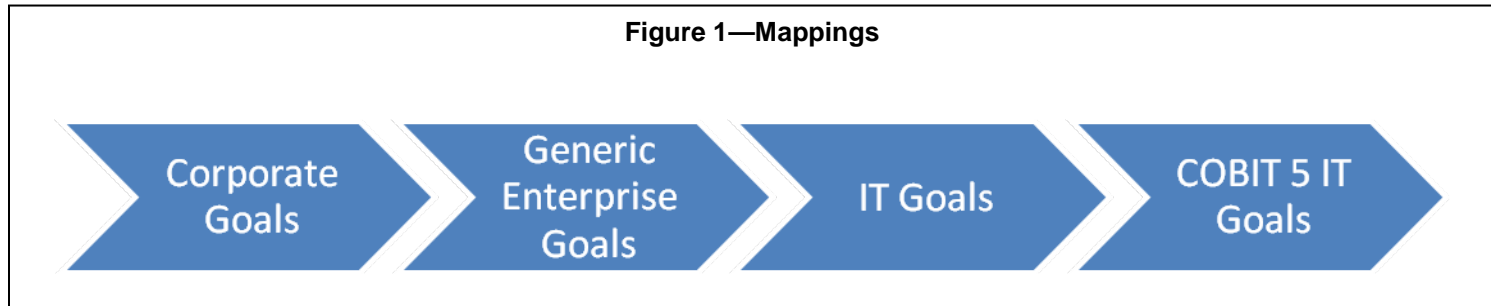
Submit articles on your experiences with these frameworks. Deadline to submit copy for volume 1, 2012: 5 December 2012

Submit articles for peer review to: publication@isaca.org

Case Studies

Visit the ISACA [Case Studies](#) page to read more.

Figure 1—Mappings



One way to analyze these mappings is to draw a COBIT process occurrence chart from the result of the mappings. The process occurrence chart represents the result of one of the sample mappings (**figure 1**). The organization's corporate goals are mapped to the generic enterprise goals. Those are then mapped to IT goals, which are then mapped to the COBIT 5 IT goals. The result can be summarized by a COBIT IT process graph displaying the number of occurrences of COBIT processes after all mappings are done (**figure 2**). The graph can be interpreted as the dependency of corporate strategic goals on COBIT 5 processes. As the relative number of occurrences increases related to a specific process, interdependency of corporate goals also increases proportionally, which affects the conditional ability of goal achievement and demonstrates the need for more attention on the related governance practices of this process.

For organizations that have already implemented COBIT or that are planning to implement the framework for the first time, a good starting point is to conduct a gap analysis throughout the organization, starting from the governance framework to tactical-level policies and then operational-level processes. After a gap analysis and an assurance audit, the process capabilities can be assessed. Therefore, COBIT process occurrence values, as shown in the process dependency graph (**figure 2**), are a good indicator of where to focus. They enable senior management to ensure that the resources are allocated where most needed to achieve objectives. A process occurrence chart can also be used as a relative weighting factor between different domains. Of course, the mapping can be adjusted and balanced with other objectives such as risk management and compliance functions on an as-needed basis.

Sample Case

In a sample case involving a growing bank, the corporate goals were:

- Improvement of the sales culture and number of customers
- Correct localization for the target group
- Increased effectiveness of the organization
- Increased effectiveness of the marketing strategy and processes
- Cost control

After all mappings were done in the sample case, it was shown that APO04 *Manage innovation*, a new process from the Align, Plan and Organize (APO) process set in COBIT 5, occurred a total of 20 times. Enabling new products by innovation in the IT domain was found to be the crucial element for achieving the corporate goals of the bank. One can conclude that, from the governance perspective, all objectives will not be met without achieving a high-enough capability score for the innovation process.

Suggested sample primary metrics for IT goals for APO04 include the:

- Percentage of business process owners who are satisfied with supporting IT products and services
- Percentage of IT-enabled investments in which benefit realization is monitored through the full economic life cycle

Suggested sample metrics for process goals for APO04 include:

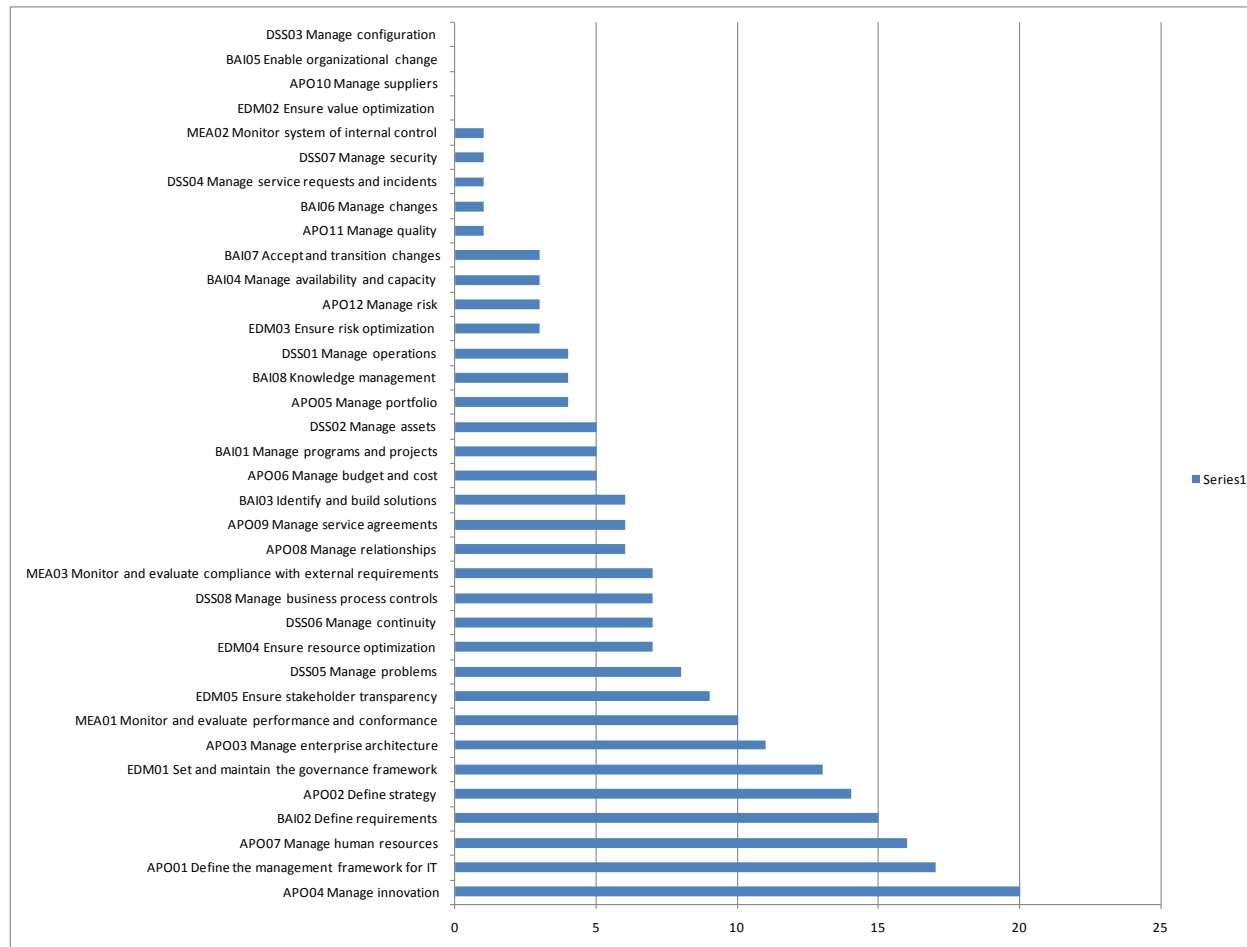
- An increase in market share or competitiveness due to innovations
- The percentage of implemented initiatives with a clear link to an enterprise objective

Process APO07 *Manage human resources* has an occurrence score of 16 in the sample case, which is also consistent with the objectives. Having highly skilled IT personnel and a competitive human resources policy plays an important role in achieving the enterprise goals.

