COBIT® Focus
Using COBIT, Val IT, Risk IT, BMIS and ITAF
Volume 2, April 2012

In This Issue:

- COBIT 5 Is Here
- Using COBIT to Aid in Hospital Risk Management, Part 2
- COBIT 5—GEIT Upgrade Guidance
- IT Risk Is Business Risk
- Between Fear and Greed, IT Value Is Losing Out!

COBIT 5 Is Here

The much-anticipated COBIT 5 framework is available!

"COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use."[1]

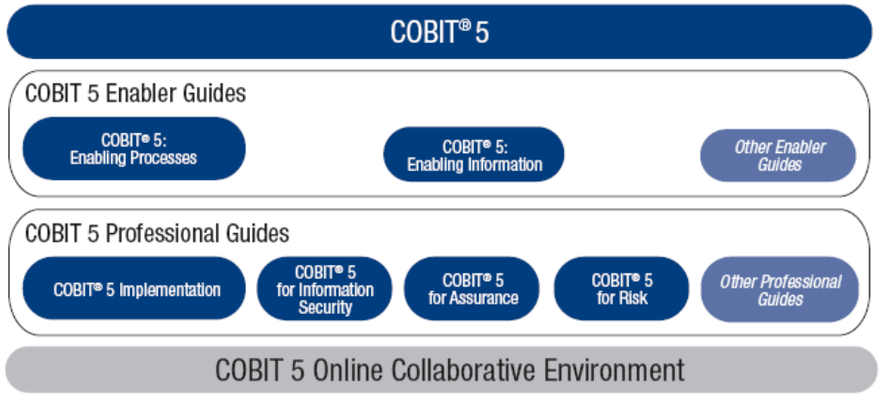
The COBIT 5 publication provides the overall guidance, comprising the five principles and seven enablers that make up this framework, for the governance and management of enterprise IT (GEIT) assets.

The initial launch includes three products:

- **COBIT 5**—The framework
- ***COBIT 5: Enabling Processes***—Expanded guidance on processes from a COBIT 5 perspective, including an illustrative process reference model with 37 processes
- ***COBIT 5 Implementation***—An implementation guide based on COBIT 5

Additional products (see **figure 1**) focusing on specific professional needs (information security, IT assurance and IT risk), COBIT enablers (information) and other topics are

Figure 1—COBIT 5 Product Family



Call for Articles

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

Submit articles on your experiences with these frameworks. Deadline to submit copy for volume 3, 2012: 1 June 2012

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

Case Studies

Visit the ISACA **Case Studies** page to read more.

planned and undergoing development to support the use of COBIT 5.

Visit the **COBIT 5** page for more information and to download the available publications today.

Endnotes

[1] ISACA, COBIT 5, "Executive Summary," USA, 2012, **www.isaca.org/cobit**

Come join the discussion! Masatoshi Kajimoto will be responding to questions in the **discussion area of the COBIT (4.1 and earlier)—Use It Effectively** topic beginning 23 April 2012.

Using COBIT to Aid in Hospital Risk Management, Part 2

By Masatoshi Kajimoto, CISA, CRISC

The author's first article "**Using COBIT to Aid in Hospital Risk Management**," (*COBIT Focus* volume 1, 2012) ended at the starting point of the system integration. This article picks up where the first left off. Next, the organization needed to clearly distinguish clinical and IT risk management subjects/objectives, define appropriate system requirements and new business processes, clearly identify performance indices, and establish appropriate new business and IT management/control processes.

To perform these tasks, the organization established the following hospital information systems (HIS) integration teams:

1. **Decision-making steering committee**—Members of this committee included top management people and the team leaders of the other teams.
2. **System integration and business process reengineering (BPR) promotion team**—Group leaders and subleaders were added to this team. These working groups completed the design and implementation of new business processes based on the new IT environment. As a consultant for this project, the author provided model HIS requirement specifications and typical HIS functions and process flow diagrams for their discussions. Under this team, the following working groups were established:
   - Doctor working process innovation working group
   - Nurse working process innovation working group
   - Ward working process innovation working group
   - Medical matter (e.g., accounting) process innovation working group
3. **System integration control team**—Team leaders and subleaders were members of this team. This team controlled the following groups:
   - Internal system division
   - System development vendor

Distinction Between Clinical and IT Risk Management Subjects/Objectives

Risk management subjects/objectives, which were described in a mixture state in the previous article, now needed to be distinguished. Then, the parties (e.g., doctors, nurses, medical staff, IT department staff) responsible for risk management at the point at which their roles come into play (e.g., planning phase, design phase, development phase, implementation phase, operation phase) had to be identified.

