COBIT® *Focus*

The newsletter dedicated to the COBIT® user community

October 2009, Volume 4

In This Issue…

How Could ITSM and COBIT Complement Each Other?
By Suresh GP ....page 1

Implementing and Continually Improving IT Governance
By Gary Hardy ....page 3

A Practical Approach to Implementing COBIT
By Lance Horne.................................page 5

Microsoft SharePoint Governance Using COBIT 4.1
By Dave Chennault and Chuck Strain.......................................page 6

COBIT as a Method for Deliberate and Emergent Strategies
By Werner Syndikus........................page 13

Identify, Govern and Manage IT Risk
By Dirk Steuperaert ....page 15

How Could ITSM and COBIT Complement Each Other?

By Suresh GP

The following case study is based on the author's recent engagement with a customer in Hong Kong.

Project Background

An organization wanted to assess the effectiveness of its existing service management processes and get insight into industry best practices on IT service management (ITSM). Therefore, an ITSM process review and planning service for the customer was performed based on structured assessment criteria.

From the assessment results, it was clear that there was a lack of tight integration between process and tools. The defined key performance indicators (KPIs) were too broad to measure the efficiency and effectiveness of the processes. Guidelines to define measurable KPIs and facilitate process alignment with a service management tool were recommended. Based on these recommendations, the customer decided to implement improvements as follows:

- New integrated tool set
- Clear process ownership using Responsible, Accountable, Consulted and Informed (RACI) charts
- Well-defined KPIs
- Improved management reporting

These parameters were driven by identified process owners within the organization, to obtain the desired results. After a six-month period, proactive follow-up was completed, to evaluate and understand the maturity of processes and metrics, by conducting a post implementation review (PIR).

The PIR provided the following insights:

- 200 high-priority incidents remained unresolved, breaching agreed service levels.
- Only three problem records had been recorded.
- The service desk was struggling with the volume of calls.
- Service desk agents were spending more time than expected resolving calls.
- Key metrics such as first call resolution rate and calls resolved before service level agreement (SLA) breach were only achieving 50-60 percent.
- Overall customer satisfaction was reported at 60 percent, based on a six-month review of stakeholders.

Continued on page 2

Action Plan
These were not the results that were forecasted and were not good news to the stakeholders. To build faith and confidence with the customers, a plan was formulated to carry out a quick assessment of how the processes were being operated. The assessment was carried out based on HP Service Management assessment material with criteria based on COBIT® and IT Infrastructure Library (ITIL) methodologies. The intent of the plan was to deliver the results and associated recommendations within a week to the executive council.

The next week was spent in review with the service desk support staff, process owners and other key stakeholders of the project, to gain a complete understanding of the operating environment and the issues being experienced. Within the week, it was realized that although processes were in place, there was a fundamental lack of IT governance practices. In response to this, it was decided to utilize COBIT and, in particular, focus on three key COBIT processes. These processes formed the basis of a "benefits realization plan," aimed at ensuring that planned benefits were achieved in a demonstrable manner:

1. **ME1 *Monitor and evaluate IT performance***—Performance monitoring was developed based on the balanced scorecard approach, to provide an all-around view of IT performance as part of the enterprise monitoring system. The review of performance against targets revealed that several incidents that had breached SLAs had dependency on third-party vendors and support from specific internal teams; hence, remedial actions were initiated as follows:
   - Establishment of underpinning contracts with third-party vendors and operation level agreements (OLAs) with internal support teams
   - Follow-up of all monitoring, reporting and assessments along with tracking of the results of remedial action committed
2. **DS8 *Manage service desk and incidents***—It was revealed that service desk support staff members were involved in analyzing the root cause of incidents, as opposed to finding workarounds and resolving incidents. This consumed a lot of their time and invariably increased the volume of unresolved incidents. To improve efficiency, a number of procedural guidelines were introduced and monitored:
   - The information recorded on incident records, including the steps required to reproduce issues, had to be sufficient enough for the next level of support to take up the call.
   - Instructions and controls were put in place to ensure that the service desk closed incidents as soon as a workaround was successfully implemented.
   - Workarounds were recorded in the knowledge base to help in resolving repeated incidents quickly.
   - The incident controller was automatically alerted to ensure that no incident record stayed in "work in progress" status past 75 percent of SLA time.
   - The RACI chart was revisited to set the expectations and make ownership and responsibilities clear for everyone involved.
3. **DS10 *Manage problem***—Problem management staff members were asked to increase focus on the following as part of this IT process:
   - Ensuring that careful categorization and prioritization were carried out before starting investigation and diagnosis
   - Giving focus to high-priority problems based on business impact and reoccurrence potential
   - Driving the identification of triggers and workarounds to mitigate the impact of incidents and reduce the time taken to achieve resolution
   - Taking ownership of problems and ensuring resolution updates to the service support staff to enable problem matches
   - Conducting problem management reviews once a month to maximize system availability and improve service levels, customer convenience and satisfaction

An IT governance group was established, comprising process owners, key process managers and associate members from key suppliers operating service management processes, to monitor the progress and results of the benefits realization plan. Communication was initiated with the senior management team to ensure their support and commitment in driving the embedding of the processes and procedures and to set their expectations regarding the expected results and the time that would be needed to build toward the identified end goals. The IT governance group was asked to submit a monthly status report regarding progress, issues and achievements against the benefits realization plan to the senior management team.

Continued on page 3

Results of the Approach
Within three months of implementation, visible improvement began to be revealed. The key metrics mentioned previously showed results of 82-85 percent of metrics achievement, and there was clear ownership among teams regarding the different tasks on which they were working. The service desk agents were handling the right volume of calls and harnessing the knowledge base extensively to resolve incidents quickly.

The customer survey results after the three-month period showed 80 percent satisfaction with clear indications that they would continue to improve. Customers and other stakeholders were able to appreciate the results of COBIT being used to complement and support ITSM, which was enabling the delivery of both value and control to be measured and demonstrated.

Suresh GP
is an ITSM consultant working for HP Global Delivery India Center since 2005. He is an IT service manager and holds the COBIT® Foundation Certificate. He specializes in delivering engagements on ITIL process consulting, ITIL assessments and the implementation of an IT governance framework for customers specifically in the Asia-Pacific and Japan region. His expertise also includes business analysis, process and service management tool alignment, and service management tool implementation using HP OpenView products.

Implementing and Continually Improving IT Governance

By Gary Hardy, CGEIT

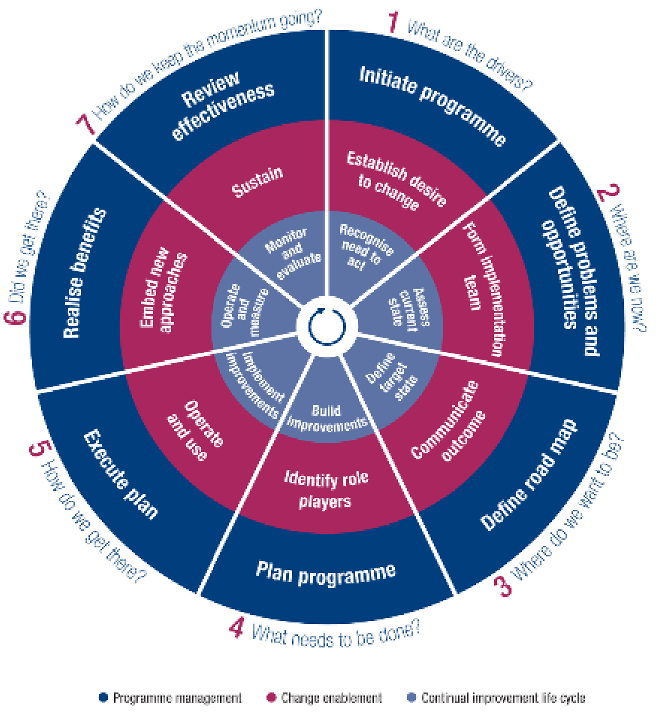
The improvement of IT governance is increasingly recognised by top management as an essential part of enterprise governance. Effective enterprise governance of IT will result in improved performance and enables compliance with external requirements, yet successful implementation remains elusive for many enterprises. Processes need to be supported with carefully prescribed roles, responsibilities and accountabilities. They also require an appropriate set of guiding principles and organisational structures that fit the style, skills and operational norms specific to the enterprise.