Suggested sample primary metrics for IT goals for APO07 include the:

- Percentage of personnel whose IT-related skills are sufficient for the competency required for their role
- Number of approved initiatives resulting from innovative IT ideas

Figure 2—COBIT IT Process Graph



As shown in **figure 2**, one of the most important processes in the sample case is EDM01 *Set and maintain the governance framework*, which is also a new process in COBIT 5. EDM01 plays a key role in the overall COBIT 5 framework. The purpose of the process is explained in *COBIT® 5: Process Reference Guide Exposure Draft*:

*Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements is confirmed, and the governance requirements for board members are met.*¹

Some of the suggested process metrics for EDM01 include:

- Actual vs. target cycle time for key decisions
- The degree by which agreed-upon governance principles for IT are evidenced in processes and practices (the percentage of processes and practices with clear traceability to principles)

The capability of EDM processes should be seen as a crucial success factor in the overall COBIT 5 framework. Therefore, necessary emphasis and priority should be allocated by the governance bodies.

Advances in COBIT 5

An important update in COBIT 5 is the use of the process capability model from ISO/IEC 15504 *Information technology—Process assessment* instead of the maturity model structure found in COBIT 4.1. This is a major change and must be studied extensively. The overarching COBIT 5 framework and its addenda will provide more concentrated information while preserving the information's integrity and ensuring proper enterprise governance.

The information model is also renewed in COBIT 5 such that it considers information as both a product and a service, covering all aspects of information attributes for different perspectives, referred to as the “information cycle.” In the information cycle, business processes generate and process data, transforming them to information and knowledge and, ultimately, generating value for the enterprise. The information cycle will enable organizations to implement necessary policies and procedures and to set required information quality attributes for all stakeholders.

Conclusion

Current global economic conditions impose very tight regulations for business governance. Additionally, proper governance of an enterprise is one of the biggest concerns of all stakeholders. With the aid of an enterprise governance concept, better utilization of IT governance methods will continue to be one of the hot topics in the foreseeable future. The latest studies show that there is still much to achieve on the governance and management sides of IT, especially in relation to the blurred roles and responsibilities of business and IT.² Adoption of COBIT 5 is one of the best opportunities to clarify and solve these issues. As an IT governance framework, COBIT 5 can be integrated with other standards and practices. COBIT 5's comprehensive structure and easy adaptability promises better IT governance for all areas as well as for all members of the financial sector.

Alpaslan Menevse, CISA, CRISC

is the operational risk manager, enterprise risk management project facilitator and a member of the audit committee at Sekerbank. He represents the enterprise on the Banks Association of Turkey Operational Risk Sub-Committee. Menevse's current focus includes the human side of change management in organizations. He was a subject matter expert on the *CRISC™ Review Manual 2011*.

Reference

ISACA, *COBIT® 5: The Framework Exposure Draft*, USA, 2011

Endnotes

¹ ISACA, *COBIT® 5: Process Reference Guide Exposure Draft*, USA, 2011

² See the following:

Banking Regulation and Supervision Agency (BRSA), “The Regulation on the Internal Systems of Banks,” *Official Gazette*, 1 November 2006, no. 26333, www.bddk.gov.tr/WebSitesi/english/Legislation/8839internalsystems03032011.pdf

BRSA, “Regulation on the Bank's Corporate Management Principles,” *Official Gazette*, 1 November 2006, no. 26333, www.bddk.gov.tr/WebSitesi/english/Legislation/8805eng_corporatemanagement_10_06_2011.pdf

Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance*, Bank for International Settlements, Switzerland, 2010, www.bis.org/publ/bcbs176.pdf

Basel Committee on Banking Supervision, *Principles for the Sound Management of Operational Risks*, Bank for International Settlements, Switzerland, 2011, www.bis.org/publ/bcbs195.pdf

Directorate for Financial and Enterprise Affairs and Organisation for Economic Co-operation and Development (OECD) Steering Group on Corporate Governance, *Corporate Governance and the Financial Crisis: Conclusions and Emerging Good Practices to Enhance Implementation of the Principles*, OECD, France, 2010, www.oecd.org/dataoecd/53/62/44679170.pdf

European Banking Authority, *EBA Guidelines on Internal Governance (GL 44)*, European System of Financial Supervision, UK, 2011, [www.eba.europa.eu/cebs/media/Publications/Standards%20and%20Guidelines/2011/EBA-BS-2011-116-final-\(EBA-Guidelines-on-Internal-Governance\)-\(2\)_1.pdf](http://www.eba.europa.eu/cebs/media/Publications/Standards%20and%20Guidelines/2011/EBA-BS-2011-116-final-(EBA-Guidelines-on-Internal-Governance)-(2)_1.pdf)

International Organization for Standardization (ISO), *ISO 31000:2009 Risk management—Principles and guidelines*, Switzerland, 2009, www.iso.org/iso/iso_catalogue/management_and_leadership_standards/risk_management.htm

Research Update

COBIT 5

The next steps in the development of the COBIT 5 publications are to finalize the following in 2011 and prepare them for release in the first quarter of 2012:

- *The Framework*
- *The Process Reference Guide*
- *The Implementation Guide*

Visit the [COBIT 5 Initiative](#) page for status updates.

COBIT PAM

The *COBIT Process Assessment Model (PAM): Using COBIT 4.1* is available on the ISACA web site as a complimentary PDF download for members and is available for purchase in the ISACA Bookstore.

Newly Released 3rd Edition
COBIT Mapping: Overview of International IT Guidance, 3rd Edition, is available on the ISACA web site as a complimentary PDF download.

Introducing the New COBIT Assessment Programme: Why and How It Is Replacing the COBIT Maturity Model

By Max Shanahan, CISA, CGEIT, FCPA, MIIA (Australia), SMAC

As part of the ISACA strategy, a task force was created to determine whether there was a need to provide a formal assessment approach based on the COBIT framework. The task force reviewed common assessment options in use, principally the Software Engineering Institute (SEI) Capability Maturity Model (CMM)/Standard CMM Integration (CMMI) Appraisal Method for Process Improvement (SCAMPI) approach (on which the COBIT maturity model [MM] in COBIT 4.1 is loosely based) and the International Organization for Standardization (ISO) approach.

Both approaches provide guidance on such topics as the level of evidence required for an assessment and the skills required of competent assessors. Evidentiary requirements and assessor skills and competencies are required to deliver reliable and repeatable results in a formal assessment approach.

ISACA decided to adopt ISO/IEC 15504-2:2003 *Information technology—Process assessment—Part 2: Performing an assessment*, which is sometimes referred to as Software Process Improvement and Capability dEtermination (SPICE). This decision reflects, in part, recognition of recent market activity in the process assessment arena, including the publication of materials that support both the Committee of Sponsoring Organizations of the Treadway Commission's *Internal Control—Integrated Framework* and ITIL Version 3 assessments using the ISO approach. This selection also recognised that the approach should continue to support COBIT users who want to benchmark process capabilities and develop process improvement plans.