Why Was COBIT Used?

The hospital's risk management maturity level was at level 1, *ad hoc*. In almost all cases, the hospital and its staff reacted to incidents in firefighting risk-response manner. While they realized the importance of IT risk management, their management style was not planned.

Establishment of appropriate, well-organized, effective and efficient risk management was a critical issue for the hospital, because its HIS are very complicated and critical to its operation. The hospital staff was short on time and lacking knowledge of risk management; therefore, it needed to quickly understand the necessities for the establishment of IT risk management.

As a result, COBIT 4.1 was chosen and proved very useful when considering which IT-related risk management/controls to establish for this hospital within the limited time span. The hospital's team examined COBIT carefully to identify what to do to establish appropriate IT-related risk management.

COBIT as the Reference Material (From a Risk Management Point of View)

Of course, as described in the author's previous *COBIT Focus* article, the COBIT 4.1 process PO1: *Define a strategic IT plan* was very important, as the hospital addressed business-IT alignment (PO1.1). The following describes the other important COBIT 4.1 processes that the hospital implemented for IT-related risk management, broken up by each phase.

Planning Phase

1. PO6 *Communicate management aims and direction*—Definition of the elements of the control environment for IT alignment with the hospital's management philosophy and operation styles, as described in PO6.1. PO6.2 *Enterprise IT risk and control framework*, PO6.3 *IT policies management*, PO6.4 *Policy, standard and procedures rollout* and PO6.5 *Communication of IT objectives and direction* must be considered. Until now, communication among doctors, nurses, medical clerks and top management was not strong. There were no official meetings among the groups. With the implementation of the HIS project, official meetings among these groups became regular, improving the lines of communication.
2. PO7 *Manage IT human resources*—This project involved the implementation of completely new systems; therefore, human resources (HR) management was very important, especially PO7.3 *Staffing of roles*, as many new roles and responsibilities were defined and, thus, new role assignment was essential. For example, new medicines, new medical treatments and new clinical passes are continually coming out; therefore, evaluation of these and the updating of dictionaries in the HIS were important new roles. Insurance points are also frequently updated, thus updating the table of medical care treatment fees in the system is important. With *PO7.4 Personnel training,* an IT-security-related training program and awareness were important, and PO 7.5 *Dependence upon individuals* was key. Patient case records are delicate personal information; therefore, all staff must understand and be aware of the importance of data security. If patient case-record data are breached, the hospital could lose the trust of the community, in addition to the potential financial losses of a lawsuit.
3. PO9 *Assess and manage IT risks*—As a matter of course, these control objectives were the key. PO9.1 *IT risk management framework*, PO9.2 *Establishment of risk context*, PO9.3 *Event identification*, PO9.4 *Risk assessment*, PO9.5 *Risk response* and PO 9.6 *Maintenance and monitoring of a risk action plan* were indispensable. Project members realized the importance of a risk management framework and processes. As a result, they designed the processes and started preparation for the implementation. They also established the organization for risk management for medical, finance and IT.
4. PO10 *Manage projects*—PO10.9 *Project risk management* must not be forgotten. PO10.11 *Project change control* and PO10.13 *Project performance measurement, reporting and monitoring* are necessary. Schedule, cost, quality and risk criteria were key. For example, the cutover date was strictly defined by top management, so project delay was not permitted. For cost savings, system utilization processes (business processes) were standardized and simplified, so redundant customizations were avoided. To attain high-quality and high-level risk criteria, all hospital staff were involved and prototyping was repeated.

