In This Issue:

- IT Organization Assessment—Using COBIT and BSC
- Laugh & Learn: Cloud Computing and the Genie
- Solo Cup: Using COBIT to Develop IT Policies
- The Need for Value Management Has Never Been Greater
- New COBIT Case Study: Banco Supervielle S.A.

IT Organization Assessment—Using COBIT and BSC

By Serena Frank, PMP

Organizations wanting to assess their maturity level and access a road map for achieving maturity objectives can benefit by using the COBIT® framework, along with the Norton/Kaplan balanced scorecard (BSC). COBIT provides best-practice guidelines and operational metrics, while the BSC provides a strategic planning and execution framework. Together, they create a powerful arsenal to evaluate and evolve the efficiency, effectiveness and quality of an IT organization’s performance.

Situation

An organization was in the process of developing a comprehensive strategy using the Norton/Kaplan strategy map and BSC approach. At the same time, its five-year IT plan was expiring. Therefore, it needed a refreshed IT strategy and multiyear plan to reflect the organizational strategy and support its objectives. A management consulting firm was engaged to provide an assessment of the enterprise’s current IT operations and to develop a strategy and three-year plan.

Figure 1—Assessment Process

- Data sources: Interviews, focus groups, documentation, observation
- Data analyzed: Project portfolio, resource, financial, technology
- Research sources: COBIT, ITIL, vendors, benchmarks
- Collaborative development of recommendations and deliverables leveraging cross-functional consultants

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 2, 2011: 10 March

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

Case Studies

See more case studies at www.isaca.org/casestudies.
Complications
Complicating the current situation was an ongoing crisis—a failed implementation of the organization’s core business operations system, an industry-specific common-off-the-shelf (COTS) application. This was the outcome of a three-year, US $12 million project. Phases I and II were implemented in the prior year, and although there were several financial anomalies, such as miscalculations of fees, the system response time was acceptable. When phase III was implemented in the current year for the business areas with the highest volume transactions, response time plummeted. In some cases, a standard record update resulted in a “hung” system—leaving the user to wonder whether the transaction had been processed (often it was “not”), which resulted in lost records. Another serious issue was lack of data integrity, which was caused by a faulty data conversion process from the previous system, which, it was later discovered, was the result of failing to successfully test the data conversion process.
Additionally, the previously identified financial issues had not been addressed, and new functionality designed to support web-based consumer transactions failed to process information correctly. In short, the organization was reeling from poor system response time, nonperforming functionality and data integrity issues.

The consultant team was, thus, tasked with responding to these serious problems in assessing the IT organization’s performance and maturity; additional root-cause issues would be discovered through the assessment process. The consultant team leveraged several frameworks, including COBIT, the Norton/Kaplan strategy map and BSC, ITIL, and Lean Six Sigma (LSS) to identify issues, determine root causes and recommend a go-forward plan.

**Objective/Approach**

The objective for this engagement was to provide a comprehensive strategy using the Norton/Kaplan BSC methodology and to present a three-year operational plan including recommendations to remedy issues and measure progress. After the start of the project, the scope was increased to include root-cause analysis of the project failures.

The time frame for the engagement was approximately three months—a relatively short period of time given the broad nature of the objectives. The consultant team designed a rapid assessment process consisting of interviews, focus groups, a documentation review and observations. Both IT and business leaders were interviewed using a structured set of open-ended questions and a COBIT self-assessment scale based on COBIT® Quickstart, 2nd Edition.

The data collection tool was tailored from COBIT Quickstart to focus on maturity and use of best practices. Practices were assessed based on five levels of maturity. Figure 2 is an excerpt from the survey tool used to assess the client organization. The maturity rating scale used in figure 2 is:

- 1—Initial/ad hoc
- 2—Repeatable but intuitive
- 3—Defined
- 4—Managed and measurable
- 5—Optimized

COBIT Quickstart was selected as the assessment framework, rather than COBIT® 4.1, for two reasons. First, the length of time for this engagement could not accommodate a full COBIT assessment, and second, the client did not specifically request a COBIT assessment. The consultant team opted to use COBIT Quickstart as part of the assessment process because it provides an organized IT evaluation framework with control objectives, best practices and suggested metrics for continuous improvement. Use of this tool enabled input from the leadership team, users and IT professionals in a consistent, reliable manner and within a compressed time frame.