Why Should COBIT Users Consider Utilising This New Assessment Approach?

The ISACA task force recognised that process assessment aspects such as the rigorous definition of process capability, evidence of achievement of process outcomes/outputs (as capability indicators), demonstration of assessor competence, and reliability and repeatability of COBIT-based process assessment results needed to be established to improve the rigour, reliability and, therefore, comparability of the results obtained, which are essential for effective use of the results in benchmarking activities. This market approach improvement includes the need for development of a scheme for training and certifying assessors on both relevant COBIT content and the assessment process to be applied, which supports the consistency of assessment performance and results.

The assessment approach also includes ISO/IEC 15504-4:2004 *Information technology—Process assessment—Part 4: Guidance on use for process improvement and process capability determination*, which 'provides guidance on how to utilise a conformant process assessment within a process improvement programme'. This is important for COBIT users who use the process MMs in COBIT 4.1 to develop process improvement plans. It also aligns with the ISACA publication *Implementing and Continually Improving IT Governance* and provides sound guidance on progressing process improvement based on an as-is/to-be analysis approach.

In addition to delivering immediate added market value from process capability assessment results in their own right (more reliable process capability assessment results provide a superior basis from which process improvement plans can be developed) and providing a sound basis for process improvement planning, such improvements can also provide the basis for the establishment of broader maturity assessments that may be of value to certain enterprises and their customers, should such a demand arise.

Finally, a less-rigorous self-assessment option will be included within the COBIT Assessment Programme. This simple approach is based on the same process assessment model (PAM) as the formal assessment approach (i.e., the same process attributes and indicator guidance), but is judgement-based and does not require formal evidential requirements to be satisfied. This option may be all that some COBIT users need to address their process improvement planning needs, or it may be used as a precursor to undertaking more rigorous formal evidence-based assessments.

What Is the Market Perspective?

The ISACA task force conducted a survey to determine the market perspective on the proposed COBIT-based process

assessment. In particular, the task force wanted to establish the perceived need and value to an enterprise of a process capability assessment based on ISO/IEC 15504, using COBIT 4.1 as the process reference model, performed by trained and certified assessors.

The survey was specifically aimed at senior enterprise leadership with the goal of obtaining an enterprise, rather than individual, perspective. Respondents included:

- Chief officers (17 percent)
- IT directors/managers/consultants (19 percent)
- IT audit directors/managers/consultants (16 percent)
- Compliance/risk/privacy directors/managers/consultants (16 percent)
- Security directors/managers/consultants (13 percent)

Survey respondents came from the professional areas of audit/assurance (30 percent), control/risk/compliance (24 percent), security (20 percent) and IT governance (18 percent).

The survey found that 88.8 percent of these senior, experienced respondents agreed that there is a need for, and value in, a rigorous and reliable IT process capability assessment. Additionally, the survey found that 92 percent agreed that there is a need for, and value in, having trained and certified assessors perform the work.

What Will ISACA Provide?

Under the COBIT Assessment Programme, the following products will be released progressively. The initial release, following the successful completion of pilot assessments, will occur in a staggered pattern beginning with September 2011's release of:

- **COBIT® Process Assessment Model (PAM): Using COBIT® 4.1:**
 - Based on COBIT 4.1 and ISO/IEC 15504, this model is the basis for the assessment of an organisation's IT processes against COBIT 4.1. The assessment process is evidence-based to enable a reliable, consistent and repeatable assessment process in the area of governance and management of IT.
 - The assessment model enables internal assessments by organisations to support process improvement.

Note: Process reference model requirements have also been provided as input to the COBIT 5 initiative for consideration in the design of the updated framework.

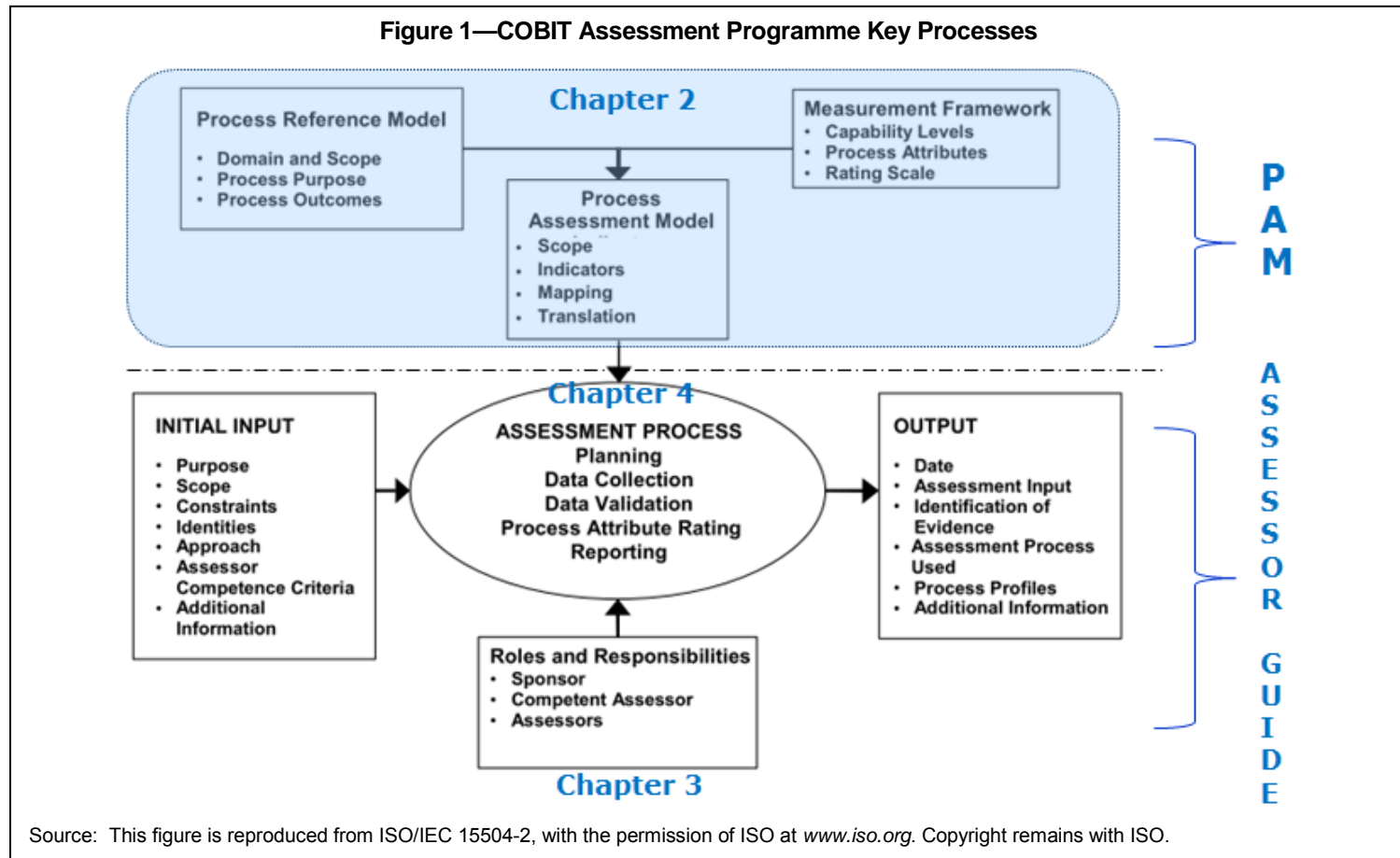
Following later this year will be:

- **COBIT® Assessor Guide: Using COBIT® 4.1**—This guide will be used to support a formal assessment and will be available for anyone wanting to undertake an assessment of this nature.
- **COBIT® Self-assessment Guide: Using COBIT® 4.1**—This guide will be used to support an informal assessment and is being developed for enterprises to perform self-assessments and to create their own process improvement plans.
- **Supplementary tools**—These will be offered to support process assessment activities and will include scoping templates. The tools will support the *COBIT Assessor Guide* and the *COBIT Self-assessment Guide* and will include mappings to:
 - Business goals
 - IT goals
 - IT governance focus areas
 - The US Sarbanes-Oxley Act
 - Cloud computing

The *COBIT PAM* and *COBIT Self-assessment Guide* provide a simple approach that will enable process improvement planning and can act as preparation for a more formal and full assessment in the future. Please note that undertaking a self-assessment does not comply with the rigour of an ISO 15504 assessment as the *COBIT Self-assessment Guide* does not include evidentiary requirements.

Figure 1 highlights the key processes in the COBIT Assessment Programme, and the guides address them.

ISACA is still considering how best to provide the required COBIT and assessor training elements of this approach. A COBIT Assessment Programme training and certification programme scheme is currently being developed for COBIT 4.1 and will be established for COBIT 5, following finalisation of the framework development in early 2012. Once the development of the *COBIT 5 Process Reference Guide* is complete, ISACA will begin the development of COBIT Assessment Programme products based on the new material.



Comparisons to the COBIT 4.1 Maturity Model

COBIT PAM uses a measurement framework that is similar in terminology to the MMs developed for each of the 34 COBIT 4.1 IT processes (referred to here as the COBIT 4.1 MM); however, there are differences. The primary difference is that, as shown in **figure 2**, the process maturity or capability levels (depending on the measurement framework used) are expressed in different terms:

- The COBIT 4.1 MM uses a scale based on the SEI CMM (a precursor to SEI CMMI).
- *COBIT PAM* uses the same scale as ISO/IEC 15504.

The assessment for the COBIT 4.1 MM is based on a set of requirements that are specified for each process. These are broadly based on the generic MM with six maturity attributes contained within COBIT 4.1; however, the requirements are not granular and are, therefore, not structured to support a rigorous assessment. The purpose is to identify where process capability issues are and how to set priorities for their improvement.

As discussed previously, *COBIT PAM* uses the capability assessment approach defined in ISO/IEC 15504. The aim is to provide a rigorous, objective and repeatable assessment of process capability.

The key outcome from these different assessment approaches is that the assessment results (in terms of levels) may well be different because *COBIT PAM* uses nine process capability attributes and defines more precise assessment criteria and evidence requirements than the COBIT 4.1 MM, and these requirements need to be achieved incrementally to progress through the assessment levels. This is not the case in the COBIT 4.1 MM approach, which results in a profile of conditions relevant to several maturity levels—without the intention to measure levels precisely or to certify that a level has exactly been met.

While it is possible that processes will be rated at the same level under the two approaches, the probability is that processes will gain a lower rating under an assessment undertaken against *COBIT PAM* due to the incremental approach taken in achieving higher-level performance (i.e., the need for the lower-level attributes to be fully addressed before higher levels can be reached) and due to the broader array of attributes to be assessed.

How to Use the COBIT Assessment Programme Approach

The objectives for using this approach are to:

- Determine the capability of the assessed entity to perform COBIT processes in a rigorous and reliable way.
- Facilitate the improvement of IT processes in an enterprise.

Because of its robustness, repeatability and basis on a recognised international standard, the COBIT Assessment Programme may, in the future, allow enterprises to provide to their customers assurance that specified IT processes (scoped using COBIT) are at a specific capability level.

One of the fundamental aspects of the COBIT Assessment Programme approach is that all entities that are being assessed must fully achieve level 1 before higher-level assessments are possible. Level 1 is where the specific outcomes and evidentiary requirements for each of the COBIT 4.1 processes outlined in the process reference model section of the PAM are undertaken. This

is a crucial first step, and enterprises that have completed assessments using the COBIT 4.1 MM may find that they have not yet reached that level in the PAM.

The second key aspect of the new approach is that, from levels 2 to 5, generic outcomes, base practices and work products are used as defined in ISO/IEC 15504.

The third key aspect is that the scoring or rating (shown in **figure 3** for each process capability attribute) must conform to the rating scale defined in ISO/IEC 15504.

This rating scale is used to ascertain the appropriate level; **figure 4** shows the tie into the levels.

It is very important to understand that, even if a process is assessed as largely achieving its purpose at any given level, for

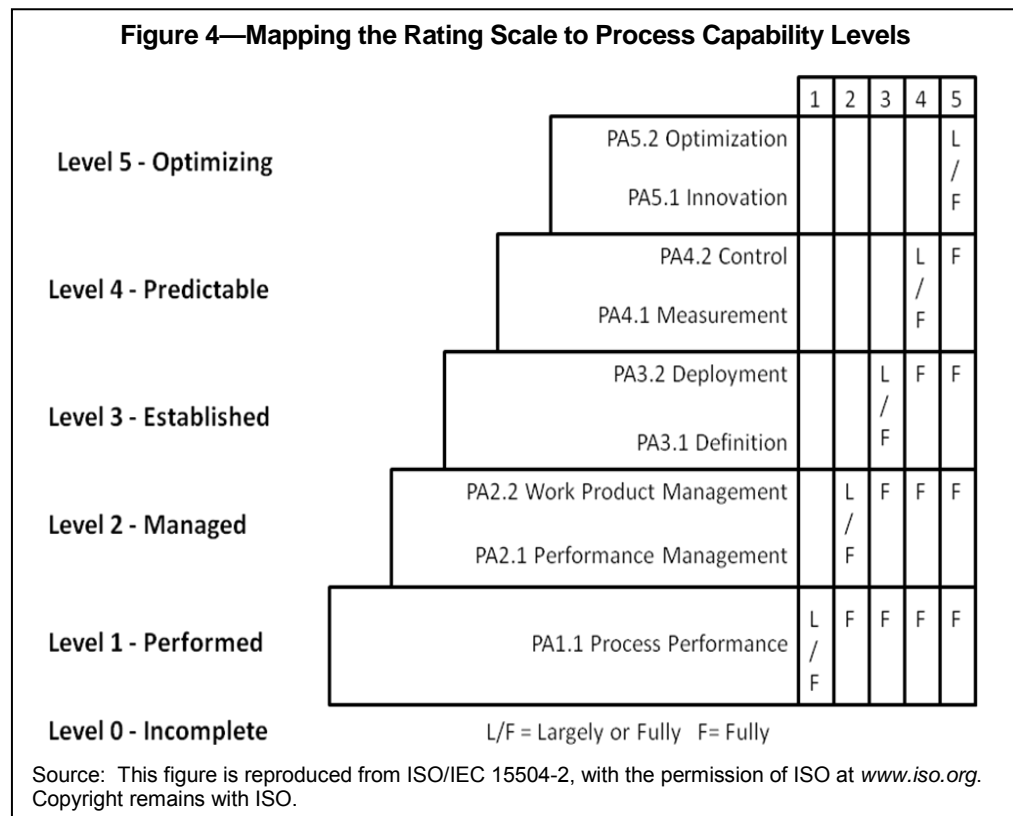
Figure 2—Terms Used for Process Maturity/Capability			
COBIT 4.1 MM Levels	Capability Levels Based on ISO/IEC 15504	Meaning of the Capability Levels Based on ISO/IEC 15504	Context
5—Optimising	5—Optimised	Continuously improved to meet relevant current and projected enterprise goals	Enterprise view/corporate knowledge
4—Managed and measurable	4—Predictable	Operates within defined limits to achieve its process outcomes	
3—Defined	3—Established	Implemented using a defined process that is capable of achieving its process outcomes	
N/A	2—Managed	Implemented in a managed fashion (planned, monitored and adjusted) with appropriately established, controlled and maintained work products	Instance view/individual knowledge
N/A	1—Performed	Achieves its process purpose	
2—Repeatable 1— <i>Ad hoc</i> 0—Non-existent	0—Incomplete	Not implemented or little/no evidence of any systematic achievement of the process purpose	