Design and Development Phase

1. AI1 *Identify automated solutions*—AI1.2 *Risk analysis report* was an important risk management resource. To establish, many indices for risk management status

COBIT 4.1 Controls Collaboration Community

ISACA has recently launched the COBIT 4.1 Controls Collaboration Community in the Knowledge Center. The new discussion groups provide COBIT 4.1 users the opportunity to:

- Exchange knowledge about specific control objectives and good practices
- Learn how COBIT 4.1 control objectives and related practices apply to specific situations across different industries, geographic locations or technologies
- Enhance the benefits gained from using COBIT 4.1

Help the ISACA community grow by sharing your thoughts, experiences and knowledge specific to COBIT 4.1 control objectives and related control practices.

Join now and be one of the first to interact with your fellow COBIT 4.1 users!

If you have begun or are planning the transition to COBIT 5, please join the **COBIT 5—Implementation** (members only) or **COBIT 5—Use It Effectively** (members and registered users) discussions in the Knowledge Center.

analysis were identified and organized, appropriate quantitative levels were assigned to indices, and personnel were assigned to measure these indices.
2. AI4 *Enable operation and use*—This is important to ensure that all related people can operate and utilize the new system. Therefore, from the earliest stage of this project, keyboard training software was provided to those who were less familiar with using computers. And, many rehearsals were repeated to verify the system and identify new problems.
3. AI7 *Install and accredit solutions and changes*—It was a difficult time as the cutover date approached. Without preparation in line with AI7.1 through AI7.9, on-time cutover may not have been possible. Within a certain period from the cutover, many troubles were expected to occur. Therefore, the preparation of many backup measures and repeated trouble response trainings at this stage were critical.

Operation Phase

1. DS1 *Define and manage service levels*—DS1.1 *Service level management framework* is operating within the hospital. No outsourcing was utilized. Based on this fact, a framework was established. For example, a very high service level must be assured for clinical purpose systems. DS1.2 *Definition of services*, 24 hours per day, 365 days per year is matter of course for clinical purposes, but this is not the case for medical staff. According to business characteristics, a service-level framework must be defined. DS1.5 *Monitoring and reporting of service level achievements*, for continuous improvement, is indispensable.
2. DS3 *Manage performance and capacity*—All control objectives (DS3.1 to DS3.5) in this process were necessary. System slowdown, for example, is not allowed for critical clinical systems. Therefore, many backup systems were prepared and tested.
3. DS4 *Ensure continuous service*—This is a matter of course for HIS. Many trouble cases, disasters and so on were identified and responses were discussed and determined.
4. DS5 *Ensure systems security*—Of course, patient data are critical and, as such, very high-level security environments must be ensured. Utilizing PO7, high-level information security environments were established, and continuous monitoring and evaluation were put in place.
5. DS7 *Educate and train users*—Doctors must utilize personal computers (PCs). If they do not, they cannot spare enough time for patients and mistakes will occur. Continuous training is very important. After the medical examination time, doctors were trained to utilize new systems efficiently.
6. DS11 *Manage data*—Same as DS5, this is a matter of course. Very high-level data management was put in place. As already mentioned, new medicines and new medical treatments are continuously being developed. Keeping dictionaries up to date is necessary. Data backup and protection procedures were defined and put into practice.
7. DS12 *Manage the physical environment*—DS12.2 *Physical security measures* and DS12.3 *Physical access* are important. The number of terminals and IT-related devices was drastically increased. Also, the number of servers was increased. Terminal custody places were newly installed, and personnel were assigned responsibility for these places. Also, the environments of the server rooms were examined and enforced.

Identification of Performance/Monitoring Indices

New business and IT processes must be appropriately measured and monitored. The following high-level indices were set for each balanced scorecard (BSC) area, utilizing the COBIT ME1 processes. The following were categorized according to the BSC areas, so they can be used for reporting to the hospital executives (ME1.5). By these indices, IT performance is monitored and evaluated (ME1.1, ME1.3 and ME1.4). Therefore, top management can grasp the current hospital status in a timely manner and decide next steps (ME1.6).

