Using COBIT for Assessing IT Process Maturity: A Case Study

By A Rafeq, CISA, CGEIT, CIA, FCA

XYZ Bank is a government-owned, frontline bank in India with a successful track record of 110-plus years. It has more than 50 million customers and more than 5,000 offices. XYZ Bank has always looked at technology as a key facilitator to provide better customer service and has ensured that its IT strategy follows the business strategy so as to arrive at the "best fit." The bank has made rapid strides in this direction. All branches of the bank use the core banking solution (CBS), which covers 100 percent of its business. The bank has a full-fledged IT department, which is spearheading the IT operations.

The IT department at XYZ Bank, in collaboration with its IT solutions provider, envisaged the need to benchmark its existing IT processes and practices using the best practices of the COBIT maturity model. The objective was to identify the current state of maturity for identified IT processes, compared with the expected level of maturity, and to identify gaps/areas of improvement. The bank appointed an IT solutions vendor to engage a team of COBIT subject matter experts (SMEs) to facilitate the bank in conducting the process maturity assessment through interactive workshops and discussions with the identified personnel/team from IT, business process owners and senior management. The head of the IT department was appointed chief coordinator of the project. A series of meetings was held by external consultants with senior management and executives of the bank to understand the requirements, and the overall approach and methodology for the assignment were finalized.

Objectives of the Assignment
The primary objective of the assignment was to prepare a dashboard of the existing/future maturity level for identified IT processes, to identify gaps in specific processes and to develop transition plans as per the agreed road map.
Approach and Assumptions for Using COBIT

The approach and assumptions of the assignment were discussed and agreed upon. The step-by-step approach (figure 1) and related assumptions follow.

The approach included the following:
1. Select the relevant IT process from COBIT (done by the bank with the IT solutions provider).
2. Identify the maturity level for the identified IT process.
3. Define the maturity level for the identified IT process.
4. Identify gaps in maturity levels.
5. Prepare an outline of the road map for bridging the gap.
6. Prioritize the transition plan, and identify brief projects for each action in the agreed-upon template.
7. Discuss and submit a draft report followed by a final report of recommendations.

The assumptions included the following:
1. The approach is generic, and estimates are approximate. These would be fine-tuned as required.
2. The assignment would cover only IT processes performed by the IT department.
3. The assessment would be through discussions and interactions during facilitated workshops with identified stakeholders from the bank.
4. The approach would not include review or validation of documentation.
5. The bank will provide relevant team members to participate in all stages as required.

<table>
<thead>
<tr>
<th>Description</th>
<th>Process/Deliverables</th>
<th>Activity</th>
<th>Day(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Select the COBIT IT process and control.</td>
<td>COBIT processes identified as relevant</td>
<td>COBIT workshop</td>
<td>1</td>
</tr>
<tr>
<td>2. Identify the maturity level for the identified IT process.</td>
<td>Maturity level for each of the identified IT processes at the current level</td>
<td>Workshop or discussion</td>
<td>2</td>
</tr>
<tr>
<td>3. Define the maturity level for the identified IT process.</td>
<td>Definition of the ideal maturity levels for each of the identified IT processes</td>
<td>Workshop or discussion</td>
<td>2</td>
</tr>
<tr>
<td>4. Identify gaps in maturity levels.</td>
<td>Gaps in processes and areas in which processes need to be improved</td>
<td>Discussion</td>
<td>2</td>
</tr>
<tr>
<td>5. Prepare an outline of the road map for bridging the gap.</td>
<td>Road map for bridging the gaps</td>
<td>Offsite and onsite</td>
<td>2</td>
</tr>
<tr>
<td>6. Prioritize the transition plan in consultation with the client, and identify brief projects for each action in the agreed template.</td>
<td>Assessment of the maturity of identified processes and a road map of process improvement</td>
<td>Workshop or discussion</td>
<td>1</td>
</tr>
<tr>
<td>7. Discuss and submit a draft report followed by a final report of recommendations.</td>
<td>Draft report and final recommendations of the maturity level assessment</td>
<td>Offsite and onsite</td>
<td>2</td>
</tr>
</tbody>
</table>

Step-by-step Methodology for Using COBIT

The assignment plan covered the following activities:
- Discussions with the identified team stakeholders from the bank and the IT solutions provider
- Finalization of the approach and methodology of the assignment
- Execution of the assignment as per the agreed-upon plan
The overall methodology (figure 2) was devised by choosing the relevant stages and steps from the ISACA publication *IT Governance Implementation Guide* (revised and updated now as *Implementing and Continually Improving IT Governance*) and the stages and steps were adapted and customized as relevant. The processes and steps of the first phase, “identify needs,” were made available by the bank before the commencement of the assignment and were used to perform the maturity assessment as outlined in the second phase, “envision the solution.” Preliminary work was done that pertained to the first step of the third phase, “plan the solution,” and the bank was expected to take these deliverables and finalize the plan of action for implementation of the next step/phase as required.