Figure 3—Rating Scale		
Rating	Percentage	Description
N—Not achieved	0-15	There is little or no evidence of achievement of the defined attribute in the assessed process.
P—Partially achieved	>15-50	There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of achievement of the attribute may be unpredictable.
L—Largely achieved	>50-85	There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed process. Some weakness related to this attribute may exist in the assessed process.
F—Fully achieved	>85-100	There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process.

it to be assessed as performing at a higher level of capability, the process must improve those attributes that are 'largely achieved' to 'fully achieved'.

Conclusion

The process assessment aspects of the COBIT Assessment Programme from ISACA include the rigorous definition of process capability, evidence of achievement of process outcomes/outputs (as capability indicators), demonstration of assessor competence, and reliability and repeatability of COBIT-based process assessment results needed to improve the rigour, reliability and, thus, comparability of the results obtained. The programme will include the development of a scheme for training and certifying assessors on both relevant COBIT content and the assessment process to be applied. Once fully in place, the programme will provide a sound basis for IT professionals and enterprises to further leverage COBIT framework guidance for the benefit of the profession and enterprise stakeholders.



Max Shanahan, CISA, CGEIT, FCPA, MIA (Australia), SMAC

is a specialist in IT audit, project risk assessment and IT governance improvement services, and his experience encompasses the management of IT and the evaluation of IT systems and practices. Shanahan has 45 years of IT and IT audit experience with five years of experience as an IT consultant and 15 years as executive director of IT at the Australian National Audit Office, where he was responsible for the provision of IT services and IT audit activity for all of Australia. Shanahan is the chair of the ISACA COBIT Enterprise Assessment Task Force and also represents the association at International Organization for Standardization meetings on governance of enterprise IT. He was the project editor for AS/NZ 8016 and is the project editor for ISO/IEC 35802.



Come join the discussion! Delton Sylvester will be responding to questions in the [discussion area of the COBIT—Use It Effectively](#) topic beginning 24 October 2011.

Why Do IT Process Improvement Initiatives Struggle?

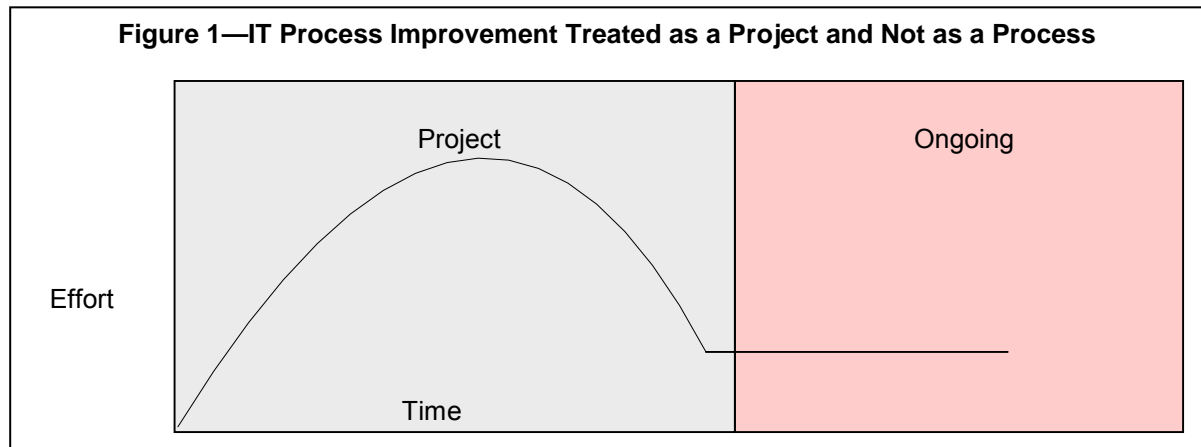
By **Delton Sylvester, CISA**

Often, IT process improvement initiatives struggle and fail to deliver the value that was initially envisaged. This article covers some of the main reasons why this is the case and presents some possible solutions.

Reasons Why IT Process Improvement Initiatives Often Struggle

Some of the top reasons that IT process initiatives often struggle to deliver the intended value or have been deemed as failures include:

- **The people factor**—The biggest constraint to an IT process improvement is people. Resistance to change is a powerful human behavioral element that helps survival, but it can derail any process improvement project. Often, management has “other” priorities or work related to IT processes or COBIT is not seen as part of everyday work.
- **Treatment as a project and not a process**—IT process improvement is often treated as a project, and the focus ends at the end of the project, e.g., reaching maturity level 3. As a result, processes slip back to their previous state or worse and the entire process starts again (figure 1).



- **A big-bang approach**—Organizations often make the mistake of bringing in a team to deliver IT process improvement or COBIT implementation in a short period of time. The result is usually a bunch of paperwork that ends up in a drawer.
- **The overcomplication of processes**—Processes are often overcomplicated and do not suit the environment. To avoid this, the design of the IT processes should be simple and efficient. People will quickly figure out when a process step is not necessary and skip the step or the process altogether.
- **Unrealistic deadlines (trying to do too much)**—IT process improvement is a long-term process and requires behavioral change. This requires strong mentoring and coaching for the process owner to get up to speed. Improving a process takes a lot of time; often, companies try to tackle too many processes at one time. It is recommended to prioritize, possibly six processes a year.
- **Lack of ownership**—Process owners often show a lack of ownership for various reasons, including not being involved in the documentation, not seeing the work as important and not receiving rewards or penalties for performance on the processes.
- **Implementation of COBIT, not improvement of processes**—The COBIT framework provides a process reference model; it is not an off-the-shelf cure. Rather, it needs to be customized according to the environment.

While COBIT can be used as a reference guide in designing the processes, the processes should be based on COBIT and not designed verbatim. Naming and measurements, for example, need to be customized and, in some instances, are not sufficiently specific for the needs of the environment.

- **Poor documentation practices**—Although some process documentation may pass an audit, they are sometimes of poor quality and/or add little value. Process documentation is sometimes not standardized. Work is often done for the sake of doing it and not to improve the working environment. Minimum standards need to be set for process documentation.
- **Poor design and standardization of processes**—Often, process owners lack the necessary knowledge or skills to design a process, which means that processes have different formats and varying levels of content. Processes need to be standardized for ease of understanding and assessment.
- **Processes that become outdated and irrelevant**—Processes often get outdated and become irrelevant because they are not continually improved and reviewed for relevancy.
- **The inability to implement processes**—Perhaps the biggest challenge is to implement the process in an environment. Even when the design and documentation have been done well, organizations struggle to embed the processes into their operations.