For many years ISACA® has researched this key area of enterprise governance to advance international thinking and provide guidance in evaluating, directing and monitoring an enterprise's use of IT. ISACA has developed groundbreaking frameworks—COBIT, Val IT™ and most recently Risk IT—to help enterprises implement sound governance mechanisms. Indeed, implementing good IT governance is almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin the frameworks and enable the design of effective policies, processes and procedures.

However, frameworks, best practices and standards are only useful if they are adopted and adapted effectively. To that end, before year-end, ISACA will release a new version of the *IT Governance Implementation Guide*, which has been renamed *Implementing and Continually*

Continued on page 4

Figure 1—Seven Phases of Implementation Life Cycle



Improving IT Governance due to the extensive new guidance that is being provided.

There are many challenges that need to be overcome, and issues that need to be addressed if IT governance is to be implemented successfully. In addition to preparing the board and managers to ask hard, pointed questions and putting a guiding framework in place, effective implementation of an IT governance programme also depends on several changes to both culture and behaviour.

In *Implementing and Continually Improving IT Governance*, the emphasis is one of continual improvement presented as a life cycle (**figure 1**). It is based on the extensive practical experiences and lessons learned by ISACA's unique membership base of IT governance, control, security and assurance professionals. It is not intended to be a prescriptive approach or the complete solution, but rather a guide to avoid pitfalls, leverage the latest good practices and assist in the creation of successful governance outcomes over time.

Every enterprise will apply its own specific plan or road map, depending, of course, on factors such as its industry and business environment and its culture and objectives. Equally important will be the current starting point. Few enterprises will have no IT governance structures or processes in place, even if they are not recognised as such currently. Therefore, the emphasis needs to be on building on what the enterprise already has.
The updated guide provides new additional material based on real experiences gained, including how to recognise the need, act and get management's commitment. One of the most important issues to be addressed when implementing IT governance is the management of often significant organisational change. The new guide covers this very important aspect with specific pointers at each phase of the life cycle.

COBIT Research Update

COBIT initiatives scheduled for availability in the fourth quarter of 2009:

- *COBIT® Mapping: Mapping of BS 25999 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of CMMI With COBIT® 4.1*
- *COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1*
- *COBIT® Mapping: Mapping of ISO 20000 With COBIT® 4.1*
- *COBIT® Mapping: Overview of International IT Guidance, 3rd Edition*
- *Implementing and Continually Improving IT Governance*
- *SharePoint Deployment and Governance Using COBIT® 4.1*

Risk IT initiatives scheduled for availability in the fourth quarter of 2009:

- *The Risk IT Framework*
- *The Risk IT Practitioner Guide*

The guide covers the following subjects:

- Positioning IT governance
- Taking the first steps towards IT governance
- Challenges and success factors
- Enabling change
- Implementing a continual improvement life cycle
- Using COBIT, Val IT and Risk IT components

The guide is also supported by an implementation tool kit, which contains a variety of resources that will be continually enhanced. The tool kit includes:

- Self-assessment, measurement and diagnostic tools
- Various presentations
- Related articles and further explanations

Gary Hardy, CGEIT
is director of IT Winners, an independent consultancy based in South Africa. He has been involved in the IT industry for more than 30 years. He has worked in a variety of IT roles, initially as a systems developer and project manager, then as a computer audit manager for a major oil company and group manager at Deloitte & Touche in London. He was previously director of consultancy for a major IT security company and a director of risk consulting at Arthur Andersen. He is currently an advisor to the ITGI and Deloitte, a thought leader on IT governance, and an author of many publications on related topics.

Editor's Note
For more information on *Implementing and Continually Improving IT Governance*, please visit *www.isaca.org*. The publication will be available in the ISACA Bookstore, *www.isaca.org/bookstore*. A zip file of Implementing and Continually Improving IT Governance—Supplemental Tools and Materials, as well as a PDF of *Implementing and Continually Improving IT Governance*, will be available as a complimentary download for ISACA members at *www.isaca.org/downloads*.

A Practical Approach to Implementing COBIT

By Lance Horne, CA (South Africa)

In the fast-paced, low-cost-of-ownership world of retail, "simplification" and "ease-of-use" are the watch phrases. Many retail IT executives are faced with the challenge of conformance to governance requirements[1] while having to display low cost of ownership (performance). This is especially true in a large-listed retailer operating according to a high-volume/low-margin strategy.[2] Being a leader in low-margin return requires extremely wise IT investment and fastidious measurement of return on investment for all IT assets. COBIT, through its tiered maturity models, provides a framework to balance cost of control vs. tolerance of residual risk in a measurable, consistent manner.

To successfully implement COBIT in such a cost-conscious environment requires specific baseline criteria to be in place before embarking on an IT culture-shifting methodology such as COBIT, including:

- There needs to be an appropriate corporate culture in support of the approach.
- Expressing senior executive support is fundamental to success.
- An independent custodian needs to drive the overall implementation plan.
- The plan itself needs to be easily acceptable.
- There needs to be simplified reporting of outcomes.
- There needs to be a commitment to invest.

An Appropriate Corporate Culture

Massmart's group of companies is fortunate to have the culture of always doing "what is right and ethical." At the same time, employees treat the company's assets as their own and respect the low-cost-of-ownership ethos. This ethos has been distilled by the company's current and previous chief executive officers (CEOs) and permeates the Massmart Group.[3]

Senior Executive Support

Any corporate framework for governance needs to be mandated and visibly supported at the highest level. The Massmart technology forum provides this framework in a formal charter mandated by the board of directors:

> *Massmart aligns its IT teams with the following international IT management standards. COBIT is a standards tool to measure compliance with the Massmart TIP strategy and accepted norms and governance practices with respect to IT. COBIT is a measurement system that is simple, can be self-administered by the chains, and gives the chain boards and the Massmart executive some level of assurance that Massmart is complying with generally accepted norms for a listed company of our size.*

An Independent Custodian

This was the second attempt at implementing a COBIT-based IT governance approach in the group. The first attempt used *COBIT® Quickstart* as an introduction to COBIT. This first approach was facilitated by an individual from one of the entities and

Continued on page 6

the assessment process was not maintained. Massmart did, however, benefit from the increased awareness from this initial implementation, which took place approximately five years prior to the current implementation. Since then, an audit committee was formally established, which gave rise to a group internal audit department, through its board-approved charter. The internal audit department is well supported and enjoys strong support from the CEO and board of directors.

An IT audit function was established within the internal audit department in response to an audit committee concern for technology risk. It was logical that one of these IT governance specialists champion the COBIT implementation across the Massmart Group, since they were independent from the IT divisions and brought board authority to the process.

Under IT audit guidance, the second attempt was well received. With the second attempt an approach to implementing COBIT was used that became known as "COBIT-light" within Massmart.

Easily Acceptable Process

"COBIT-light" was essentially the standard approach of performing maturity modelling using the high-level maturity models within each COBIT process. In this implementation, the COBIT generic framework was not used to measure maturity but instead was used to pose additional probing questions. This "light" approach allowed the organisation to cover all of COBIT without losing the audience across Massmart.

Simplified Reporting

Each division's IT maturity was plotted on spider diagrams showing their current and future maturity scores per process. This was presented to the group technology forum and then the board as a benchmarking of IT risk management across Massmart. Massmart's CEO acknowledged the approach as a best practice and requested ongoing training for all senior management staff, not only in IT, but also in operations.

Commitment to Invest

Ongoing investment is required to keep any culture of governance alive. Two training programmes were implemented across Massmart. The first training programme included ISACA's COBIT Foundation Course and IT Governance Implementation Course and was attended by all IT managers and business analysts. More than 30 senior managers across the organisation attended the courses.

The second workshop was the integration of a high-level training module in Massmart's management development programme. This programme is run annually and is required for managers wanting to advance in their careers at Massmart.