**Assignment of Tasks**
The IT solutions vendor was appointed to manage the project. The vendor met with the bank and COBIT SMEs. The project was owned by the bank team that participated and monitored the execution of the project at each phase. Key steps of the methodology included:
- Define the approach for the IT process maturity assessment.
- Finalize usage of the methodology/templates.
- Conduct a COBIT workshop for identified staff, and use this workshop to identify the IT process and assess the maturity level based on the management guidelines of COBIT with the stakeholders from the bank.
- Identify the current maturity level, define expected maturity levels and obtain conformance.
- Identify gaps between the current and expected maturity levels.
- Present assessment findings.
- Prioritize gap areas.
- Prioritize transition plans/projects as relevant.
- Prepare a detailed report of the action plan for recommendations, and identify projects as relevant.

The contents of the COBIT maturity level were presented in template form in the interactive workshop, and the agreed-upon responses were documented. After documenting responses for each of the statements for all levels, the current maturity level for the selected IT processes was computed, and after deliberation, the right level of maturity was set for those IT processes (figure 3). These steps were repeated until the assessment was completed for all identified processes.
Once the current/future level of maturity was completed for all the processes, the activities or tasks that had to be performed, but were not performed in each of the maturity levels of the identified processes, were identified. These were marked as material gaps based on criticality. The specific details of the gaps, as identified in each of the areas, were mapped with the input and output documents matrix to identify documentation gaps; with the Responsible, Accountable, Consulted, Informed (RACI) charts to identify responsibility gaps; and with the goals and metrics to identify metrics gaps. For each of the identified processes, the final report and presentation highlighted the current/future level of maturity, and in the case of processes with material gaps, details regarding areas of weaknesses in documentation, IT processes, IT policies, procedures and practices, and IT infrastructure requirements were provided. The bank’s IT department integrated the current/future level of maturity in the relevant IT performance metrics, as appropriate, to ensure monitoring and implementation by senior management.

**Figure 3—Maturity Level Assessment for IT Process DS4 Ensure Continuous Service**

<table>
<thead>
<tr>
<th>Ideal Score</th>
<th>Maturity Statement</th>
<th>Not at All</th>
<th>Somewhat</th>
<th>Largely</th>
<th>Fully</th>
<th>Item Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>There is no understanding of the risks, vulnerabilities or threats to IT operations or the impact of loss of IT services to the business.</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>0.00</td>
</tr>
<tr>
<td>0</td>
<td>Service continuity is not considered as needing management attention.</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>Integrated, continuous service processes take into account benchmarking and external best practices.</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td>0.67</td>
</tr>
<tr>
<td>1</td>
<td>The IT continuity plan is integrated with business continuity plans and is routinely maintained.</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>The requirement for ensuring continuous service is secured from vendors and major suppliers.</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>Global testing of the IT continuity plan occurs, and test results are input for updating the plan.</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td>0.33</td>
</tr>
<tr>
<td>1</td>
<td>Gathering and analysis of data are used for continuous improvement of the process.</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td>0.33</td>
</tr>
<tr>
<td>1</td>
<td>Availability practices and continuous service planning are fully aligned.</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td>0.33</td>
</tr>
<tr>
<td>1</td>
<td>Management ensures that a disaster or a major incident will not occur as a result of a single point of failure.</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td>0.00</td>
</tr>
<tr>
<td>1</td>
<td>Escalation practices are understood and thoroughly enforced.</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td>0.33</td>
</tr>
<tr>
<td>1</td>
<td>Key goal indicators (KGIs) and key performance indicators (KPIs) on continuous service achievement are measured in a systematic fashion.</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td>1.00</td>
</tr>
<tr>
<td>1</td>
<td>Management adjusts the planning for continuous service in response to the KGIs and KPIs.</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td>1.00</td>
</tr>
</tbody>
</table>