The Solution

What is the solution to the aforementioned issues? First, an IT process management framework must be developed that will provide guidance and standards for the design, approval, implementation and management of IT processes within the organization. The benefit of having such a framework is that all IT processes will be designed and managed in a consistent manner, which will allow for the measurement and, ultimately, improvement of the IT processes and their expected results.

For each IT process, a process guidebook that contains certain IT process attributes and will guide the process owners in the design, implementation and maintenance of the IT processes must be developed.¹ Frameworks such as COBIT and ITIL should be used to design the processes so that they are fit for purpose, but the frameworks must be customized to the environment. As should be outlined in the guidebook, the typical attributes required for each IT process are depicted in **figure 2**.

All processes should go through the three phases (**figure 3**):

1. **Design**—The IT process guidebook and the outputs are documented.
2. **Implementation**—Processes are institutionalized by defining roles and responsibilities, key performance indicators, updating job descriptions, training, etc.
3. **Maintenance**—Processes are measured, assessed and audited, and improvement plans are produced to improve the process. These improvements then enter the design phase of the process and go through the entire process again; thus, a process of continuous improvement is adopted.

Imagine a process as a conveyor belt that requires equipment, people and tools to operate it; the output of the process will be a product, e.g., a box of cereal. It is important to note that while the conveyor belt must be put in place for the process owner, it is up to the process owner to deliver the product. Therefore, the process owners are primarily responsible for the process outputs; however, they can obtain assistance.

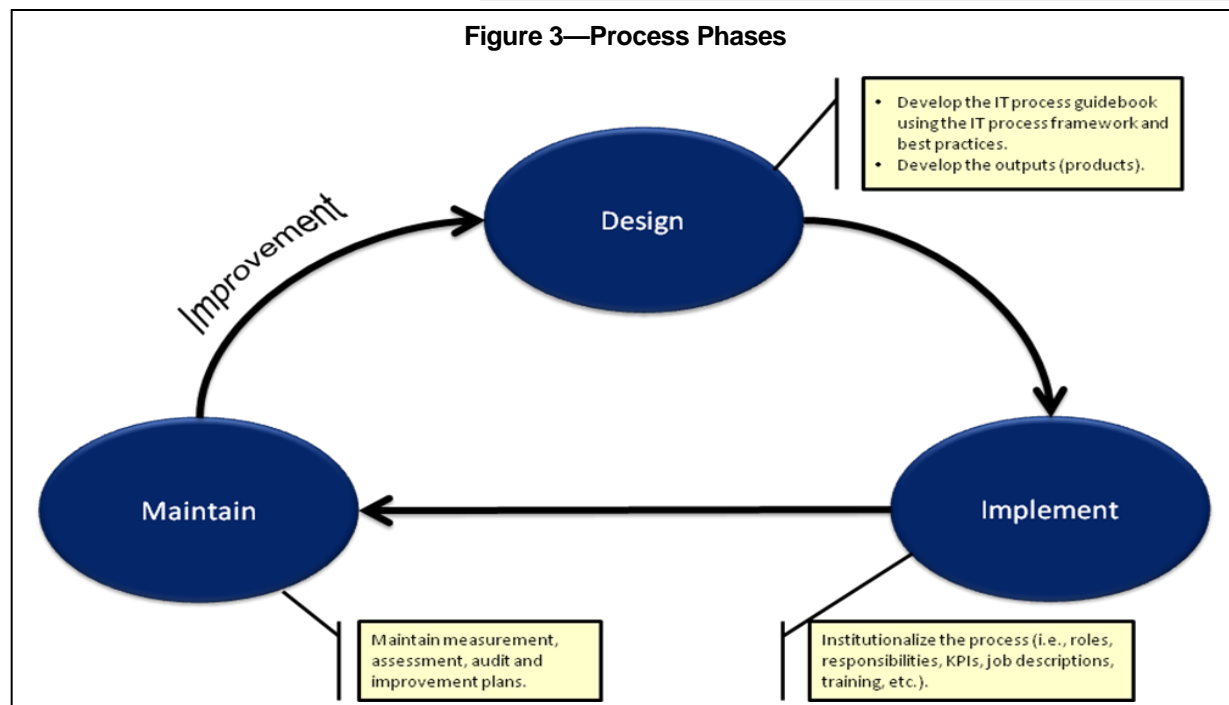
A Suggested Approach

Although not prescriptive, the following systemic approach is recommended for IT process improvement:

1. Conduct awareness research, and assess the current state of the IT processes. IT processes must also be prioritized, and only the priorities that have a business benefit justification

Figure 2—Typical IT Process Attributes

Process Identity	
Document Number	Process Number
Process Name	
Process Ownership	
Process Owner	Process Roles and Responsibilities
Process Owner KPIs	Role Player KPIs
Informative Material	
Introductory Notes	Best Practice References
Templates	Flow Charts (DIM)
Process Inputs/Outputs	Recommended Reading
Practices	Glossary
Process Purpose	
Purpose Statement	Process Goals
Process Outputs	
Typical Work Products	Policies and Procedures
Framework/Approach	
Process Measurement	
Process Maturity	Process Measures
Process Controls	Process Risks
Process Improvement	
Improvement Programme (DIM)	



should be included in the improvement program. Feedback must then be given to management to obtain approval to proceed with the program.

2. Design the IT processes, and document the key outputs of the process.
3. Implement the design phase's deliverables, including applying organizational change management; motivating, mentoring and coaching all process stakeholders (including the process owner); institutionalizing the IT processes (including integrating them with existing business processes); and reviewing and providing feedback on IT process performance and progress made.
4. Conduct a reassessment of the prioritized IT processes, and incorporate improvements into the design of the processes.

Process performance measures/metrics and performance criteria should be addressed in progressing this approach, and tools should be considered for use to support process improvement activities as appropriate.

Conclusion

IT process improvement, as one of the streams of an IT governance program, can add value to an organization. Unfortunately, more often than not, this is not the case.² Unless a holistic, well-thought-out approach to IT process improvement is adopted, the value will not be realized and the program will become a meaningless paper chase with frustrated participants. People need to be aware of the issues before embarking on such an initiative and need to have clear plans to address these issues or they could be headed for failure.

Delton Sylvester, CISA

has more than 10 years of experience in the IT industry, with a key focus on project management and IT governance, including COBIT, IT strategy, IT architecture and process design. He is considered a subject matter expert on COBIT and is often called on to assist with COBIT implementations. Sylvester is a part of the COBIT development team and recently contributed to the development of COBIT 5 materials. He was one of the pioneers in implementing COBIT within South Africa at De Beers from 2000 to 2003 and played a key role in the South African Revenue Services' governance of IT program, hosting a disaster management course that prepared delegates to handle disasters within their organization.

Editor's Note

The new ISACA COBIT Assessment Programme provides an approach to process capability assessment that includes the rigorous definition of process capability, evidence of achievement of process outcomes/outputs (as capability indicators), demonstration of assessor competence, and reliability and repeatability of COBIT-based process assessment results needed to improve the rigor, reliability and, thus, comparability of the results obtained. The approach is based on ISO/IEC 15504 *Information technology—Process assessment* and recognizes the need to support development process improvement plans.