In summary, COBIT has received an elevated status and is reported on to the board of directors and, as a result, there have been fewer crises and more successes in delivering IT services to Massmart.

Lance Horne, CA (South Africa)
is senior audit manager at Massmart Internal Audit Services, responsible for the Massmart Group's IT audit team.

Endnotes

[1] All listed entities in South Africa are required to comment on the state of their governance according to the *King Committee Report on Governance, 2nd Edition*, known locally as King II. Refer to *www.iodsa.co.za/*.

[2] Massmart is a managed portfolio of nine wholesale and retail chains, each focused on high-volume, low-margin, low-cost distribution of mainly branded consumer goods. Refer to *www.massmart.co.za/*.

[3] Massmart received the Association of Certified Chartered Accountants (ACCA) award for the Best Sustainability Report (Non-Extractive Industries), South Africa.

Microsoft SharePoint Governance Using COBIT 4.1

By Dave Chennault, MCP, and Chuck Strain, CISA, MCSE, MCTS

SharePoint has grown into a software platform that is currently in production or planned for deployment in tens of thousands of organizations both large and small throughout the world. SharePoint's decentralized administration, workflow and forms automation, content publishing, and search capabilities married with a self-service model have given IT and end users the keys to unlock process bottlenecks and enable greater employee productivity. The ability to rapidly roll out SharePoint with decentralized administration and self-service publishing is one of the key reasons for its

Continued on page 7

acceptance and widespread success.

Unfortunately, many organizations have failed to realize the risk and liability that exist in an ungoverned SharePoint deployment. Users can produce Wikis, MySites and entire web portals easily from out-of-the-box tools and expose this information to employees, partners, customers and the general public. From there, any number of troubling issues can ensue, from the display of offensive material to the outright publishing and sharing of confidential intellectual property. Many organizations are unknowingly allowing the publishing of sensitive and strategically important information without proper security or protective strategies. If a SharePoint deployment is pointed to the World Wide Web, which is done in many cases because the platform lends itself nicely to becoming the company web site, the potential for exposure grows exponentially. The amount of risk is directly proportional to the number of users that can access content. A sensitive piece of information only seen by a few internal resources is one thing, while a sensitive piece of information available through the web is quite another. A recent survey conducted by Rohati Systems of 117 chief information officers found that more than 31 percent feared that a lack of proper security in collaborations systems, such as SharePoint, could lead to a data breach.

A large number of SharePoint deployments are launched without any thought or planning to implement proper governance. When asking “what are you doing to govern your SharePoint deployment?,” the questioner is often met with blank stares. Many organizations that currently have SharePoint deployed may be at great risk and not even realize it.

This article will explore why proper governance is an essential component to mitigate risk and ensure successful deployment and operation of SharePoint. The article examines the issues and problems and provides concrete steps for applying COBIT 4.1 as a framework for SharePoint governance.

The SharePoint Effect

Although SharePoint has been widely adopted, it has often been accompanied by a wave of frustration and false starts that the authors call the “SharePoint Effect.” The pressure on IT resulting from the SharePoint Effect causes organizations to look for shortcuts and organic deployment approaches. This is potentially risky and damaging to an organization.

The SharePoint Effect is characterized by:

- SharePoint users hijacking control, adding content, and setting policies and permissions independently of enterprise planning or strategy
- Users camping outside the SharePoint administrator’s door, demanding a never-ending stream of enhancement, site creation and integration requests
- Content monitoring and control growth beyond the reach of IT resources
- Uncontrolled access inviting unauthorized exposure of sensitive data
- Business goals that are not properly aligned with content creation

Many readers may recognize these symptoms from their own work. Governance can help mitigate the risk and results of the SharePoint Effect.

SharePoint Governance Options

A number of organically developed resources for SharePoint governance can be found by searching the web. Microsoft also hosts a web site called the Governance Resource Center for SharePoint Server 2007.[1] This site and others contain a wealth of information about SharePoint governance, and they are certainly worth review by anyone concerned with SharePoint governance. Unfortunately, after reviewing these materials, the authors have not found adequate material to relate the governance process to specific control objectives that would identify and prescribe SharePoint governance methodologies known to be consistent with audit and regulatory compliance.

Suggested Approach to SharePoint Governance

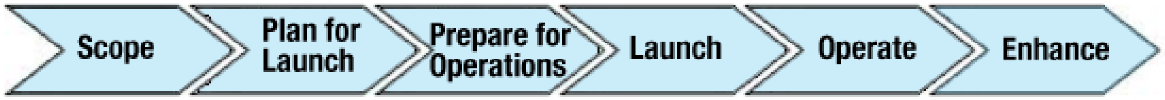
Given the existing shortcoming of current SharePoint governance options, a governance framework has been developed with the following guiding principles in mind:

- SharePoint requires controls and repeatable processes to ensure its orderly deployment, operation and maintenance.
- A team of senior business and technical users is required to set policies, procedures and guide the ongoing deployment.
- Management reviews should be built into the governance policies and procedures.
- Business needs should lead technical decisions.
- IT resources including staff and systems should be leveraged and integrated into SharePoint.

Having seen first-hand how SharePoint is planned, deployed and maintained, a governance framework has been developed that parallels real-world

Continued on page 8

Figure 1—Processes Framework



SharePoint deployments.[2] The resulting framework and practical and prescriptive guide can be found in the upcoming ISACA book *SharePoint Deployment and Governance Using COBIT® 4.1*. It represents the first-known attempt to map COBIT® 4.1 in a practical way to the governance of SharePoint.

It is never too late to start proper governance for a SharePoint deployment. The methodology described here is designed for new or existing SharePoint deployments. If SharePoint is already deployed, the steps outlined in the upcoming book and within this article can be followed (with some minor modifications) to implement a successful governance program.

Methodology Overview

The governance framework blends activities from each area of COBIT 4.1 into cohesive phases for the deployment, operation and enhancement of SharePoint 2007. An overview is shown in **figure 1**.

The framework groups COBIT 4.1 processes and SharePoint-specific activities within each of the six phases of the deployment life cycle described in **figure 1**. Once the COBIT 4.1 process is mapped within a phase, specific activities that relate to SharePoint are prescribed to satisfy the requirements of the process. A narrative explaining the risk of not conforming to the guideline and a definition of risk mitigation, followed by a detailed discussion of a prescriptive approach for mitigation or compensation to meet the objectives of that process, are offered in the upcoming ISACA book. A sample is included in **figure 2**.

The COBIT 4.1 process P02 *Define the information architecture* is used here to illustrate how COBIT principles can be applied to a deployment. This process is placed within the scope phase of the framework described previously.

The prescribed activities capture the essence of relevant control objectives within the SharePoint context, rather than an explicit one-to-one mapping. It is important to note that the upcoming book explicitly maps every COBIT 4.1 process to one of the six phases in **figure 1**. All of the processes in COBIT 4.1 are relevant and should be thoroughly reviewed and applied to form a solid governance plan for SharePoint 2007. (The processes defined in the mapping in **figure 2** are denoted by a letter rather than a number to highlight that these items are SharePoint-specific and related to the COBIT process P02.)

This framework is a starting point that can be changed to meet the specific needs of each organization. The activities and tasks addressed are generic enough to form a foundational basis for the application of COBIT 4.1, while allowing the flexibility to identify specific process areas to meet the needs of each unique initiative.

Implementation—Getting Started

Knowing how to get started is often the biggest impediment to successful governance. The remainder of this article offers a suggested approach

Continued on page 9

Figure 2—Sample Risk and Mitigation Strategy

PO2 Define the Information Architecture
A. Identify scope of site types in deployment. B. Identify owners. C. Identify roles. D. Develop process for site request, approval and creation with auditing, including content types and permissions.

Risk: A lack of proper assignment of roles and responsibilities will inhibit organizational directives and delegation of responsibilities.

Mitigation/compensation: Develop a properly defined organizational chart with specifically defined roles and responsibilities and an orderly, accountable chain of command.

to begin implementation of a governance framework. Once the steps have been completed, a SharePoint governance program incorporating processes and controls satisfying desired business alignment objectives and regulatory requirements should be well underway.