**Current Level of Maturity (Overall Rating From Level 0 to 5): 3.70**

**Targeted Maturity Level by March 2010: 4.50**

Note: A toolkit (zip file) of Excel templates with contents of COBIT maturity models for all 34 IT processes is available as part of ISACA’s new publication Implementing and Continually Improving IT Governance.
Conclusion
The bank was able to obtain the current level of maturity and a fixed target level of maturity for the identified IT processes from COBIT. It was able to identify gaps/areas of improvement for which a detailed action plan was prepared with specific time frames. The assessment approach adapted for this assignment was successful because of the detailed planning and the execution of a COBIT project plan, continuous monitoring, use of appropriate SMEs and the involvement of relevant stakeholders from the bank. User involvement and ownership establishment resulted in a transfer of knowledge of COBIT best practices and empowered the stakeholders for future implementations.

This case study provides the approach adapted as per the requirements of the bank. Hence, the task/activities and time estimates were relevant to this assignment. In any COBIT implementation, it is important to remember that the generic approach provided needs to be tailored as required. Hence, specific tasks and activities under each of the phases and time required for implementation would vary based on factors such as scope/objective of the assignment, area of implementation, user involvement, complexity of the processes, maturity of relevant processes, documentation available, extent of implementation and deliverables. Similarly, generic contents of COBIT need to be selected, customized and extended as required.

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

Align Technical Content With Business Thinking Using BMIS
By Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS

From a business perspective, the primary objectives of any enterprise are often far removed from the technical world of IT and information security. To bridge the gap between what the enterprise does and how this is supported by strong security, the Business Model for Information Security™ (BMIS) realigns technical content with business thinking and a strategic point of view.

In January 2009, ISACA introduced the security community to BMIS. The introductory publication offered security professionals a look into a new approach for effective management of information security. ISACA has now published the full version of BMIS, which provides a more detailed explanation of the model and how it works. Detailed in the new publication *The Business Model for Information Security*, BMIS focuses on the business environment within which information security operates amongst other business processes. This particular focus provides a broader view of value-driving processes and systems within the enterprise that impact or are impacted by information security.

Low budgets, limited staffing and restricted access to executive support are common hurdles that information security professionals face while trying to protect information assets, minimise risks and deliver value to the business. Add to this a continuously changing regulatory environment and constantly emerging new risks, and it is easy to see why information security has struggled to thrive as a function within enterprises.

These obstacles in day-to-day security work often arise out of a fundamental misunderstanding. Although organisational leaders are aware of risks and are willing to address risks in a hands-on manner, the complexity of information security requires specific skills and knowledge. More often than not, security experts find it difficult to articulate the value that information security can bring to the business by ensuring that information assets are not only protected from those who should not have access to them, but also by ensuring that information is available and accurate for those who should have access. BMIS provides the frame and mind-set to structure communications amongst senior management and security professionals.

Until now, there has been no holistic or dynamic model for security managers to use as guidance. There are many standards that can be used for benchmarking and providing direction, and there are just as many frameworks that can serve as useful guides for
implementation, but there has been no overarching model that could exist in any enterprise regardless of geographic location, industry, size, regulation or existing protocol. Many people may think that they are on the right path because they have aligned their programme with an existing standard or framework. While these avenues may seem to lead the security professional in the right direction, there is one essential component missing. Frameworks and standards have helped to address specific needs, but they have not provided a holistic solution that examines the entire enterprise and studies how the organisational mission affects the security programme and vice versa. To understand the big picture, information security managers must take a broader view.

BMIS fills this gap and addresses the security programme at the strategic, or business, level. The model allows security managers to gain a broad view of what is happening in the enterprise, enabling them to better treat information risk while assisting senior management in meeting its goals. By looking at the security programme from a systems perspective, BMIS provides a means for security professionals to consider areas that may not have been accounted for in existing standards. BMIS also provides a mechanism for security professionals to internalise the fact that new threats and new attacks come up regularly. To understand the model, it is important to distinguish amongst models, standards and frameworks. While BMIS can help overcome some of the known difficulties in information security, it is primarily an overarching model that should be supported and complemented by additional standards and frameworks.

Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS

has 22 years of experience in the IT field, some of which were spent as chief information officer in the utilities field and 14 of which were spent in the information security arena. She specialises in consulting in information security issues, with a particular emphasis on governance in the commercial and operational areas of businesses. Stewart-Rattray provides strategic advice to enterprises across a number of industry sectors, including banking and finance, utilities, automotive manufacturing, tertiary education, retail, and government, throughout the Asia-Pacific region. She is the chair of ISACA’s Leadership Development Committee and its Security Culture Development Group, sits on the association’s Knowledge Board, and is the immediate past president of ISACA’s Adelaide Chapter.