1. High-level indices:
    - Top-management-vision-related:

Research Update

COBIT 5 Publications

The following are available on the **COBIT 5** page of the ISACA web site.

First COBIT 5 releases:

- COBIT 5 (framework)
- *COBIT 5: Enabling Processes*
- *COBIT 5 Implementation*

New PowerPoint presentations and COBIT 5 supporting material:

- COBIT 5 Executive Summary
- COBIT 5 Introduction
- Comparing COBIT 4.1 and COBIT 5
- COBIT 5 Tool Kit (self-assessment, measurement and diagnostic tools; presentations; related articles and further explanations), which supports *COBIT 5 Implementation* activities
- COBIT 5 Laminate PDF

Additional initiatives in development:

- *COBIT 5: Enabling Information*
- *COBIT 5 for Information Security*
- *COBIT 5 for Assurance*
- *COBIT 5 for Risk*
- COBIT 5 Online Collaborative Environment
- COBIT 5 Training (foundation, implementation and assessment level)

- Security level of personal information data protection
- Raising and keeping a high level of medical services
- Minimizing medical mistakes (malpractices)
- Rapid response to medical needs of the community
- Information sharing between the hospital and the community
- Raising staff's skills and knowledge
- Searching for new chances of challenge

- Mission-statement-related:
  - Cooperation between each facility within the group (systems and information)
  - Total supporting system of health care, treatments and nursing care
  - Establishing good supporting systems and then developing the doctors' research activities environment, and returning results of research activities to health care site

2. Customer-satisfaction-related indices:
   - Improvement of level of patient satisfaction:
     - Percentage of medical treatment reservations
     - Waiting time for medical examination
     - Average treatment periods (classified by disease)
     - Satisfaction level of provided information
     - Increasing use of consultation from patients
     - Satisfaction level resulting from consultation
     - Percentage of informed-consent executions
   - Improvement of cooperation level among hospitals and clinics in same community (medical care zone):
     - Ratio of patients with a letter of referral from clinics within the same medical care zone
     - Ratio of patients transferred to clinics in the same medical care zone (patients who can receive medical care from clinics near their home)
     - Quickness of response to patients who transferred clinics
     - Satisfaction level of cooperating clinics
     - Utilization rate of high-level medical equipment with cooperating clinics
     - Increasing ratio of trusted medical tests
   - Improvement of the local government's satisfaction:
     - Adoption rate of the local government's Community Medical Program
     - Acceptance of ambulances at the hospital
     - Acceptance of emergency patients (admission to the hospital)
   - Improvement of the general public's satisfaction:
     - Patients from outside of the secondary medical care zone
     - Satisfaction level of people living in the medical care zone
3. Finance-related indices:
   - Growth:
     - Rate and number of omissions of a request to the health insurance society for remuneration for medical treatments (hereafter referred to as "request")
     - Ratio of request denials
     - Delay and delayed amount of the request
     - Accuracy of correspondence between medical treatments and a request
     - Status of profit (classified by medical divisions and other divisions)
   - Profitability:
     - Billing amount and cost (classified by patients, disease and day)
     - Ratio of cost of medicines
     - Procurement cost and billing amount of medicines
     - Procurement cost and ratio of medical supplies
     - Bed utilization ratio (classified by medical division)
   - Liquidity:
     - Recovery rate of uncollected income
     - Effective utilization of lease
     - Ratio of fixed asset
     - Stock turnover