The consultant team leveraged several frameworks, including COBIT, the Norton/Kaplan strategy map and BSC, ITIL, and Lean Six Sigma (LSS) to identify issues, determine root causes and recommend a go-forward plan.

**Objective/Approach**

The objective for this engagement was to provide a comprehensive strategy using the Norton/Kaplan BSC methodology and to present a three-year operational plan including recommendations to remedy issues and measure progress. After the start of the project, the scope was increased to include root-cause analysis of the project failures.

The time frame for the engagement was approximately three months—a relatively short period of time given the broad nature of the objectives. The consultant team designed a rapid assessment process consisting of interviews, focus groups, a documentation review and observations. Both IT and business leaders were interviewed using a structured set of open-ended questions and a COBIT self-assessment scale based on COBIT® Quickstart, 2nd Edition.

The data collection tool was tailored from COBIT Quickstart to focus on maturity and use of best practices. Practices were assessed based on five levels of maturity. Figure 2 is an excerpt from the survey tool used to assess the client organization. The maturity rating scale used in figure 2 is:

- 1—Initial/ad hoc
- 2—Repeatable but intuitive
- 3—Defined
- 4—Managed and measurable
- 5—Optimized

COBIT Quickstart was selected as the assessment framework, rather than COBIT® 4.1, for two reasons. First, the length of time for this engagement could not accommodate a full COBIT assessment, and second, the client did not specifically request a COBIT assessment. The consultant team opted to use COBIT Quickstart as part of the assessment process because it provides an organized IT evaluation framework with control objectives, best practices and suggested metrics for continuous improvement. Use of this tool enabled input from the leadership team, users and IT professionals in a consistent, reliable manner and within a compressed time frame.
**Actions**
As a result of the COBIT Quickstart analysis, several key issues were identified. These are indicated by the low maturity levels shown in figure 3.

The issues identified in the survey and by the consultant (see figures 4-7) were summarized, and recommended initiatives were defined. The summary tables were organized by COBIT process groups and indicate the issues, recommendations and associated initiatives that the client adopted.

**Results**
With the input of the organization’s leadership team, a future vision and strategy were created that defined the results expected from the IT organization, such as accurate, timely and accessible data; proactive support; and innovative ideas. These were translated into timeless objectives depicted in a strategy map. Corresponding metrics were then defined. Together, these comprised the BSC, which provided long-term direction for achievement of the strategy.

The BSC typically has four perspectives: financial, customer, internal process, and learning and growth (or human capital). Figure 8 shows a slice of the BSC representing an objective for “quality solution delivery” in the process perspective.

A thorough organizational assessment was executed that included evaluation of each staff member’s skills, abilities and interests, which were then matched to a new organization structure and role set. This resulted in new roles, responsibilities and expectations. Additionally, the longer-term initiatives, aligned with the strategy, are now underway. A program management office in which project disciplines are defined has been put in place, a solution architect has been

---

**Figure 4—Plan and Organize Summary**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Recommendation</th>
<th>Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclear or inaccurate organization structure, roles and responsibilities</td>
<td>Clearly define roles, responsibilities and expectations. Ensure resources are appropriately leveled and titled.</td>
<td>Organization alignment</td>
</tr>
<tr>
<td>Lack of planning for projects, resources, technology direction</td>
<td>Institute planning processes for scheduling work, resources and architecture.</td>
<td>COBIT governance</td>
</tr>
<tr>
<td>Insufficient communication within IT and with business partners and stakeholders</td>
<td>Define specific communication expectations in roles and processes.</td>
<td>Organization alignment (business technology partner role); project management discipline</td>
</tr>
<tr>
<td>Undefined IT processes for project request and management</td>
<td>Develop a clear process and focal point for requesting IT work. Assign requests to an individual for management and communication.</td>
<td>COBIT governance; project management discipline</td>
</tr>
<tr>
<td>Undocumented performance management</td>
<td>Use expectations as a measurement tool for performance management and coaching.</td>
<td>Organization alignment; performance measurement</td>
</tr>
<tr>
<td>Limited management and control of IT spend</td>
<td>Ensure that financial oversight is incorporated into specific job responsibilities. Benchmark with peers and negotiate with vendors.</td>
<td>Organization alignment; performance measurement</td>
</tr>
</tbody>
</table>