Acknowledgement

ISACA would like to thank all of the volunteers who worked to prepare and deliver BMIS, especially Rolf M. von Roessing, CISA, CISM, CGEIT. This article is largely based on The Business Model for Information Security.

Editor’s Note

The Business Model for Information Security is available as a complimentary PDF download. Print copies are available for purchase from the ISACA Bookstore.

When IT Governance Stifles

By Delton Sylvester

When one IT consultant first started consulting for a large insurance organization, he was firmly told that if he mentioned the word “governance,” he would be escorted out of the building. He was told that the correct term to use is “process.” The consultant wondered why there was such an aversion to governance. It turned out that the organization had a very agile product development process and the culture was to go to the market fast. The past experience of the organization was that governance slowed this process down, and the term governance was thus viewed negatively as “red tape.” Since then, there has been...
a massive turnaround in the appreciation of the benefits of governance, and currently, there is a major drive to implement IT governance in the organization.

Another example is a major bank with a six-month turnaround time for business cases for IT projects. The problem here is that by the time the business case is approved, in many cases, the technology has moved on and the project is back to square one.

Then, there is the case of a major state-owned bank that had a scandal break out over its governance practices. Afterward, the bank decided that all purchases, however small, needed to go through three directors before approval. One can only imagine the impact this had on business within the bank.

In another state-run organization, after an IT governance implementation, it was found that there were so many meetings and so much paperwork that no work got done.

These examples highlight the problems that can occur when risk and benefits are not properly balanced in a governance model. Often, companies weigh too heavily on the risk side and forget that true governance is also about benefits realization.

So, too, an IT governance implementation using COBIT is often heavily weighed on the risk side. There is no doubt that the risk issues, e.g., IT continuity, compliance, information security, are important, but the benefits side cannot be forgotten. The Board Briefing on IT Governance clearly states: “Successful enterprises understand the risks and exploit the benefits of IT,” but how often is this really the case? Many times, an IT governance implementation becomes a paper chase that may help an organization pass an IT audit, but has no real benefit in terms of process efficiencies or added value to the business. When this is the case, the “paper” ends up in a drawer gathering dust.

What is the solution? How does one achieve a balanced IT governance program?

• First and foremost, there must be a good understanding of the organization’s risk appetite. In certain industries, there is a need for stronger controls and, thus, a stronger leaning toward the risk side. In some organizations, to go too far on the risk side will stifle the business, especially if it is part of a profit-bearing industry. Once one has a clear indication of the risk appetite, the IT governance implementation can be modeled around it.

• Keep it simple. Probably the main reason for the failure of so many IT governance implementations is that the processes and structures have been overcomplicated. The IT processes of COBIT should be kept simple and efficient. People will quickly figure out when a process step is not necessary and skip the step or the process altogether.

• It is important to incorporate IT governance into the IT strategy. This will ensure the inclusion of the benefits side in the IT governance program and will ensure that IT value is maximized in the organization.

• It is important to adopt a culture of continuous improvement. Processes should be reviewed regularly, and contributions should come from all levels. A helpful approach to continuous improvement is Kaizen. Western philosophy can be summarized as, “if it ain’t broke, don’t fix it.” The Kaizen philosophy is that everything, even if it “ain’t broke,” can be improved.

• It is important to adapt the IT processes of COBIT to the culture and size of the organization. For example, when implementing PO10 Manage projects, one should tailor it to the size and culture of the organization. In some cases, basic project management is required with few steps in the process. In other cases, a more rigorous project management framework is required.

• Last, when selecting the IT processes of COBIT, it is important not to try to do it all. Rather, one should look at the processes that are not being performed well as the most important and target these for improvement initially.
Delton Sylvester

has more than 10 years of experience in the IT Industry, with a key focus on project management and the governance of IT, including COBIT, IT strategy, IT architecture and process design. He was one of the pioneers in implementing COBIT within South Africa at De Beers from 2000 to 2003. Sylvester is also considered a subject matter expert on COBIT and is often called on to assist with COBIT implementations. He currently travels across Africa consulting with the central banks of the South African Development Community (SADC) and East Africa and a few commercial banks in the southern Africa region.