Endnote

¹ This three-stage approach (design, implementation and maintenance) is based on the author's practical experience and on basic concepts from Software Engineering Institute, Capability Maturity Model Integration, Carnegie Mellon University, USA, 2000.

² This is based on the experiences of the author.

Updated COBIT Mapping Overview Publication Released

By **Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC**

ISACA makes available to users of COBIT an assortment of mapping documents that communicate the alignment between COBIT and other frameworks.

The mapping documents support the effective use of COBIT in conjunction with various IT-related frameworks and standards. Generally, the mapped frameworks and standards are selected based on their common, global use, although there are a few exceptions where regional volunteer support resulted in region-specific mappings.

ISACA's **COBIT Mapping** series includes mappings of:

- The US Federal Financial Institutions Examination Council (FFIEC) with COBIT 4.1
- IT Infrastructure Library (ITIL) Version 3 with COBIT 4.1

- US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 1 *Guide for Assessing the Security Controls in Federal Information Systems and Organizations* with COBIT 4.1
- Capability Maturity Model Integration (CMMI) for Development, Version 1.2 (V1.2) with COBIT 4.1
- ISO/IEC 20000 *Information technology—Service management* with COBIT 4.1
- ISO/IEC 17799:2000 *Information technology—Code of practice for information security management* with COBIT 4.0 (the second edition of this mapping)
- ISO/IEC 17799:2005 *Information technology—Security techniques—Code of practice for information security management* with COBIT 4.0
- The Project Management Body of Knowledge (PMBOK) with COBIT 4.0
- The Open Group Architecture Framework (TOGAF) 8.1 with COBIT 4.0

ISACA has just revised the COBIT mapping overview piece: *COBIT Mapping: Overview of International IT Guidance, 3rd Edition*. This third edition provides an overview mapping of the following standards and frameworks:

- **COBIT**—Released initially as an IT process and control framework linking IT to business requirements, COBIT was first used mainly by the assurance community in conjunction with business and IT process owners. With the addition of management guidelines in 2000, COBIT was used more frequently as a management framework, providing management tools such as metrics and maturity models to complement the control framework. With the release of COBIT 4.0 in 2005, it became a more complete IT governance framework. Incremental updates to COBIT 4.0 were made in 2007; they can be seen as a fine-tuning of the framework, not fundamental changes. The current version is COBIT 4.1; COBIT 5 is under development and scheduled for publication early in 2012.
- **ITIL V3**—ITIL is a collection of best practices in IT service management. It is focused on the service processes of IT and considers the central role of the user.
- **ISO/IEC 17799:2000**—This international standard based on BS 7799-1:1999 is presented as best practice for information security management. Although this standard has been superseded, the COBIT mapping remains available, for now, to support users of this version.
- **ISO/IEC 17799:2005**—This international standard based on BS 7799-1/ISO/IEC 17799:2000 is presented as best practice for implementing information security management. (Note: This standard was rebranded with the introduction of the ISO 27000 series of information security standards and is now published as ISO/IEC 27002.)
- **ISO/IEC 20000**—This series consists of two publications:
 1. ISO/IEC 20000-1:2005 *Information technology—Service management—Part 1: Specification* describes audit requirements.
 2. ISO/IEC 20000-2:2005 *Information technology—Service management—Part 2: Code of practice* provides further guidance for service providers.
- **NIST SP 800-53 Rev 1**—This publication was issued in February 2005 and is the first in this series.
- **FFIEC**—The FFIEC *IT Examination Handbook* represents a collection of documents that can be classified as generally accepted best practices for IT governance, control and assurance for financial institutions.
- **PMBOK**—ANSI/PMI 99-001-2004 *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, from the American National Standard Institute (ANSI), is described as the “sum of knowledge within the profession of project management” by the Project Management Institute.¹
- **CMMI for Development, V1.2**—This publication combines three source models—CMM for Software (SWCMM) v2.0 draft C, Electronic Industries Alliance Interim Standard (EIA/IS) 731, and Integrated Product Development CMM (IPD-CMM) v0.98—into a single improvement framework for use by organizations

Conference Update

Online COBIT Training and Exams

The ISACA eLearning Campus offers a comprehensive [Online COBIT Foundation Course and Exam](#) and access to the [Online Implementing the Governance of Enterprise IT Using COBIT Exam](#). The course and exams are applicable to IT professionals in all industries and enterprises. Passing the exams recognizes that the candidate understands the COBIT fundamental concepts and the core elements of the implementation of the COBIT framework for supporting governance of enterprise IT (GEIT).

ISACA's Licensing Program

Expanded course delivery options include classroom-based training and online and blended course offerings. Current company and/or individual licensees are posted on the [Training](#) page of the ISACA web site.

COBIT Training Week Course

The COBIT: Strategies for Implementing IT Governance course will be offered at the [ISACA Training Week](#) in Baltimore, Maryland, USA. Held 24-28 October, this comprehensive COBIT training program will highlight IT issues, governance concepts, risk management and control. [Register](#) now to attend.

- pursuing enterprisewide process improvement.
- **TOGAF 8.1**—This guidance provides a detailed method and set of supporting tools for developing an enterprise architecture.

The COBIT mapping overview publication and COBIT Mapping series include several mappings that relate to older releases of the referenced frameworks and standards, e.g., ISO/IEC 17799 and NIST SP 800-53. Mappings to these older versions remain available from ISACA since many enterprises still use these older standards/frameworks as their reference documents. ISACA will continue to support these enterprises and will, therefore, continue to provide these valuable mappings.

Once **COBIT 5** is published, ISACA intends to develop a new, more collaborative environment for COBIT users within which they can work with ISACA to map COBIT content to relevant standards, frameworks and practices of their own choosing.

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

is the chief executive officer of UK-based audit consultancy Ravenswood Consultants Ltd., which he founded in 1995, and is an information audit and security specialist with 30 years experience, working on audit, security and governance projects throughout Europe. 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. Oliver is regarded internationally as an expert in information governance, audit and security and has spoken at international conferences on various information security and audit topics. Oliver is cochair of the COBIT 5 Development Task Force and a member of the ISACA Framework Committee and Cloud Security Task Force.

Endnote

¹ Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*, USA, 2000



Come join the discussion! Paul Lokuciejewski, Karsten Wilop and Werner Syndikus will be responding to questions in the **discussion area of the COBIT—Use It Effectively** topic beginning 24 October 2011.

Using COBIT to Support IT Risk Management

By Paul Lokuciejewski, Ph.D., Karsten Wilop, CISA, CGEIT, CRISC, and Werner Syndikus, CISA, CGEIT, CRISC

IT plays a vital role in today's business world. Crucial incidents in IT substantially impact business processes and can result in loss of revenue and image damage. The increasing relevance of IT moves IT risks and their detection and handling into the focus of those responsible for IT. Furthermore, legal and regulatory requirements for operational risk management are growing, demanding proactive risk management with an early warning system.