Step One—Meet With IT and Project Management Staff

The governance process begins with a meeting of key IT resources participating with the SharePoint initiative. This meeting should be held as a two-hour workshop. The following activities reference a subset of key processes from the scoping phase of the governance framework and give a general guide of what should be accomplished with IT staff to start the governance process:

1. A SharePoint governance champion should be identified to guide the initial governance activities outlined within this section. This will often be a member of the IT staff or an outside consultant. The governance champion will be responsible for all of the activities leading up to a self-sustaining SharePoint governance framework and steering committee.
2. The governance champion should begin the governance initiative by identifying all of the relevant staff associated with SharePoint and their roles. These individuals are likely to be later assigned to infrastructure, support and development teams or to the steering committee in alignment with the objectives of COBIT PO4 *Define the IT processes, organization and relationships*.
3. If SharePoint has been deployed, a survey should be created of current SharePoint sites, including a site map, and any documentation associated with the current deployment should be reviewed. This is similar to COBIT PO2 *Define the information architecture*.
4. Significant risks to adopting governance for SharePoint should be identified, including:
   - Inadequate executive sponsorship and direction
   - Unwillingness of IT to align or support business needs
   - Inability of the governing body to make decisions
   - Internal staff or third parties not following the policies and procedures set by the governing body
   - IT staff lacking discipline to follow policies and procedures
   - SharePoint being deployed widely across the organization, and current users being resistant to governance because they do not understand the risks or costs of the current ungoverned approach
   - The business demanding service levels that are not possible within the allocated budget or technology
   - The business demanding system features and functionality that are not possible within the allocated budget or technology
5. If SharePoint is currently deployed, the current content stored in SharePoint should be reviewed. The comprehensive list should include who uses the content and what document retention schedules are in place.
6. A list of business initiatives that are considered “in scope” for the SharePoint deployment should be created. If SharePoint has already been deployed, the list should contain initiatives that are desired. The list should include the key stakeholders associated with each initiative. This is similar to COBIT control objective P01.4 *IT strategic plan* and can be mapped to SharePoint functionality. Typical examples include posting of standard financial information by the finance team, posting of expense and medical reimbursement form by human resources, or an announcement by the marketing department.
7. An operational review should be conducted. A representative sample from the upcoming book includes:
   - **Backup requirements**—A review of backup and recovery requirements and practices should be conducted for any existing or planned SharePoint initiatives. This activity begins building information required to meet COBIT process DS4 *Ensure continuous service*.
   - **Backup practices**—If SharePoint has been deployed, a review of backup practices for existing SharePoint deployments should be conducted. This activity also builds information required to meet DS4.1.
   - **Review of how costs are currently or will be allocated**—This activity includes an overview of how costs for SharePoint are or will be allocated to system users.
   - **Review of how change requests are managed**—This activity encompasses change request management including how requests are logged and how they are evaluated.
   - **Review of security requirements and security practices**—This activity includes a review of security requirements and how these

Continued on page 10

are implemented or planned to be implemented.

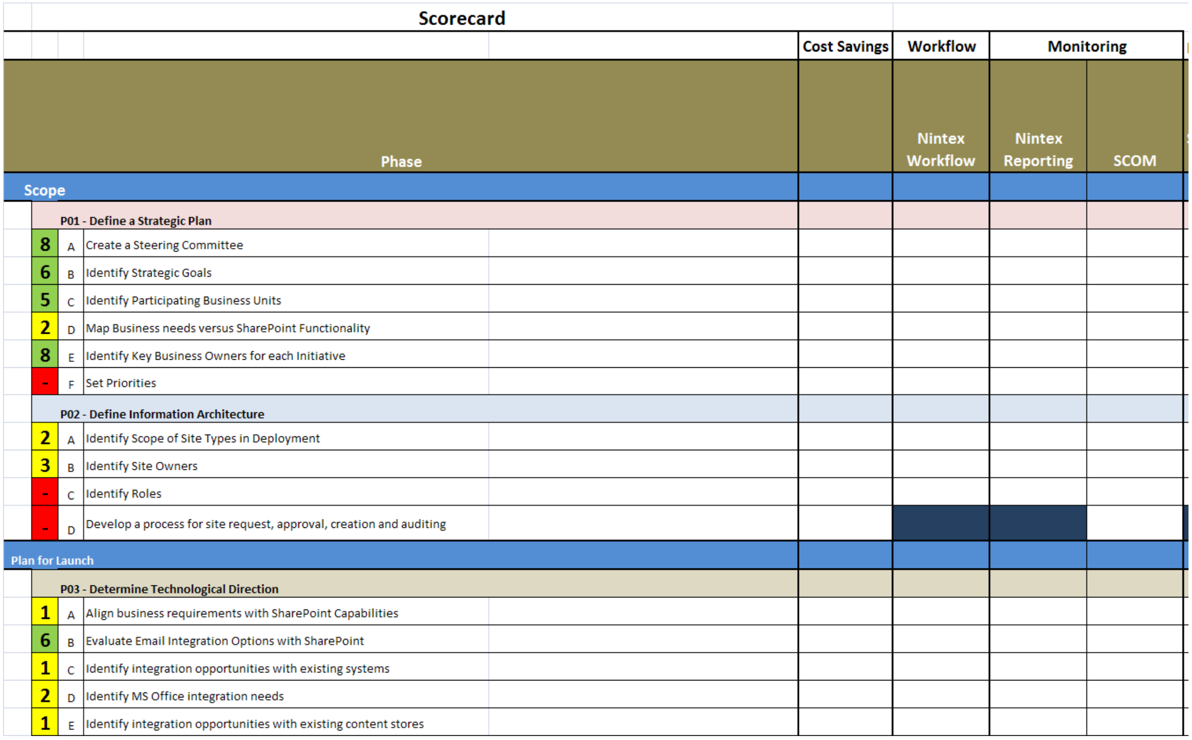
- **Review of training materials and plans**—This activity encompasses a review of training materials and training plans that are currently in place and planned.
- **Review of help desk processes**—This activity includes a review of the help desk capabilities and processes currently in place.

After the workshop, the following activities should be completed with IT leadership prior to a final follow-up meeting with the entire IT team:

1. **Findings and risk assessment review**—A review of the collected data should be summarized into a written report that identifies the maturity of the current SharePoint governance process and outlines the risks currently facing the organization. This report should be reviewed with the IT team to validate findings and agree upon readiness and desired next steps to implement SharePoint governance.
2. **Decision to proceed with governance initiative**—A frank discussion should be held with the IT leadership team to assess the organization's readiness to proceed with implementing governance for SharePoint. Any key impediments identified in the workshop should be evaluated and mitigated or compensated for prior to embarking upon the governance initiative. If the impediments are deemed significant enough to stop the governance framework, a plan should be devised to overcome each item prior to beginning.
3. **Preliminary scorecard**—If the decision to proceed with the governance initiative is approved, a preliminary effort to complete a scorecard should be undertaken. The scorecard should track governance progress and highlight areas requiring additional attention. A preliminary survey should be conducted to assess the current state of governance using the scorecard as a guide. A small sample of the scorecard from the upcoming book is shown in **figure 3**.
4. **Detailed scorecard**—A second detailed scorecard to assess the maturity of controls in the scorecard should also be completed. A sample detailed control scorecard is presented in **figure 4**.
5. **Plan**—A scope and timeline indicating which portions of the COBIT 4.1 framework will be adopted, including approach and timing, should be developed. The upcoming ISACA publication provides a clear road map that can be followed to meet the objectives of

Continued on page 11

Figure 3—Scorecard and Tools



Scorecard

			Cost Savings	Workflow	Monitoring	
		Phase		Nintex Workflow	Nintex Reporting	SCOM
Scope						
		P01 - Define a Strategic Plan				
8	A	Create a Steering Committee				
6	B	Identify Strategic Goals				
5	C	Identify Participating Business Units				
2	D	Map Business needs versus SharePoint Functionality				
8	E	Identify Key Business Owners for each Initiative				
-	F	Set Priorities				
		P02 - Define Information Architecture				
2	A	Identify Scope of Site Types in Deployment				
3	B	Identify Site Owners				
-	C	Identify Roles				
-	D	Develop a process for site request, approval, creation and auditing		■	■	
Plan for Launch						
		P03 - Determine Technological Direction				
1	A	Align business requirements with SharePoint Capabilities				
6	B	Evaluate Email Integration Options with SharePoint				
1	C	Identify integration opportunities with existing systems				
2	D	Identify MS Office integration needs				
1	E	Identify integration opportunities with existing content stores				

COBIT 4.1. This plan should be shared with the business units participating in the governance initiative to get their buy-in and input.