**Figure 5—Acquire and Implement Summary**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Recommendation</th>
<th>Initiative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor vendor management, oversight and influence—unsophisticated and uncoordinated; no financial checks and balances</td>
<td>Appoint an individual to be responsible for vendor management. Ensure that contracts are fair and reasonable through benchmarking and negotiation.</td>
<td>Organization alignment; performance measurement</td>
</tr>
<tr>
<td>Noncentralized technology procurement, systems administration and relationship management</td>
<td>Define guiding principles for technology acquisition and governance.</td>
<td>COBIT governance; enterprise architecture</td>
</tr>
<tr>
<td>Insufficient planning and discipline for systems implementation</td>
<td>Ensure proper planning and risk management.</td>
<td>Project management discipline</td>
</tr>
<tr>
<td>Minimal change management process discipline</td>
<td>Utilize ITIL best practices for documenting, reviewing and approving all changes.</td>
<td>ITIL</td>
</tr>
</tbody>
</table>
appointed, change and quality management disciplines have been adopted, and vendor and financial management is now functioning. An active and proposed project portfolio now provides a basis for prioritization of work and governance. In just a few months, these changes have already resulted in positive outcomes. As one example, a recent core system upgrade was implemented without a single issue.

As a result of this analysis, recommendations and tactical action items (e.g., elimination or redefinition of certain roles, release of certain employees) have been fulfilled. Also, system issues such as performance and data quality have been resolved. Internal and external clients have provided unsolicited positive feedback on IT’s overall performance and responsiveness, which is evidence of the success of this approach.

The organization adopted an integrated change model consisting of people, process and technology (figure 9). The focus on “people” means ensuring that the right people are in the right roles with the right expectations for their performance. This effort will be completed over a four- to six-month time frame. Optimizing these processes will take longer; however, preliminary definitions of governance, project management and quality management are already underway. These will be refined over time through
use and feedback. Technology and/or tools are being implemented to drive efficiency in previously defined processes, which are executed by skilled people. This organization has now deployed and implemented a quality management tool, which is enabling the organization to evaluate its project management and portfolio management options more efficiently, accurately and comprehensively.

**Conclusion**

The consultant team used COBIT Quickstart to evaluate the current state of the organization and the BSC to define and refine the vision and strategy. Leveraging both of these frameworks, a three-year road map was presented, which will evolve the organization’s maturity level to at least a level three. The organizational assessment was completed four months after the engagement concluded. This resulted in the release of several low-performing associates, the elimination of low-value positions, and the creation or redefinition of several critical roles. Although processes are still being developed and refined, the organization’s internal and external clients have already experienced improved system performance, proactive support and a customer-centric attitude through IT leadership.

**Serena Frank, PMP**

has been a leader in strategy and project management for nearly 25 years. Frank is the principal consultant for 360° performance excellence, which includes corporate strategic planning, governance, project management office and organizational alignment, at Diane Meiller & Associates in 2009. She is currently leading engagements focused on project management, organizational strategy and development, metrics-based management, process improvement, leadership development, risk management, and governance. Frank has previously worked at Walt Disney World, Harcourt, and Wyndham Vacation Ownership.

**Endnotes**


---

**Laugh & Learn: Cloud Computing and the Genie**

*By Corjan Bast*

A chief information officer (CIO) who recently got involved in her first cloud computing initiative was walking on the beach in Atlantic City, New Jersey, USA, when she came across a bottle. When she rubbed the bottle, a genie appeared. The genie was so grateful for being freed that he said that he would grant the CIO one wish.

The CIO thought about it for a moment, and then said, "I've always wanted to go to Bermuda. What I really wish is that you would build me a superhighway from Atlantic City to Bermuda so I could drive there easily."
The genie got annoyed, saying, "What kind of idea is that? Do you know how hard that would be and how much concrete it would take? Not to mention the environmental impact…"

So, the CIO said she would think of another wish. "OK then, what I want is this," she said. "I wish that all the applications that my organization is currently running, new or old, developed in-house or off-the-shelf, are moved into the cloud."

The genie thought for a moment and then replied, "So, how many lanes did you want on that superhighway?"