    - Squeezed dead stock
  - Stability:
    - Ratio of personnel expenses (e.g., reduction of messengers, medical clerical workers)
    - Utilization of outsourcing
    - Ratio of fixed cost
4. Internal-process-related indices:
  - Improvement of the quality of medical services:
    - Applied ratio of clinical paths
    - Ratio of patients who are applied to a clinical path
    - Result of variance analysis
    - Average hospital stay in days (classified by disease)
    - Number of papers and presentations by doctors; number of quoted papers of doctors
    - Number of surgeries
    - Substantial nursing status
    - Ratio of special region professional nurses
    - Ratio of planned admission and departures
  - Medical risk management:
    - Incidence of medical mistakes (e.g., errors, malpractices)
    - Incidence of hospital infections
    - Incidence of bed sores
    - Rate of carried-out instruction on medical management
    - Rate of providing information about side effects
  - Improvement of business process:
    - Reduction ratio of volume of hospital business processes
    - Ratio of automated business processes of mechanical processes
    - Ratio of automated business processes of standardized processes
    - Ratio of professional processes that are supported by systems
  - Utilization of information:
    - Ratio of expansion and utilization of shared information and knowledge
    - Ratio of PC capacity utilization
    - Status of end-user computing (EUC) utilization
5. Learning- and growth-related indices:
  - Improvement of professionalism of staff:
    - Expansion status of intellectual properties and professional knowledge within the hospital
    - Status of electronically gathered new knowledge and its utilization
    - Status of information literacy of staff
  - Optimization of roles and responsibilities:
    - Substantial information support for decision-making processes
    - Improvement of transparency of decision-making processes
    - Matching status of organizational roles and responsibilities assignment and access authorization assignment of information systems
    - Status of information security environment
  - Becoming an always-learning organization:
    - Utilization status of intellectual properties and professional knowledge
    - Substantial staff education and training programs and participation status
    - Updated and expanding status of knowledge-sharing systems

Consideration of Regulatory Aspect

Regulations are constantly being updated and new ones are coming out. Therefore, flexibility and quick response are very important. For example, the following are current big issues:

- Response to Diagnosis Procedure Combination (DPC) (Japanese regulatory issue) (similar to Diagnosis Related Group/Prospective Payment System [DRG/PPS])—To appropriately adopt this, detailed cost analysis functions were integrated into the HIS. They enabled the cost tracking of each patient and each disease.
- Regional general hospital coordinating community health care—Information exchanges with the hospital and many clinics in the same medical care zone are very important. As a result, patient case record data protections are a critically important issue.

- Introduction of electronic itemized statement of medical expenses (hospital to medical insurance)—Interface of these functions is defined by the Japan Ministry of Healthcare, Labor and Welfare (MLHW). Therefore, quick and accurate response is required.

To appropriately respond to these, controls related to ME3 *Ensure compliance with external requirements* are essential. To comply with many new regulatory requirements, management must keep abreast of regulations (mainly MLHW). To comply with such regulations, updating or renewal of HIS is critical. Sometimes, external audits for the medical care records and related process are required by MLHW. Therefore, hospitals must be prepared for the external audits.

Application Controls

As described in COBIT 4.1, application controls are also important for appropriate risk management. Appropriate IT audit should be in place as follows:

1. AC1 *Source data preparation and authentication*—Patient records are very critical. Predicated on a need-to-know, need-to-do basis, data preparation is authorized to appropriate personnel. Access rights are carefully categorized (for doctors, nurses and medical staff), and IDs and passwords are assigned to them. Updates to access rights are done via links with HR management.
2. AC2 *Source data collection and entry*—Decisions about medical care for patients are permitted only by doctors. All other personnel are prohibited from inputting or updating patient case records. All updates for patient case records are recorded and protected from deletion. Also, all access logs are recorded and examined periodically.
3. AC3 *Accuracy, completeness and authenticity checks*—Expert medical matter staff members are always checking this based on their knowledge and experience. For example, the auditing of patient case records is ordered by law. With patient case records now in the HIS, the role of the IT auditor becomes very important.
4. AC5 *Output review, reconciliation and error handling*—For example, the accuracy of the request to the health insurance society for remuneration for medical treatments directly impacts financial liquidity. Calculations of medical treatment fees for patients are now done automatically, so the burden on medical clerks is lessened—they can now concentrate on checking the accuracy of the requests to the health insurance society.

Conclusion

COBIT 4.1 proved extremely useful for the establishment of IT-related risk management/control.[1]

IT goals must be connected to business goals, and IT output cannot automatically become outcomes. Therefore, continuous monitoring and evaluation from a business point of view is necessary. The baseline of the IT-related risk management of this hospital was established; however, issues remain that require continuous improvement. For example, medical institutions' specific IT-related risk has not been completely identified. Therefore, continuous improvement of the risk management system is indispensable. Rapidly and frequently, new medicines, new medical treatments and new regulations are coming out, requiring constant risk management.