Endnotes

1 This article is based on the experiences of the author.
2 IT Governance Institute, Board Briefing on IT Governance, USA, 2003
3 In Japanese, “kai” means change and “zen” means good, literally translating to “change for the better” or “improvement.”

CRISC, A New Step in Professionalism

By Brian Barnier, CGEIT

Wanted: IT risk manager

Needed: Strong understanding of the business, able to converse easily with a wide range of leaders across the organization. Experience in finance and planning, project management, and the complete range of IT operations and support areas. Experience in driving process assessment and improvement.

IT risk is a hot topic. When researching job opportunities with a popular job search engine,1 1,464 open job positions included the term “technology risk” and 2,580 job openings included the term “IT risk.”

Hiring managers are seeking a new skill set in professionals: management of IT-related risks to the business and management of business risks related to the implementation of information systems (IS) controls. In a world of change, made more difficult by tough economic times and increasing business dependencies on information technology, chief information officers (CIOs) (and chief risk officers [CROs]) are seeking professionals who can see the broad risk picture, can cross silos and can manage a wide range of IT-related risks to the business.

People applying for such positions look for ways to differentiate themselves—to stand out from the crowd. Most important, they want to differentiate themselves across the range of skills needed for success in the enterprise. Success in managing IT-related risk to the business is more than risk-based compliance, security, project management or auditing.

IT-related risks to the business can be defined in three major categories:

- Operations/service delivery
- Program/project management
- IT investment value/portfolio management

These are the categories used in ISACA’s Risk IT: Based on COBIT®. Business leaders wanting to deliver a product or service to customers face these risks daily.

Each of these categories of risk is important to one or more roles:

- Business line, function and/or geographic area management
- Chief financial officers (CFOs)
- CROs
- General counsels
- CIOs
- Leaders of IT functional areas (applications development, infrastructure operations, business liaison, finance, etc.)

IT-related business risk managers must be able to communicate with each role in a way that matters to that role.
This business perspective on IT-related risks is different from risk-based analysis for activities such as security or change management. Hiring managers know this and are seeking evidence of the right risk-related skills in business process understanding, financial risk-return analysis, project management and exposure to a range of operational areas. The problem hiring managers face, especially for external hires, is that it is difficult to know who really has the right skills—without conducting time-consuming, detailed interviews with many candidates.

With this need in mind, ISACA developed the Certified in Risk and Information Systems Control™ (CRISC™, pronounced “see-risk”) certification. CRISC is intended to recognize a wide range of professionals for their knowledge of enterprise risk and their ability to design, implement, monitor and maintain IS controls to mitigate such risk. It is designed particularly for IT professionals who have hands-on experience with risk identification, assessment and evaluation; risk response; risk monitoring; IS control design and implementation; and IS control monitoring and maintenance.2

While CRISC is designed primarily for practitioners working with IT-related risks and controls (similar to the Certified Information Systems Auditor® [CISA®] designation for IT audit practitioners), it is also beneficial to all involved in IT-related business risk management. With a holistic risk management approach, CRISCs would ideally liaise across IT areas (such as application development, infrastructure, architecture, security, disaster recovery and facilities) to aggregate a comprehensive view of IT-related risks to a particular business activity (e.g., process, product, facility, geographic area). CRISCs may also coach the various functional and organizational areas to help improve efficiency and effectiveness in risk and control techniques.

CRISC provides a way for hiring managers to identify qualified candidates and for job seekers to demonstrate their knowledge. Certifying eligible staff may also help demonstrate a sufficient risk management skills portfolio within the enterprise to auditors and regulators. For those in a regulated organization, it may help to make the enterprise’s risk or compliance leader aware of CRISC.

Brian Barnier, CGEIT
is a principal at ValueBridge Advisors. He has worked in both business line and IT roles and researches, teaches and writes on business-IT effectiveness. Barnier served on the task forces that created The Risk IT Framework; the team developing the CRISC Review Manual 2011; and the program committee for the IT Governance, Risk and Compliance Conference. He contributed to the Wiley & Sons book Risk Management in Finance. Barnier can be reached at brian@valuebridgeadvisors.com.

Editor’s Note
To date, ISACA has certified more than 1,000 practitioners with the CRISC designation. The grandfathering provision is open through 31 March 2011. The early-bird discount for CRISC grandfathering is available through 31 October 2010. Please visit the CRISC Certification page for more information on how your enterprise can take advantage of this next step in professionalism.