Transitioning to the Cloud

Cloud computing is not a new phenomenon; the concepts have been around for years, but only recently have providers of cloud solutions started to offer innovative solutions that really benefit the organization. The move to the cloud for an organization, however, can be quite a challenge. It is probably not as complex as building a superhighway and taking into account considerations of the environment, complexity of design and impact on people’s habitat, but it is still something that will involve significant organizational change.

The first thing to do is to ensure a strong understanding of what cloud computing is all about. For example, the CIO in the story wants to move all applications to the cloud. But it may not make sense to run all applications in the cloud. It may not be possible or necessary to run applications developed in-house in a virtual environment.

To determine the need and appropriateness of moving an application to the cloud, try to find out the business challenge: What is being solved by running the application in a virtual environment? If it is improved availability, consider the availability processes of ITIL to see whether something is lacking there. If it is cost, there may be a cheaper option; consider the COBIT processes that focus on the financials. For example, AI5 Procure IT resources can improve the organization’s ability to negotiate good deals and obtain value for money. DS9 Manage the configuration can help clarify the cost of assets, reduce the number of software licenses that are not used, etc. There are many more processes provided by COBIT that can help focus on the financial side of IT.1

In addition, perhaps the application or service that is intended to move to the cloud already exists in the cloud in one way or another. Moving an organization to the cloud will mean massive change, and a solid strategy is essential to back it up. It seems that the CIO in the story does not have a clear picture yet. Here are some tips to get started:

1. Try to clearly understand the types of clouds. There are two primary types: the public cloud and the private cloud (a third one, the hybrid cloud, is a combination of the two).
2. Understand the three major cloud service models: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

There are some good sources to get started:
- Defining a Framework for Cloud Adoption,2 which provides a good overview and a framework to take the first steps
- Cloud Computing for Dummies3
- Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives4
- Cloud Computing Management Audit/Assurance Program5
Once a solid understanding of cloud computing is reached, it may be time to start an awareness and training program to help the organization move forward and prepare itself for the necessary change. Here are a few ingredients:

- Start with a message from the CIO that outlines the strategic direction for the organization and the benefits that the cloud will bring.
- Start training key employees on the concepts, terminology and fundamentals of virtualization and cloud computing.
- Provide certification at the end of training to help build credibility for the program.
- Offer town-hall sessions and lunch-and-learn meetings to engage employees and involve them. Key people will move on to learn about the tools and software products that the organization starts using.

Do not underestimate the journey of cloud computing; anyone who believes that adopting cloud computing is as easy as flipping a switch probably also believes in fairy tales. But, with the correct approach and a good understanding before the journey begins, there is no need for a genie in a bottle, either.

Corjan Bast

is global product manager of ITpreneurs, where he is responsible for overseeing the IT governance portfolio. He works closely with experts at standards authorities to shape best-practice standards into innovative learning solutions. In addition, he collaborates with other professionals to publish articles and present the latest trends in the IT governance arena at industry consortia events. Previously, Bast was an IT governance consultant for a firm that focused on assisting Fortune 1,000 organizations implementing IT governance frameworks, such as COBIT and Val IT. He currently resides in Tampa, Florida, USA, and can be reached at corjan.bast@itpreneurs.com.

Endnotes


3 Hurwitz, Judith; Robin Bloor; Marcia Kaufman; Fern Halper; Cloud Computing for Dummies, Wiley Publishing, USA, 2009


5 ISACA, Cloud Computing Management Audit/Assurance Program, USA, 2010, www.isaca.org/auditchemnents. In addition to this audit program and the previously noted white paper, ISACA also offers a webcast, held a virtual seminar (archive available) and dedicates a web page in its Knowledge Center to the subject.

Solo Cup: Using COBIT to Develop IT Policies

By Michael Ryan, CIA, CPA, and Kumar Setty, CISA

The following case study represents an example in which COBIT was used to assist in the development of a set of IT policies. COBIT was used effectively to identify the key control elements for Solo Cup Co.’s initial set of draft IT policies. COBIT was selected because the organization recognized it as the standard and framework for IT controls. In addition, the control objectives presented by COBIT link very well with Solo’s existing IT processes. The principal advantage of using COBIT was that it affords flexibility and ensures sufficient coverage through its detailed control objective statements, ensuring that no critical areas were neglected.