6. **Tools**—A review of tools required to govern SharePoint should be completed. A list of suggested tools mapped for each process and control is contained within the upcoming publication.
7. **Budget and plan**—A preliminary budget and plan should be developed so funds and resources required for the effort can be allocated.

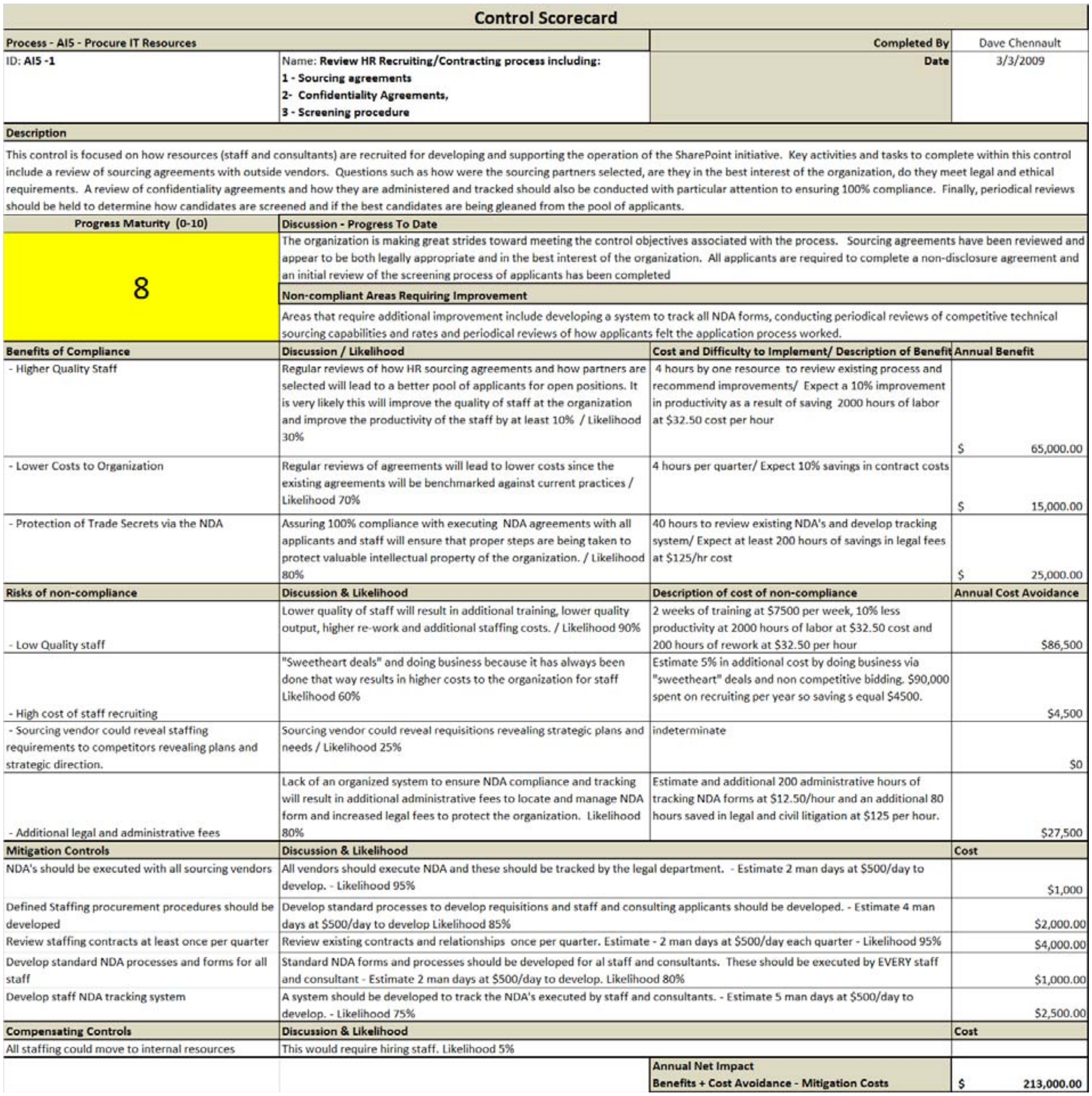
Once these activities have been completed, and if there are no significant impediments remaining, the organization is ready to begin the governance process in earnest. A meeting should be called with key business stakeholders and executives to review the SharePoint governance framework. Items to review should include key findings, such as business impact and associated risks and costs, of the current or proposed SharePoint deployment and plan.

Step Two—Meet With Key Business Stakeholders

After the initial survey with IT staff outlined in step

Continued on page 12

Figure 4—Detailed Control Review



Control Scorecard

Process - AI5 - Procure IT Resources		**Completed By**	Dave Chennault
ID: **AI5 -1**	Name: **Review HR Recruiting/Contracting process including:** **1 - Sourcing agreements** **2- Confidentiality Agreements,** **3 - Screening procedure**	**Date**	3/3/2009
Description			
This control is focused on how resources (staff and consultants) are recruited for developing and supporting the operation of the SharePoint initiative. Key activities and tasks to complete within this control include a review of sourcing agreements with outside vendors. Questions such as how were the sourcing partners selected, are they in the best interest of the organization, do they meet legal and ethical requirements. A review of confidentiality agreements and how they are administered and tracked should also be conducted with particular attention to ensuring 100% compliance. Finally, periodical reviews should be held to determine how candidates are screened and if the best candidates are being gleaned from the pool of applicants.			
Progress Maturity (0-10)	**Discussion - Progress To Date**		
8	The organization is making great strides toward meeting the control objectives associated with the process. Sourcing agreements have been reviewed and appear to be both legally appropriate and in the best interest of the organization. All applicants are required to complete a non-disclosure agreement and an initial review of the screening process of applicants has been completed		
	Non-compliant Areas Requiring Improvement		
	Areas that require additional improvement include developing a system to track all NDA forms, conducting periodical reviews of competitive technical sourcing capabilities and rates and periodical reviews of how applicants felt the application process worked.		
Benefits of Compliance	**Discussion / Likelihood**	**Cost and Difficulty to Implement/ Description of Benefit**	**Annual Benefit**
- Higher Quality Staff	Regular reviews of how HR sourcing agreements and how partners are selected will lead to a better pool of applicants for open positions. It is very likely this will improve the quality of staff at the organization and improve the productivity of the staff by at least 10% / Likelihood 30%	4 hours by one resource to review existing process and recommend improvements/ Expect a 10% improvement in productivity as a result of saving 2000 hours of labor at $32.50 cost per hour	$ 65,000.00
- Lower Costs to Organization	Regular reviews of agreements will lead to lower costs since the existing agreements will be benchmarked against current practices / Likelihood 70%	4 hours per quarter/ Expect 10% savings in contract costs	$ 15,000.00
- Protection of Trade Secrets via the NDA	Assuring 100% compliance with executing NDA agreements with all applicants and staff will ensure that proper steps are being taken to protect valuable intellectual property of the organization. / Likelihood 80%	40 hours to review existing NDA's and develop tracking system/ Expect at least 200 hours of savings in legal fees at $125/hr cost	$ 25,000.00
Risks of non-compliance	**Discussion & Likelihood**	**Description of cost of non-compliance**	**Annual Cost Avoidance**
- Low Quality staff	Lower quality of staff will result in additional training, lower quality output, higher re-work and additional staffing costs. / Likelihood 90%	2 weeks of training at $7500 per week, 10% less productivity at 2000 hours of labor at $32.50 cost and 200 hours of rework at $32.50 per hour	$86,500
- High cost of staff recruiting	"Sweetheart deals" and doing business because it has always been done that way results in higher costs to the organization for staff Likelihood 60%	Estimate 5% in additional cost by doing business via "sweetheart" deals and non competitive bidding. $90,000 spent on recruiting per year so saving s equal $4500.	$4,500
- Sourcing vendor could reveal staffing requirements to competitors revealing plans and strategic direction.	Sourcing vendor could reveal requisitions revealing strategic plans and needs / Likelihood 25%	indeterminate	$0
- Additional legal and administrative fees	Lack of an organized system to ensure NDA compliance and tracking will result in additional administrative fees to locate and manage NDA form and increased legal fees to protect the organization. Likelihood 80%	Estimate and additional 200 administrative hours of tracking NDA forms at $12.50/hour and an additional 80 hours saved in legal and civil litigation at $125 per hour.	$27,500
Mitigation Controls	**Discussion & Likelihood**		**Cost**
NDA's should be executed with all sourcing vendors	All vendors should execute NDA and these should be tracked by the legal department. - Estimate 2 man days at $500/day to develop. - Likelihood 95%		$1,000
Defined Staffing procurement procedures should be developed	Develop standard processes to develop requisitions and staff and consulting applicants should be developed. - Estimate 4 man days at $500/day to develop Likelihood 85%		$2,000.00
Review staffing contracts at least once per quarter	Review existing contracts and relationships once per quarter. Estimate - 2 man days at $500/day each quarter - Likelihood 95%		$4,000.00
Develop standard NDA processes and forms for all staff	Standard NDA forms and processes should be developed for al staff and consultants. These should be executed by EVERY staff and consultant - Estimate 2 man days at $500/day to develop. Likelihood 80%		$1,000.00
Develop staff NDA tracking system	A system should be developed to track the NDA's executed by staff and consultants. - Estimate 5 man days at $500/day to develop. - Likelihood 75%		$2,500.00
Compensating Controls	**Discussion & Likelihood**		**Cost**
All staffing could move to internal resources	This would require hiring staff. Likelihood 5%		
		Annual Net Impact **Benefits + Cost Avoidance - Mitigation Costs**	$ 213,000.00