Endnotes
1 www.indeed.com
2 For more information, see the job tasks and knowledge statements that relate to this certification.

Governing and Managing the Operational Environment
With COBIT and ITIL
By Robert E. Stroud, CGEIT

For almost 10 years, this question has been repeatedly asked: “Is COBIT a replacement for ITIL®?” Of course, this line of thinking is a fallacy, and this article details the value and benefits of using COBIT and ITIL together for business value and the effect on enterprise governance of IT.

To implement effective enterprise governance and management of information and related technology, business managers must work with service managers to ensure that IT activities are aligned with business needs and that services are reliable, resilient and responsive to change. Together, COBIT and ITIL provide guidance to help service managers identify the key steps and identify who is responsible for them, eliminating any gaps.
COBIT provides useful guidance and examples for defining business and IT objectives and for describing how they relate to each other. It is a framework for effective governance and management that focuses on what should be addressed to ensure good performance of all IT-related processes, including those related to service management. It provides structured guidance and tools for implementing the IT processes required to satisfy business needs. By using COBIT, an enterprise can ensure that its service management efforts are aligned with its overall business, governance and internal control requirements. ITIL complements COBIT by providing the how—how to plan, design and implement effective service management capabilities.

Used together, COBIT and ITIL provide a top-to-bottom approach to the governance and management of enterprise IT resources and IT service management. COBIT guides management’s priorities and objectives with a holistic approach to a full range of IT activities, focusing all stakeholders (business and IT management, auditors, and IT professionals) on an integrated and common approach. ITIL supports this with good practices for service management.

When enterprises combine the two frameworks, the power of both approaches is enhanced, with a greater likelihood of management support and direction and a more cost-effective use of resources. Used together, COBIT and ITIL provide an effective way to understand business priorities and requirements and how to then utilize this knowledge to drive a focus on IT services. This approach allows management to better understand the significance of IT services and how they support the business, and it also enables operational IT managers to better understand the impact that services have on business processes. The result is more highly effective business cases for service improvements.

The COBIT and ITIL mapping (figure 1) varies based on each individual process. For instance, COBIT process DS1 Define and manage service levels has almost a one-to-one correlation with ITIL. The mapping is detailed on an activity level in COBIT User Guide for Service Managers. This publication also details the requirements for a service manager to implement the two frameworks together and includes a mapping of IT goals to process goals; an ITIL-specific Responsible, Accountable, Consulted and Informed (RACI) chart; and goals and metrics for each process to allow practitioners the capability to build effective governance for their IT service management implementations.

ISACA and itSMF both acknowledge that COBIT and ITIL are complementary and mutually beneficial. The organizations jointly developed publications such as COBIT User Guide for Service Managers and Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit.

For enterprises implementing COBIT and ITIL, the following guidelines are recommended:

- Tailor the guidance appropriately to the specific organization, adapting the good practices to fit particular business objectives and needs.
- Treat the implementation as a project with a series of phases, rather than as a one-off step.
- Remember that cultural change is required, and motivate this change.
- Ensure that there is a clear understanding of the objectives.
- Manage expectations. Achieving successful oversight of IT takes time and is a continuous improvement process.
- Focus first on where it is easiest to make changes and deliver improvements; build from there.
- Obtain top management buy-in and ownership.
- Do not let the initiative be perceived as a bureaucratic exercise.
- Avoid the unfocused checklist approach.

Sun Microsystems is an example of an enterprise that successfully implemented COBIT and ITIL. As Bob Frelinger discussed in his Information Systems Control Journal® (now the ISACA® Journal) article titled “Building Acceptance and Adoption of COBIT at Sun Microsystems,” Sun was looking for a common framework to view and measure the company’s IT alignment with and contribution to the overall business strategy. However, as Frelinger describes in

![Figure 1—Mapping COBIT and ITIL](Image)
his article, many executives showed resistance, asking “If the organization already knows what it needs to work on, and it follows industry best practices as it makes improvements, what does COBIT give it that it does not already have? Does COBIT replace ITIL?”

To get buy-in, Sun’s chief information officer (CIO) demonstrated a clear link between COBIT and the processes that the organization had already adopted. For example, Sun’s internal product Helios, which is part service catalog and part configuration management database, was influenced by ITIL service level management and configuration management processes. COBIT supporters showed graphically that the COBIT Deliver and Support domain provides the generic “what is to be done” with suggested measures, ITIL provides the generic “how it should be done,” and Helios provides the specific implementation.