Use of COBIT

Developing an IT policy framework from scratch can be a very daunting challenge for even the most experienced audit professionals. It is not uncommon to find even larger companies lacking an IT framework and policies. Solo inherited a broader set of policies from IT and then utilized COBIT to develop the secondary nodes of its draft IT policy framework (figure 1).

At Solo, the policy framework was defined to cover the following major IT general computer control areas:

- Ensure systems security.
- Manage the configuration.
- Manage data.
- Manage operations.
- Install and accredit solutions and changes.
- Manage problems and incidents.
• Manage third parties.
• End-user computing

The major general computer control areas were used to develop the IT policy framework shown in figure 1 and represent, to a large extent, the top node.

The top node of figure 1 represents the policy areas that were inherited from IT. The COBIT guidelines were used to further refine the subcontrol areas below the top node. The COBIT control objectives were added to Solo's risk control matrix and were prefixed with the question “What ensures that...?”

Once the basic framework was established, a set of draft IT policies was developed by asking the question: What are we supposed to do? This question enabled IT and the audit teams to develop the major policy topics and appropriate policy language to ensure control objective compliance. Then, the procedures within the policies were developed by asking the question: How are we supposed to do it? This question facilitated the development of the specific procedures within the policies to ensure that the appropriate and correct actions were linked back to the original control objectives.

The first versions of the policies were checked for adequacy by comparing the policy content and the risk control framework with the appropriate COBIT control areas. Subsequent refinements of the policies were developed in cooperation with IT and by prefixing the COBIT control objectives in the risk control matrix with “What ensures that...?” This question facilitated the identification of content gaps along with the comparison with COBIT control objectives to ensure that existing controls covered...
the elements of the COBIT controls. After gaps were identified, the policies were edited to close content gaps. After several iterations between internal audit and IT management, IT policies were developed and made available to the entire company.

**Example—Developing the User Access Management Policy**

Access control was identified as a critical element in the top node of Solo’s IT policy framework (figure 1). Using COBIT, it was determined that user access management should be a subelement of access control. The User Account Management control objective (figure 2) makes reference to the life cycle of user accounts with respect to hires, changes and terminations. Using Solo’s existing access control policy and the COBIT control objective in the risk control matrix (figure 3), a general outline and resulting first draft of the user access management policy were developed.

Prefixing the control objective in the risk control matrix with “What ensures that..?” enabled the IT and audit teams to further develop the first draft of the user access management policy by checking each part of the COBIT control objective, which resulted in a subsequent refinement of the first draft.

The user access management policy draft then underwent successive refinements by asking the question “What are we supposed to do?” This question enabled the team to determine that there should be a topic devoted to separations of employees from the company and that a secure notification process, an execution process and an audit trail of the separation should be developed and outlined in the policy (figure 4).

The associated procedures were then further developed by asking, “How are we supposed to do it?” The specific procedures for notification of separation, execution of separation and recording of the separation event were developed and refined to complete the final draft of the policy.

The COBIT control objective was used to develop successive refinements to the user access management policy. To identify content gaps, the “What ensures that...?” column was prefixed to the control objective within Solo’s framework (figure 3). After gaps were identified, the policy was edited to close the content gaps.

---

**Figure 2—COBIT 4.1 Control DS5**

Deliver and Support
Ensure Systems Security

**CONTROL OBJECTIVES**

**DS5 Ensure Systems Security**

**DS5.1 Management of IT Security**
Manage IT security at the highest appropriate organisational level, so the management of security actions is in line with business requirements.

**DS5.2 IT Security Plan**
Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users.

**DS5.3 Identity Management**
Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.

**DS5.4 User Account Management**
Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.

**DS5.5 Security Testing, Surveillance and Monitoring**
Test and monitor the IT security implementation. In a proactive way, IT security should be reaccredited in a timely manner to ensure that the approved enterprise’s information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.

**DS5.6 Security Incident Definition**
Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.

**DS5.7 Protection of Security Technology**
Make security-related technology resistant to tampering, and do not disclose security documentation uncessarily.

**DS5.8 Cryptographic Key Management**
Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure.

**DS5.9 Malicious Software Prevention, Detection and Correction**
Put proactive, protective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).

**DS5.10 Network Security**
Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detections to authenticate access and control information flows from and to networks).