one, key business stakeholders should be invited to a workshop to review findings and create the management team for the SharePoint governance initiative. The activities involved in this step include:

1. **Hold a workshop to review findings of the IT survey with key business stakeholders and to identify steering committee members**—Key business stakeholders and IT staff should be invited to the workshop by the SharePoint governance champion to review the findings outlined in step one. Candidates selected as key business stakeholders should be reviewed and added to a pool of prospects for the SharePoint governance steering committee. This begins to build the list of candidates required to satisfy one of the objectives of COBIT 4.1 process PO1 *Define a strategic IT plan*.
2. **Create a steering committee**—Once the candidates for the steering committee have been identified, the SharePoint governance champion should review the candidates and form a list of steering committee members. These candidates should be notified and given the opportunity to accept or decline an invitation to join the steering committee. A list of steering committee members should be compiled and a meeting should be set. This completes control objective P01.1 *IT value management*.
3. **Hold the initial steering committee meetings**—Once the team has been identified, initial meetings should be held to lead the governance initiative. Once these meetings have begun, the committee should be well on its way to establishing a formal governance process for SharePoint. Suggested sample agendas for the first three meetings can be found in the upcoming publication.

Step Three and Beyond

Once a functioning steering committee is in place, attention can be focused on satisfying the requirements of the processes and controls needed to govern SharePoint properly. The steering committee should review the scope of the governance initiative and reaffirm its commitment to these goals.

Next, a formal plan should be developed to guide the governance initiative. COBIT 4.1 should be used to frame the plan. Processes such as P01 *Define a strategic IT plan* and P02 *Define the information architecture* should be completed prior to the SharePoint deployment. These processes will likely be followed by P03 *Determine technological direction* and P04 *Define the IT process, organization and relationships*.

Conclusion

Microsoft SharePoint's appeal lies in its ability to empower end users with the ability to create and maintain their own site content, giving them the capability to produce and publish information internally or to the Internet. That power must be monitored and controlled to address the risks associated with unbridled collaboration possibilities.

Good governance is a must with SharePoint, and COBIT 4.1 provides an ideal framework for applying governance into the SharePoint domain. Given the demands on IT and the risks presented by SharePoint, it is never too late to start a SharePoint governance initiative.

Dave Chennault, MCP
specializes in SharePoint architecture, governance and deployment. He has more than 20 years of IT experience, developing and leading large software development and deployment efforts. His experience includes nearly 10 years as a software developer and more than 10 years of consulting as a senior manager with Deloitte Consulting, Coopers and Grant Thornton. He is cofounder of his own services firm, specializing in SharePoint deployment and cloud strategy and migration, with a special focus on BPOS (Microsoft's cloud offering). He can be reached at *Info@SPGovernance.com*.

Chuck Strain, CISA, MCSE, MCTS
specializes in project management and business process engineering. He has more than 25 years of IT experience in all phases of IT management and delivery. Strain's experience includes running his own IT business for 15 years, consulting services, and business planning and development services. He currently works for DynTek Services Inc. in Southern California, USA, and can be reached at *Info@SPGovernance.com*.

Editor's Note

SharePoint Deployment and Governance Using COBIT® 4.1: A Practical Approach is scheduled to be available in the fourth quarter in the ISACA Bookstore, *www.isaca.org/bookstore*.

Endnotes

[1] *http://technet.microsoft.com/en-us/office/sharepointserver/bb507202.aspx*

[2] The authors' efforts are the direct result of hard-learned lessons of SharePoint 2007 deployments.

COBIT as a Method for Deliberate and Emergent Strategies

By Werner Syndikus, CISA, CGEIT

A good, respectively successful IT governance program is characterized by an intensive business-IT alignment. Thus, COBIT, as a method of IT governance, must be judged as to whether it succeeds in establishing a strategic fit between business strategies and an IT strategy. Therefore, the question arises whether the kind of strategies that appear in practice are sufficiently supported by COBIT.

There are different approaches to classify strategies. The following article deals with the differentiation between deliberate and emergent strategies and their support when they are implemented with the COBIT framework. The development and the implementation of deliberate strategies (in the sense of planned measures packages) are relatively obvious to those who are regularly confronted with it in their daily routine. Emergent strategies, on the other hand, look different—the words "emergent" (in the sense of unintended) and "strategy" could cause a discrepancy.

The following article points out that the COBIT framework is very helpful when implementing both types of strategies. First, the synergy between COBIT and deliberate strategies will be demonstrated, then it is shown how COBIT supports emergent strategies.

In COBIT, the Plan and Organize (PO) domain is basically responsible for business-IT alignment. The structure of this domain is process-oriented and is based on the classical strategic understanding that is causing associations among terms such as "planning," "rationality" and "formal processes."