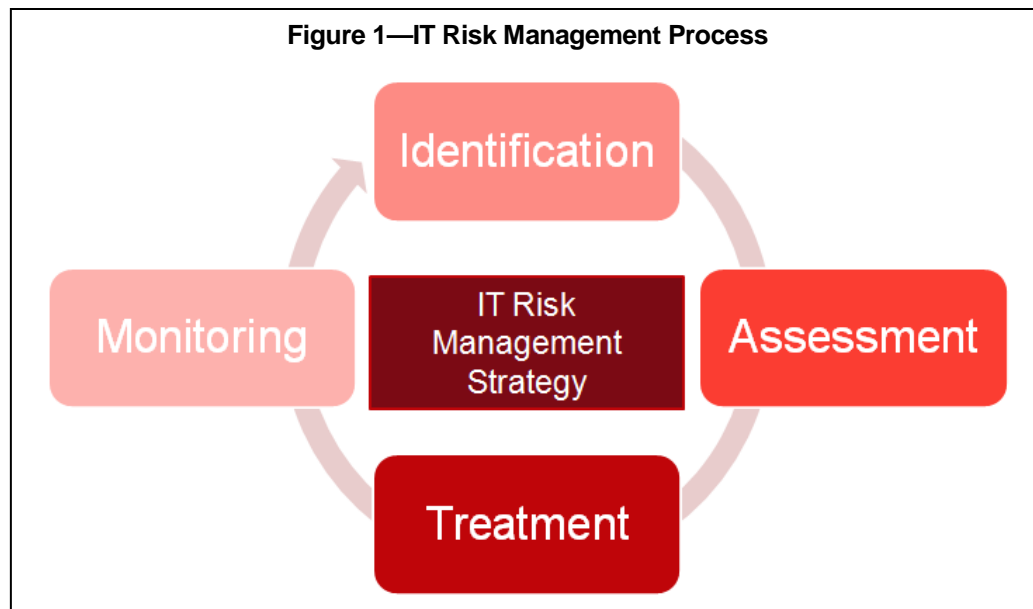
IT risk management is described in conventional standards and best practice frameworks as a cyclical process (**figure 1**).

Regulatory requirements, standards and frameworks provide differing levels of detail for the practical deployment and execution of this process. For this reason, a group of experts in Germany formed the IT Risk Management With COBIT group with the objective of developing practically oriented tools for the substantive deployment of IT risk management.¹

Goals and Approach

The starting point for the IT Risk Management With COBIT group was a collection of questions arising in the context of a practical deployment of an IT risk management process. The following essential questions were identified:

- How can a comprehensive inventory of generic risks be defined to prevent overlooking fundamental risks in the course of developing enterprise-specific risk scenarios?
- What key indicators can be used to measure vulnerabilities, and which key indicators can be utilized to support the implementation of an early warning system?



- How can suitable countermeasures for risk treatment be identified?
- How can risk impact be represented to IT management and business in particular?

Based on these issues, the objective of the IT Risk Management With COBIT group was formulated as follows: development of tools for the practical issues raised previously that can be provided to the relevant target group (e.g., IT supervisors, risk managers and line supervisors) in the form of a practical guideline.

The group first carried out a general analysis of COBIT to determine whether and how information could

be derived from this framework to provide answers for the questions posed previously and to create the planned guideline. In parallel, a wide range of other IT risk management standards and frameworks (e.g., ISO/IEC 27005:2011 *Information technology—Security techniques—Information security risk management*, ONR 49000 *Risk management for organizations and systems—Terms and basics—Implementation of ISO 31000*, Risk IT, etc.) was analyzed to check whether they contain answers to the identified issues, which would make the planned guideline superfluous.

Although the analyzed standards/frameworks all present good approaches to the methodical deployment of IT risk management, only a small number of practical aids was found to resolve the identified issues. In particular, none of the standards/frameworks contained extensive information on the creation of a “comprehensive risk inventory” for risk scenario development.²

In contrast, the general analysis of COBIT showed that COBIT, as a comprehensive framework for IT processes, offers a high potential for the derivation of such a risk inventory because it covers all relevant IT control areas. Furthermore, COBIT’s control objectives implicitly cover areas of IT that inherently entail risk. COBIT also provides a wide range of auxiliary information, e.g., goals and metrics at the IT, process and activity levels.

Based on the results of the general analysis, a systematic and detailed analysis of COBIT was performed to extract useful components of the framework for a substantive deployment of an IT risk management process. The following conclusions were drawn:

- To provide an initial basis for scenario development, the inventory of generic risks should be formulated as an inversion of the detailed control objectives that indirectly represent vulnerabilities.
- Early-warning indicators should be derived from COBIT’s goals and metrics and then allocated to the respective risk areas.
- Information on risk treatment should be derived from COBIT’s maturity model.
- The mapping of IT processes to the IT objectives and business objectives contained in COBIT should be exploited to explain the impact of the detected risks to IT management and business.

Results and Outlook

The detail analysis showed that valuable information on the substantive deployment of IT risk management can be derived from the information in COBIT. These essential results were formulated in the following work packages (WPs):

- **WP1: Derivation of IT vulnerabilities from control objectives**—COBIT states that IT processes have to be managed in a proper way to achieve business objectives. This implies that missing or poorly managed IT processes endanger business objectives and, thus, represent a vulnerability (leading to a risk). Based on this assumption, vulnerabilities from all control objectives were systematically derived, resulting in a risk inventory containing 222 vulnerabilities that represent a starting point for scenario development.
- **WP2: Identification of risk indicators from goals and metrics**—For each identified vulnerability, goals and metrics of

the corresponding processes were analyzed to see whether they were suitable as risk indicators. As a result, goals and metrics were allocated directly to a specific vulnerability. Goals and metrics were indirectly allocated to the vulnerabilities at the process level due to their higher abstraction level.

- **WP3: Derivation of risk treatment countermeasures**—Countermeasures for a systematic treatment of the identified vulnerabilities were extracted from the maturity model in connection with the requirements from control objectives.
- **WP4: Derivation of risk impacts on IT and business objectives**—The COBIT tables, the mapping of IT processes to IT objectives and business objectives were exploited to represent the impacts of the identified risks on business objectives.

The complete approach of the detail analyses, including all of the results, is currently being compiled by the IT Risk Management With COBIT group in a comprehensive guideline. In parallel to the creation of the guideline, the expert group is developing a tool in which the information from the WPs are centrally collected and evaluated.

Paul Lokuciejewski, Ph.D.

is a consultant at PwC in Dusseldorf, Germany. He has several years of experience in technology consulting, internal and external audits in the financial sector, and software development.

Karsten Wilop, CISA, CGEIT, CRISC

is a senior manager at PwC in Dusseldorf, Germany. He has more than 10 years of experience in the areas of IT compliance, internal and external audits, and IT consulting within the financial sector.

Werner Syndikus, CISA, CGEIT, CRISC

has 10 years of experience as a software developer and 10 years of experience as head of IT in the wholesale industry.

Endnotes

¹ The group includes the following members: Mohammad Hamidi, Ralf Herter, Paul Lokuciejewski, Ph.D., Heinz-Dieter Schmelling, Ph.D., Werner Syndikus, Martin Urban and Karsten Wilop.

² Risk IT provides a clear framework for implementing an IT risk management process. This article demonstrates how COBIT 4.1 can be used to build upon Risk IT's series of generic scenarios to identify a more detailed set of IT risk scenarios in support of IT risk management.

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.

© 2011 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 Julia Fullerton at jfullerton@isaca.org.

Framework Committee

Patrick Stachtchenko, CISA, CGEIT, CA, France, chair
Steven A. Babb, CGEIT, CRISC, UK
Sushil Chatterji, CGEIT, Singapore
Sergio Fleginsky, CISA, Uruguay
John W. Lainhart IV, CISA, CISM, CGEIT, CRISC, USA
Anthony P. Noble, CISA, USA
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, UK
Rolf M. von Roessing, CISA, CISM, CGEIT, Germany

Editorial Content

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



©2011 ISACA. All rights reserved.