**DS5.11 Exchange of Sensitive Data**
Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.

Source: IT Governance Institute, COBIT 4.1, USA, 2007
### Figure 3—Risk Control Matrix Excerpt

| Controls provide reasonable assurance that financial reporting systems and subsystems are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data. | WHAT ENSURES THAT... Procedures exist and are followed relating to timely action for requesting, establishing, issuing, suspending and closing user accounts. (Include procedures for authenticating transactions originating outside the organization.) | Source: Solo Cup Co. Used with permission. |

### Figure 4a—Draft User Access Management Policy

**User Access Management Policy**

- Each email sent to the Service Desk is automatically created and forwarded to the Application Security Administration Team (Security Admin) mailbox and other defined service groups within Solo Cup.

  - Emails to the Service Desk website are imported into the Track-it ticketing system. A work order ticket is automatically created and forwarded to the Application Security Administration Team (Security Admin) mailbox and other defined service groups within Solo Cup.

  - The Application Security Administration Team reviews the request and determines if it requires action on their assigned applications/services. If action is required, required approvals are gathered if the application is ‘critical’, access is granted or changed and the ticket is marked ‘completed’. MS Access database Security Tables are manually updated to maintain the users’ access. If action is not required, the ticket is marked ‘completed’. When all service groups have ‘completed’ their copies of the ticket, the parent ticket is closed and a confirmation of services email is automatically sent to the requestor.

- **7.3 Separations:**
  - Managers call their local HR manager to request a Separation Form code, which is required to gain access to the Separation Form. Each of the Field and Corporate HR Managers has access to the code list. It is the responsibility of the HR manager to verify the legitimacy of the request.
  - At the Service Desk website, Managers enter the code and access a standard Separation Form. When the form is electronically submitted, an email to the Service Desk mailbox is automatically generated and imported into the Track-it ticketing system. A work order ticket is automatically created and forwarded to the Application Security Administration Team (Security Admin) mailbox and other defined service groups within Solo Cup.
  - The Application Security Administration Team reviews the request and determines if it requires action on their assigned applications. If action is required, access is terminated and the ticket is marked ‘completed’. Access termination responsibilities include the supporting IT systems required to access the application (network, UNIX, mainframe, databases). MS Access database Security Tables are manually updated to maintain individual users’ termination history. If action is not required, the ticket is marked ‘completed’. When all service groups have ‘completed’ their copies of the ticket, the parent ticket is closed and a confirmation of services email is automatically sent to the requestor.

Source: Solo Cup Co. Used with permission.
Conclusion

COBIT offers a proven and effective set of guidelines for ensuring that IT policies present sufficient coverage of common control objectives and for identifying control gaps. The control elements within COBIT contained the appropriate content, depth and breadth to ensure that the major IT policy control areas were meeting the control objectives as described by COBIT. The COBIT framework streamlined the process of developing a comprehensive set of IT policies. In the absence of COBIT, this effort might not have been as comprehensive and could have required an inordinate amount of time.

Michael Ryan, CIA, CPA

has 18 years combined internal and external auditing experience for a variety of organizations including Solo Cup Co., Career Education Corp., United Airlines and PricewaterhouseCoopers LLP. His experience includes building new audit departments and improving the efficiency and effectiveness of existing departments. His primary responsibility over the past seven years has been to build and execute the US Sarbanes-Oxley Act 404 compliance strategies, focus and coverage for two multibillion-dollar companies with brand-new audit functions. Ryan is the director of internal audit for Solo Cup Co. and a past officer of the Northwest Metro Chicago Chapter of The Institute of Internal Auditors (IIA).

Kumar Setty, CISA

has more than 10 years of experience in the areas of data analysis, systems administration, auditing and computer security. Setty worked as a consultant for many small to large companies performing US Sarbanes-Oxley Act compliance, auditing, fraud detection and prevention, and computer security reviews for a variety of industries and organizations. He is the IT audit manager for Solo Cup Co.

The Need for Value Management Has Never Been Greater

By Peter Harrison

The disciplines of value management, as contained in The Val IT™ Framework 2.0, will have even more relevance in 2011 as the ever-increasing focus on value drives many enterprises to review seriously and strengthen their approaches and practices to optimising business value from their portfolio of IT-enabled investments and services.