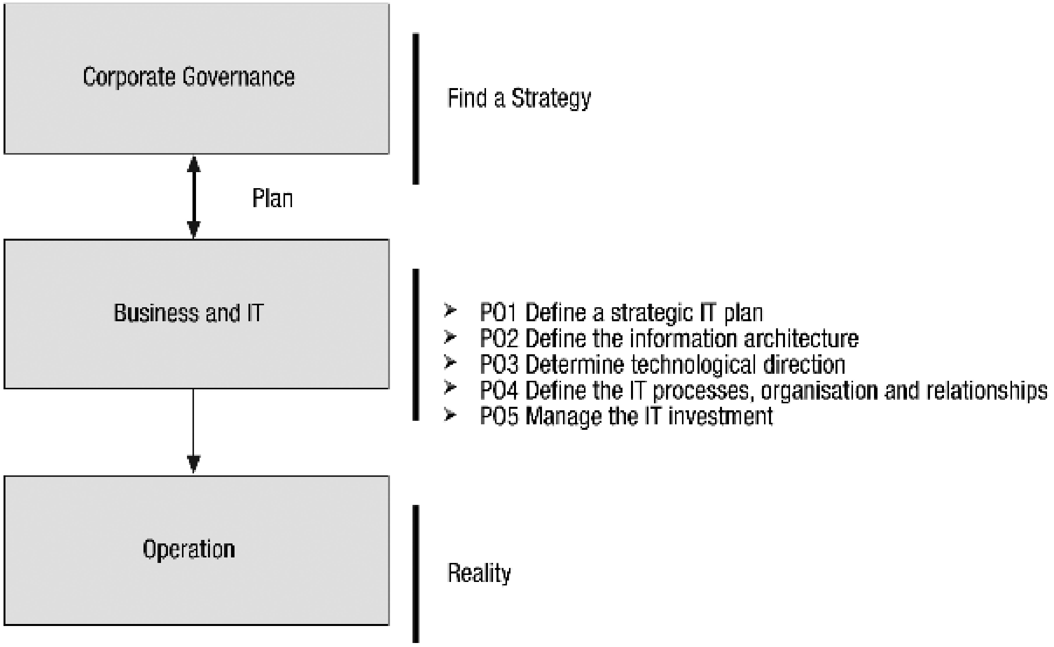
The term "deliberate strategies" can be defined by the following features, which are also features in COBIT:

- Planning and structuring of strategies as a top management task
- Influence of strategies on the allocation of the basis of resources
- Focusing of strategies on competitive edge
- Time pattern of the strategy term

The contents and the structure of COBIT (processes, controls, top-down approach) are very helpful when deliberate strategies are implemented both from the development to the operational implementation of strategies. The business requirements are generating the input for the strategic cluster with processes PO1, PO2,

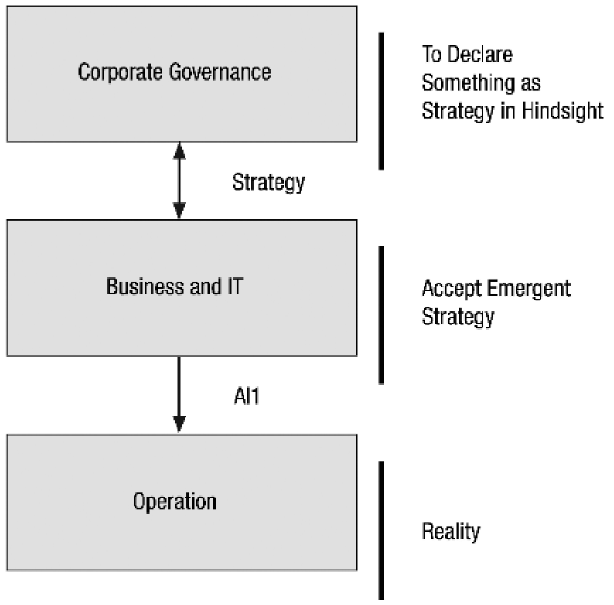
Continued on page 14

Figure 1—Development of Deliberate Strategies


Corporate Governance
Find a Strategy
Plan
Business and IT
PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine technological direction
PO4 Define the IT processes, organisation and relationships
PO5 Manage the IT investment
Operation
Reality

PO3 and PO4. The successful implementation of the PO5 process is an essential condition for current and future investments. The reason for the well-operating synergy between deliberate strategies and COBIT is because the procedural, formal and structured setup of COBIT corresponds to the character of deliberate strategies (see **figure 1**).

Figure 2—Development of Emergent Strategies



Consequently, the PO domain is completely in accordance with the concept of deliberate strategies.

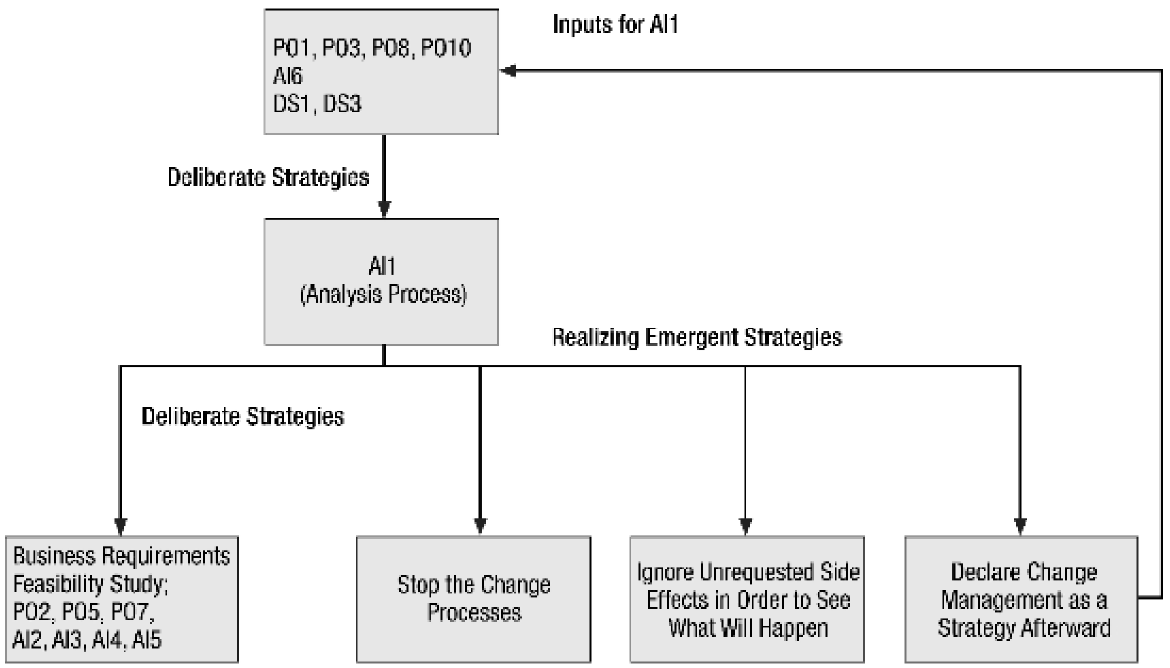
Not only in economic theory but also on the practical level, an alternative perspective for the term “strategy” is being encountered. As it concerns the unintended or so-called emergent strategies, operation comes before strategy. Strategy is understood as the “master pattern within the flow of decisions and operations.”[1]

Emergent strategies are characterized by the fact that they are not a result of a planning process, but are about single operation schemes that are self-developing during the ongoing business operations but later become a strategy (see **figure 2**).

COBIT does not offer an explicit reference to emergent strategies, but process AI1 *Identify*

Continued on page 15

Figure 3—Model for the Handling of Emergent Strategies


Inputs for AI1
PO1, PO3, PO8, PO10
AI6
DS1, DS3
Deliberate Strategies
AI1
(Analysis Process)
Realizing Emergent Strategies
Deliberate Strategies
Business Requirements Feasibility Study;
PO2, PO5, PO7,
AI2, AI3, AI4, AI5
Stop the Change Processes
Ignore Unrequested Side Effects in Order to See What Will Happen
Declare Change Management as a Strategy Afterward

automated solutions shows an inherent approach. The translating of business functional and control requirements into an effective and efficient design of automated solutions is in fact understood as the result of a tactical process, but is also responding to the possibility of identification of operational—not yet IT-supported—schemes and their conversion into automatic IT solutions.

Whereas the PO domain is intensely constrained to the top-down approach, even with the underlying coordination between IT and business, process Al1 can also be attributed to the bottom-up approach. Based on operational schemes, automated solutions will become strategies.

This emergent change can develop parallel to the planned strategies. Related to the AI1 process are analyses that deal with the implementation of the planned strategies, but, during these analyses, an already instated emergent change may be visible. Indicators for this change are frequently self-developed tools within the business departments (usually in the form of Microsoft Excel applications). Especially within sectored or decentralized organizations, approaches to a problem (even new organizational change processes) are resulting that will not be found in any deliberate strategy. By using the AI1 process, such developments can be recognized at an early stage and can be used accordingly. In these cases, the PO1 process is not the input for the AI1 process, but AI1 is providing the input for the business strategy and is consequently leading to the input of PO1.