Author's Note

I think there is always uncertainty relating to risk management. We can try to list what will happen, but we cannot predict correctly when, how, to what level, where, etc. And, when reality strikes, "strength" may be "weakness," "opportunity" may be "threat," and *vice versa*. After the 11 March 2011 disaster in Japan, the hospital is updating its business continuity planning (BCP), business continuity management and disaster recovery. In many cases, the traditional approach of BCP would and did not apply. Following DS4 *Ensure continuous service*, the hospital's staff is now updating its BCP. In DS4, continuity is strongly emphasized, describing what to do to establish an efficient and effective IT continuity plan. With this in place, the hospital staff now recognizes what will happen in the event of a huge disaster, and as a result, staff will be able to easily establish new IT continuity plans.

Masatoshi Kajimoto, CISA, CRISC

Is an IT auditor and independent consultant providing services in business process reengineering (BPR), human resources management, IT governance and IT-related risk management for educational, medical and financial institutions. He currently serves as technical advisor for the Ministry of Internal Affairs & Communications (Japanese government). He is a director of the ISACA Tokyo Chapter and is a cofounder and executive director of ITGI Japan. He also serves on ISACA's Government and Regulatory Advocacy (GRA) Subcommittee Area 1 and is a member of the GRA Committee.

Endnote

[1] To respond to the need for a risk management framework, ISACA developed Risk IT, which is based on COBIT. However, this project began prior to the release of Risk IT; therefore, the hospital developed its own risk management framework based on COBIT. Risk IT is now incorporated in COBIT 5.

COBIT 5—GEIT Upgrade Guidance

By Jimmy Heschl, CISA, CISM, CGEIT

Whenever a new version of something arrives, IT questions arise, for example: Should we upgrade at all? When should we upgrade? What are the resources required? Who will be driving the upgrade?

Governance of enterprise IT (GEIT) is an integral part of enterprise governance and addresses the definition and implementation of processes, structures and relational mechanisms in the organisations that enable both business and IT personnel to execute their responsibilities in support of business-IT alignment and the creation of business value from IT-enabled investments.

COBIT 4.0, in 2005, included the five IT governance focus areas introduced by ISACA in the *Board Briefing on IT Governance, 2nd Edition*, published in 2003, with the addition of a need for attention towards framework establishment and use. ISACA has now released COBIT 5, which further expands on the governance aspects within the framework.

The first thing to consider is the current situation of the enterprise. Even though common patterns throughout different enterprises are recognisable (e.g., highly regulated and audited companies, technology-driven start-ups, enterprises relying on legacy IT), each organisation is different and—as the people within them—needs to be treated differently. Another driver is the direction the enterprise follows and its velocity. Some companies are slower than others.

Answering the upgrade questions posed here is as easy as just combining those two aspects—the current and the future (or intended) state—applying a sound methodology to move from today (or yesterday) to tomorrow, or just being fit for upcoming challenges.

COBIT 5 Implementation

The COBIT 5 family of products includes an implementation guide, *COBIT 5 Implementation*, to help enterprises effectively adopt and adapt COBIT to suit the enterprise's unique environment and business goals. This guidance helps to avoid commonly encountered pitfalls and to leverage good practices and assist in the creation of a successful outcome. The guide comes with an implementation tool kit that contains resources for measurement and diagnostics of an organisation's status, presentations, and further explanations.

The implementation guide provides a solution to manage the complexity of implementation initiatives by clearly separating three components of the life cycle: the management of the programme, the enablement of change and the core improvement initiatives. These three layers of the cycle are separated into seven phases of activity:

1. What are the drivers?
2. Where are we now?
3. Where do we want to be?
4. What needs to be done?
5. How do we get there?
6. Did we get there?
7. How do we keep the momentum going?