An example that describes the use of COBIT and ITIL is provided in figure 2.

ISACA has developed a series of frameworks to deliver IT governance, including Risk IT: Based on COBIT for the understanding of enterprise risk, Val IT™: Based on COBIT® for ensuring the value of IT-enabled investments and COBIT as the overarching governance framework (visit the COBIT® 5 of the ISACA web site for more information on the upcoming release). COBIT can serve as an overarching IT governance and management framework for organizations using other good practices such as the Project Management Body of Knowledge (PMBOK®), the Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook, the Committee of Sponsoring Organizations of the Treadway Commission’s Enterprise Risk Management—Integrated Framework (COSO ERM), the UK Office of Government Commerce (OGC)’s PRINCE2 and the International Organization for Standardization’s ISO/IEC 27002. ISACA provides detailed mapping guides related to many of these and ITIL v3.

But, why is an overarching framework necessary?

As stakeholder and market focus on corporate governance continues to grow, the board is increasingly adding IT governance to the agenda because IT is so critical to business operations, it is complex to manage and it affects nearly all future business strategies. For example, the King III Report on Corporate Governance for South Africa identifies a strong focus and dependence on IT governance to meet the corporate governance objectives. It is critical that senior management realizes the benefits of effective IT governance, including that it:

- Helps control the increasing risks the organization faces
- Ensures continuity of critical business processes that depend on information systems
- Integrates organizational objectives with the growing dependence on service providers and outsourcers
- Is dramatically changing organizations and business practices to create new opportunities and reduce cost
- Ensures continuity of IT knowledge, which is essential to sustain and grow the business

Implementing COBIT and ITIL, with buy-in from the top and following recommended guidelines, will help enterprises achieve the governance and service management levels they need to stand out from their competition, achieve greater value from IT investments and maximize trust in one of their greatest assets—their information.

Figure 2—Example Case Using COBIT and ITIL

A bank had approximately 25 branches, but only the head office and eight branches were computerized. The branches did not use the online facility, nor did they offer an online banking service. Information on branch performance was available only at the head office at month-end. For remote branches, it was available 15 days after the end of the month. The system had extensive limitations pertaining to data storage, security and the management information system (MIS).

COBIT and ITIL were used to develop an IT strategy and to increase the efficiency of and streamline the bank’s day-to-day business procedures. An IT governance road map that was scalable, user-friendly and able to support the business for another 10 years was required to prepare the bank for joining a national electronic funds transfer (EFT) system. Leading practices from COBIT and ITIL were used to populate the IT governance road map.

The IT governance road map resulted in the following key projects being initiated:

- Reviewing, in detail, the existing IT infrastructure, including the hardware, software and communications networks:
  - Performance and capacity management
  - Reporting system (within the bank and to the external agents)
  - Service level analysis
  - Disaster recovery
  - Automated backup
  - Help desk
- Reviewing the IT information security framework
- Building a road map for comprehensive IT and MIS
- Framing of strategy to expand e-payment services
- Identifying training requirements and other capacity building issues

Robert E. Stroud, CGEIT
is international vice president of ISACA and the service management, governance and cloud computing evangelist at CA Technologies.

Endnote


New Risk IT Case Study: MetLife

MetLife Inc. is a leading provider of insurance and other financial services to millions of individual and institutional customers throughout the US. Outside of the US, MetLife companies have direct insurance operations in Asia, Latin America and Europe.

MetLife considers averting risk to its clients, stakeholders and reputation to be paramount. While every business is exposed to some level of risk, it is MetLife’s attention to and successful management of those risks that set it apart from the others. Establishing IT risk management processes and embedding them into the business has allowed MetLife to reduce operational losses, effectively prioritize investments, confidently react to business changes and concentrate resources on addressing high-risk areas.

To this end, when ISACA published Risk IT: Based on COBIT, MetLife’s IT risk professionals quickly leveraged the document to create a MetLife-specific IT risk management framework. While ISACA’s version was easily understood and digested by risk professionals, MetLife customized a framework that used internal terminology, summarized certain areas and expanded on others to ensure that the document could be easily understood and used globally across the enterprise. The tailored version enables management to understand, consider and communicate all aspects of managing IT risk consistently across the global enterprise and to better connect management to business operational risk activities.

Visit the Case Studies page of the ISACA web site for the full text of this and other ISACA framework case studies.