Three action alternatives result after the emergent change has been recognized:

- To stop the change processes
- To ignore unrequested side effects in order to see what will happen
- To declare change management as a strategy

Figure 3 shows how the AI1 process can be used as a screening model to discover emergent strategies in time and to initiate corresponding alternatives. For this to be possible, it is necessary for the AI1 process to have already reached an adequate maturity level within the company. A clear and structured approach in determining IT solutions (COBIT maturity level 3, defined), should be a solid basis for the cognition of emergent strategies.

Conclusion

From the development to the implementation of deliberate strategies, COBIT is a good management approach for the business-IT alignment. This is because certain characteristics can be found in both approaches (e.g., top-down approach). With the above-mentioned screening model, COBIT also offers an approach for emergent strategies. More and more IT professionals are working in complex situations during which the early cognition of emergent strategies provides an important competitive advantage.

Werner Syndikus, CISA, CGEIT
has 25 years of experience in the IT business. He started as a system developer, became a manager of a business consultancy and is now the head of IT for a German logistics company.

Endnotes

[1] Mintzberg, Henry; Bruce Ahlstrand; Joseph Lampel; *Strategy Safari*, Redline Wirtschaft, 2007, p. 22-29

Identify, Govern and Manage IT Risk

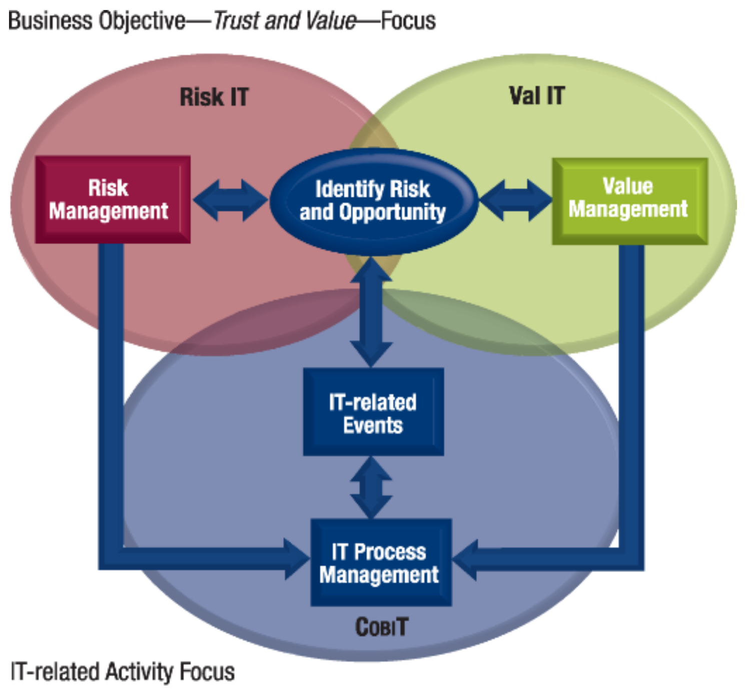
By Dirk Steuperaert, CISA

ISACA will publish shortly the first two publications in its Risk IT: Based on COBIT® framework: *The Risk IT Framework* and *The Risk IT Practitioner Guide*. The Risk IT framework complements ISACA's COBIT®, which provides a comprehensive framework for the control and governance of business-driven, IT-based solutions and services. While COBIT sets good practices for the means of risk management by providing a set of controls to mitigate IT risk, Risk IT sets good practices for the ends by providing a framework for enterprises to identify, govern and manage IT risk.

Figure 1 shows how ISACA's three major IT governance frameworks work together to provide comprehensive guidance on IT governance. COBIT describes IT processes, managing all IT-related activities within the enterprise. Internal and external IT-related events, e.g., operational IT incidents, project failures, full (IT) strategy

Continued on page 16

Figure 1—Positioning COBIT, Val IT and Risk IT


Business Objective—*Trust and Value*—Focus
Risk IT
Val IT
Risk Management
Identify Risk and Opportunity
Value Management
IT-related Events
IT Process Management
COBIT
IT-related Activity Focus

switches, mergers, changes in market conditions, new competitors, availability of new technology and new regulations affecting IT, interfere with IT. These events pose risk and/or opportunity that need to be assessed. The risk dimension and how to manage it are the main subjects of the Risk IT framework. When opportunities for IT-enabled business change are identified, the Val IT framework describes best how to progress and maximise the return on investment. The outcome of the assessment will feed back into the IT processes.

IT risk is business risk—specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives. IT risk can be categorised in different ways:

- IT benefit/value enablement risk, associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes, or to use technology as an enabler for new business initiatives
- IT programme and project delivery risk, associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programmes. This ties to investment portfolio management.
- IT operations and service delivery risk, associated with the performance and availability of IT systems and services, and can bring destruction or reduction of value to the enterprise

It is important to realise that IT risk always exists, whether or not it is detected or recognised by an enterprise.

Risk IT is aimed at a wide audience, as risk management is an all-encompassing and strategic requirement in any enterprise. The target audience includes:

- Top executives and boards who need to set direction and monitor risk at the enterprise level
- Managers of IT and business departments who need to define risk management processes
- Risk management professionals who need specific IT risk guidance
- External stakeholders

Applying good IT risk management practices as described in *The Risk IT Framework* will provide tangible business benefits, e.g., fewer operational surprises and failures, increased information quality, greater stakeholder confidence and reduced regulatory concerns, innovative applications supporting new business initiatives, and many more.

Risk IT is based on the principles of numerous enterprise risk management standards/ frameworks, such as COSO ERM[1] and AS/NZS 4360[2] (soon to be complemented or replaced by ISO 31000), and provides guidance on how to apply these principles to IT. Risk IT differs from existing IT risk guidance documents that focus solely on IT security (or other detailed focus areas in IT) in that Risk IT covers all aspects of IT risk.

Risk IT contains two volumes:

1. ***The Risk IT Framework***—Contains the guiding principles for IT risk management, based on generally accepted standards. Based on these principles, a detailed and comprehensive process model is built. This model includes three domains, each containing three processes. The processes are structured much as in ISACA's COBIT and Val IT frameworks, and they contain ample materials to define, implement, optimise and manage the processes.

Continued on page 17

2. ***The Risk IT Practitioner Guide***—Contains comprehensive practical guidance on how to manage IT risk. The book is divided into eight chapters and discusses topics such as defining a risk universe, how to define risk appetite, how to describe risk, how to develop relevant risk scenarios, how to respond to risk, and how COBIT and Val IT can assist in mitigating risk. The guide contains several templates, as well as a comprehensive list of generic IT risk scenarios.

Like COBIT and Val IT, Risk IT is not a standard but a framework, including a process model and good practice guidance. This means that enterprises can and should customise the components provided in the framework to suit their particular enterprise and context.

Dirk Steuperaert, CISA

is currently running his own consulting company, IT In Balance, providing IT governance-related services. Previously, he was a director at PricewaterhouseCoopers in Belgium, responsible for IT governance services. During the early years of his career, Steuperaert gained IT and IT audit expertise at SWIFT and ING Belgium. He was also a member of the COBIT Steering Committee (CSC) from 2006-2008. Steuperaert provided consulting support to ISACA as project manager of the development team for the new Risk IT framework and is currently performing a similar role for the new COBIT® 5.0 research initiative.

Editor's Note

For more information on Risk IT: Based on COBIT, please visit *www.isaca.org/riskit*. The initial publications will be available in the ISACA Bookstore, *www.isaca.org/bookstore*. *The Risk IT Framework* will be available as a complimentary PDF for ISACA members and nonmembers at *www.isaca.org/downloads*. *The Risk IT Practitioner Guide* and tool kit will be available as complimentary downloads for ISACA members at *www.isaca.org/downloads*.

Endnotes

[1] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management—Integrated Framework*, 2004, *www.coso.org*

[2] Standards Australia, *Australian/New Zealand Standard for Risk Management*, 2004, *www.saiglobal.com*

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

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.