Applying the methodology within the implementation guide will reduce the need for external support and enable the enterprise in the implementation of good practice for GEIT. Considering that the exercise is not a project where external impulse and support are beneficial, but is a continual improvement and alignment process, it is necessary to have a dedicated internal owner of this process. One of the key success factors is to have top management providing the direction. Enterprise governance should rely on senior management to evaluate, direct and monitor (EDM) the enterprise IT needs and arrangements, ensuring that they are in alignment with the organisation's goals and governing principles and practices.

One of COBIT 5's principles is to recognise the separation of GEIT assets. This is probably one of the most challenging aspects of implementing COBIT 5: getting the governing bodies to account for IT by setting the direction, based on sound evaluation, and to apply continuous monitoring of enterprise IT. This should not be a staff function within an IT department or even outsourced to a third party. This key area needs to be part of the usual governance of the enterprise and not a separate exercise. Managing IT—in COBIT terminology the planning, building, running and monitoring (PBRM) of IT—can be separated and accounted for by an IT function, a business unit or an outsourced service provider, as appropriate.

Why will it be hard to separate governance and management? There are two main reasons: IT organisations have the tendency to assume ownership of GEIT and are likely to resist passing on this accountability. On the other hand, all IT matters are—from top management and business management perspectives—often passed to IT (in whole or in part). Thus, there are two parts of the enterprise likely to resist this change.

However, enterprises that have made the shift report significant benefits such as transparency over IT; higher reliability on the delivery of business projects (also referred to as IT-enabled business initiatives) in time, cost and quality; reduced level of risk from a strategic, delivery and operational perspective; and, of course, the ability to demonstrate the quality of IT controls to internal and external auditors. Enterprises with superior governance over IT had at least a 20 percent higher profitability than firms with poor governance, given the same objectives.[1] Increasing the profitability by 20 percent: is this not a good argument to implement GEIT?

New Perspectives

COBIT 5 combines all of the key building blocks of GEIT, rather than focus only on the processes involved. All significant enablers, such as principles, policies and frameworks; processes; organisational structures; culture, ethics and behaviour; information; services, infrastructure, and applications; and people, skills and competencies, are addressed in COBIT 5. This will serve as valuable input to further improve the current state and to provide a complete picture to steer the continual improvement process for GEIT. Based on stakeholder needs, the required enabler performance requirements can be identified and—where required—improved and aligned to meet stakeholder needs.

Migration

If the organisation's set of general IT controls on access control, change management and other core IT tasks is based on previous versions of COBIT, renumbering those controls and control activities might be nice to ease the work of auditors. A table mapping the COBIT 4.1 control objectives to the COBIT 5 governance and management practices is included in the *COBIT 5: Enabling Processes* publication (appendix A). If these areas are not under full control already, the organisation has bigger issues than just the implementation of COBIT. And, if it implements COBIT 5 just to meet auditors' needs, there are probably more beneficial opportunities to use the resources available.

A key strength of COBIT 5 is to combine and steer the use of IT-focused frameworks, good practices and standards, such as ITIL V3 2011, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 Series and Capability Maturity Model Integration (CMMI). COBIT 5 is the integrating framework. Whatever the enterprise is using, it can be integrated with COBIT 5 and there are likely some good practices in the framework that are worth being considered and adopted as part of the ongoing improvement process. *It is not a question of version numbers; it is, rather, a question of the fulfilment of stakeholder needs.* These needs do in fact exist, explicitly or implicitly. Organisations should be prepared to meet the upcoming challenges.

Timing

Implementing GEIT is not rocket science. The key challenge is to start. And, just as with anything one does to improve one's life (such as a diet or quitting smoking), the organisation should begin today. There is no reason to postpone it until next year.

When travelling and having the good fortune of being offered a free upgrade to the next higher class, do you hesitate? I would think not. Why wait any longer and stick with COBIT 4.1 or COBIT 3rd Edition, Risk IT, Val IT or other IT-focused frameworks, such as ITIL and ISO/IEC standards? Now is the time to upgrade!

Conference Update

COBIT 5 at North America CACS

Want to learn more about COBIT 5? ISACA's North America Computer Audit, Control and Security℠ (CACS℠) conference is the perfect opportunity. Consider attending the following sessions, among others, in Orlando, Florida, USA, on 7-10 May 2012.