The Val IT 2.0 value management practices and processes are more relevant today than when they were when first published...
in 2008. The International Organization for Standardization (ISO), legislators and analysts are now talking the value language—promoting the need for stronger business governance of IT and the need for IT to strengthen its business partnerships to jointly focus on outcomes. Indeed, many public and private enterprises are now successfully institutionalising the value management disciplines. This is resulting in:

- An increased understanding of the nature of value and how it is created
- Transparency in costs, risks and benefits
- The ability to make more informed business decisions (based on business value)

What Has Changed Since Val IT 2.0 Was Launched?
The challenges most enterprises have in realising business value from their IT-enabled investments have remained the same—namely, how to understand and manage IT, not as an end to itself, but as a means to enable business outcomes.

However, the opportunity for value management disciplines to add value has grown significantly since 2008. This is evidenced by the impact of the global financial crisis (GFC) on many enterprises. The GFC highlighted value management weaknesses in many enterprises. It has been identified that many enterprises were facing unparalleled challenges in managing their (IT) investment portfolio. In particular, these challenges involved the four issues outlined in figure 1.

During the GFC, it was difficult to avoid the ‘slash and burn’ of the portfolio of IT-enabled investments. However, approaching this cutback reflected a great deal on the maturity of those enterprises in value management. Several enterprises, in response to directives to cut portfolio spending, cut 20 percent off all projects. This response indicates insufficient understanding of the value of prioritising what was the least valuable 20 percent to the organisation.

Working out the GFC impacts has brought a return to limited spending on growth initiatives (including those enabled by IT) and, thus, the need to prioritise and fund the most valuable opportunities that these investments provide. There is now much more caution and interest in value-based approaches to this task.

In the meantime, failures of large IT-enabled transformation initiatives continue and feature prominently in the press, such as the headline from the UK newspaper The Independent: ‘Labour’s Computer Blunders Cost £26bn’. The article featured alarming details on the ‘series of botched IT projects [that] has left taxpayers with a bill of more than £26bn for computer systems that have suffered severe delays, run millions of pounds over budget or have been cancelled altogether’.

The author concludes that many more enterprises are now ready and keen to have a serious value management conversation. When making investment decisions, enterprises are recognising that outcomes and value are far more important focuses than cost and technology.

<table>
<thead>
<tr>
<th>Figure 1—The Unparalled Challenges Facing Organisations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Cost take out.</strong></td>
</tr>
<tr>
<td>How to quickly remove the impact on our budget—in cost and effort—of low value investments?</td>
</tr>
<tr>
<td><strong>2. Prioritise.</strong></td>
</tr>
<tr>
<td>How to prioritise “first things first” so that focus is only on those investments that will deliver the greatest value?</td>
</tr>
<tr>
<td><strong>3. Understand value.</strong></td>
</tr>
<tr>
<td>How to ensure that the business understands, defends and realises the value from the investments it makes?</td>
</tr>
<tr>
<td><strong>4. Align IT spend.</strong></td>
</tr>
<tr>
<td>How to best align IT spending with the business strategy, to ensure that the business is investing in the right things?</td>
</tr>
</tbody>
</table>
standard (not a framework) for corporate governance of information technology. It defines six principles, on which it is based:
1. Establish responsibilities.
2. Plan to best support the organisation.
3. Acquire validly.
4. Ensure performance when required.
5. Ensure conformance with rules.

This standard has been well received as a means of engaging business executives in the discussion of business governance of IT. As a framework for value governance and management, Val IT can support the implementation of the standard’s principles.

- **Legislative interest in improving governance around IT**—The US House of Representatives is currently considering a bill cited as the ‘Information Technology (IT) Investment Oversight Enhancement and Waste Prevention Act of 2009’ (S. 920). This bill seeks to require federal agencies to have greater oversight of project progress and success and more detailed reporting on, amongst other things, ‘the achievement of program and investment outcomes’. This bill aims to assist in holding agencies accountable for project spending and achievement of business value. Val IT, as well as COBIT and Risk IT, will be well placed to support agencies with this legislative requirement.

- **Articles and book publications on business value of IT**—InformationWeek recently ran a series of articles titled ‘The Business Value of Technology’, and books continue to be written on this subject. The Real Business of IT—How CIOs Create and Communicate Value argues that the importance of the IT function is being able to show value for money, focus on business outcomes (vs. on the ‘machines’ of IT), manage the portfolio transparently and manage IT projects as business investments. All of these messages align with the Val IT framework.

- **Research and surveys**—The subject of whether IT projects are delivering measurable business value has been the subject of many research studies. One of the latest is ‘Shifting Focus—Shifting Results’ from the CIO Executive Council and Capability Management. The key findings affirm the challenges of value management:
  - 20 years of improving project practices and standards have not led to improved value delivery.
  - 82 percent of IT business cases are designed to deliver IT assets only.
  - Almost half of CIOs (46 percent) consider their current business case a ‘destroyer’ of value.
  - 82 percent of businesses do not have a formal process to govern benefits realisation.

There is currently much discussion and seriousness of intent about value governance and management, and a growing need for enterprises to comply with good practices in this area. Val IT is well placed to support this need.

**Practical Experiences of Enterprises After Introducing Value Management Based on Val IT**

The author has assisted several global enterprises in developing or strengthening their value management disciplines. These include:

- A manufacturing firm where the challenge of prioritisation of transformation programs was addressed by introducing a portfolio management value scoring framework and a benefits realisation process
- A mining enterprise where the challenge of the historical tactical focus of IT was addressed by introducing stronger portfolio management disciplines with alignment to business strategy and stronger governance structures and processes

The experiences from these and other enterprises in introducing value management emphasise the need to develop value management capabilities that recognise a number of points: the maturity of the organisation, the level of executive support and the need to manage this as a change programme in its own right. Further reading on the practicalities of introducing value management can be found in the Val IT publication Getting Started With Value Management.

To articulate these types of experiences, ISACA is continuing to identify and record Val IT success stories. A recent case study detailed the implementation of Val IT by ICW.

**Future of Val IT**

Val IT 2.0 was developed to help enterprises optimise the realisation of value from IT investments. It is a governance framework that consists of a set of guiding principles and a number of processes that conform to those principles and are further defined as a set of key management practices. It supports the business (enterprise) governance of IT.
The processes and key management practices are structured into three domains:

- **Value Governance (VG)**—Aims to ensure that value management practices are embedded in the enterprise, enabling it to secure optimal value from its IT-enabled investments
- **Portfolio Management (PM)**—Aims to ensure that the enterprise secures optimal value across its portfolio of IT-enabled investments
- **Investment Management (IM)**—Aims to ensure the enterprise’s individual IT-enabled investments contribute to optimal value

An overview of the processes in each domain is found in **figure 2**.

As part of the evolution and consolidation of ISACA’s frameworks, the Val IT framework will be incorporated into the new COBIT® 5 framework and will form the value delivery components of COBIT 5 practices.

In conclusion, the Val IT Framework 2.0 provides proven practices to help enterprises address the value management and governance challenges described in this article. The principles and practices of Val IT will be relevant in 2011 and beyond to enterprises who seek to implement and operationalise value management disciplines.

**Peter Harrison**

is the lead for the value management practice with IBM Australia. He was a member of the ISACA Val IT Steering Committee and development team and is a member of the ISACA COBIT 5 Task Force.

**Endnotes**

1 This is based on the author’s work with global clients.
New COBIT Case Study: Banco Supervielle S.A.

Banco Supervielle S.A. has grown considerably and steadily in the last 15 years, and is now one of the main private banks of the Argentine Republic. To increase this expansion, the directors of the enterprise have focused on improving technology services administration, specifically by implementing a master plan providing for the governance of IT.

In 2009, Banco Supervielle S.A. launched an IT governance project, which stemmed from key issues such as the improvement of strategy-business alignment; the need to generate a language friendly enough to be interpreted, managed, improved and understood by both IT and business areas in terms of fulfilling internal controls and being aware of each person’s role within IT processes; and compliance with all regulations set by the different controlling agencies governing the bank’s activity—most important, the Central Bank of the Argentine Republic.

Based on the needs of the enterprise, COBIT was seen as the best reference framework to use as a guideline. Using COBIT’s control objectives and processes allowed Banco Supervielle S.A. to trace a road map to better achieve the enterprise’s desired maturity level. Several initiatives are underway, and business continuity has been improving. Management is confident that implementing the COBIT framework will enable the bank to achieve its objective of growth.

Click here for the full text of this and other COBIT case studies.