Monday, 7 May
8:30 a.m.—Welcome Address presents COBIT 5
5:15-6:15 p.m.—Introduction to COBIT 5, presented by Rob Stroud of CA Technologies

Tuesday, 8 May
7:15-8:15 a.m.—Comparing COBIT 4.1 to COBIT 5, presented by Rob Stroud of CA Technologies

Thursday, 10 May
8:30-9:45 a.m.—Migrating to COBIT 5 for Auditors, presented by Tony Noble of Viacom

COBIT Lounge (All days)
Visit with COBIT 5 subject matter experts, who will be available to answer your questions.

Visit the **North America CACS** page of the ISACA web site for more information and to register.

Jimmy Heschl, CISA, CISM, CGEIT

Is head of process analytics and control at Bwin.Party Digital Entertainment plc. Previously, he worked as IT advisor at KPMG and Ernst & Young. He has strong experience in GEIT and has supported numerous national and international organisations in the adoption of good practices, such as COBIT, COSO, ITIL and ISO/IEC standards. Heschl has assisted in the development of the CGEIT certification and has authored several publications and initiated and led ISACA's COBIT mapping programme.

Endnotes

[1] Weill, Peter; Jeanne W. Ross; *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, USA, 2004

Come join the discussion! Mike Gill will be responding to questions in the **discussion area of the COBIT (4.1 and earlier)—Use It Effectively** topic beginning 23 April 2012.

IT Risk Is Business Risk

By Mike Gill, CISA, CISM, CISMP, ISO 27001 LA, PCIRM

To make a dangerously sweeping generalisation, most folks outside the risk management, finance and technical control sectors frequently see information security and controls as 'getting in the way'—an inconvenience to business as usual.

Often, business colleagues trying to launch state-of-the art systems to support marketing initiatives, or perhaps newly redesigned business processes, say they could do without the "hassle" of jumping through all those security hoops (i.e., pre-launch controls assessments and gate reviews). IT risk management is often seen in a negative light when important deadlines are looming. Too often, IT risk (business risk relating to IT usage) is treated as an afterthought, possibly even overlooked completely. Why does this happen?

Similar to the testing phase of the project management life cycle, IT security is often seen as something that can be sacrificed—needless bureaucracy that negatively impacts launch timings. IT risk and enterprise value somehow have become separated. What is needed is a way of integrating IT risk into enterprisewide risk and governance models, so the value of IT risk management can be demonstrated.

Mixed Audiences Require Different Approaches

Of course, it depends on the target audience. Marketing people are not afraid to take risks in business because there are high returns to be had, and such risk taking is essential to a continually healthy business environment; understanding risk appetite and risk tolerance levels in the enterprise is crucial to a successful governance framework.

That approach can be compared to the largely risk-balanced finance community, where gaining support for control initiatives from chief financial officers or finance directors is generally not too difficult to obtain, because the risk/value model is ingrained in the finance community. Alignment of risk appetite can happen successfully only when the right tone is established and communicated from the top down. Another critical success factor in the integration of risk management processes is defining and enforcing personal accountability for operating within acceptable and well-defined risk tolerance levels throughout the enterprise as a whole. ISACA's Risk IT: Based on COBIT (now incorporated in COBIT 5) introduces a framework that allows IT risk to be aligned and integrated with operational risk models, delivering a method of enabling mature discussion of IT risk at senior levels within the enterprise.

How does one handle such mixed business audiences? In the author's experience (20-plus years in the automotive, media and finance IT risk management space), this diversity is a healthy asset—essential in fact to that age-old conundrum of assessing risk vs. cost. It is a business balancing act, a necessary reality check.

For example, finance colleagues will not approve purchase requisitions without the inclusion of strong, sound cost-benefit analysis. Marketing colleagues will not accept proposals for new application or infrastructure developments without a rational business case, written in plain language, and without the usual overly dramatic worst-case scenarios. Synchronisation of risk management streams can flourish only by ensuring that the management of IT-related business risk is aligned with the overall enterprise risk management (ERM) initiatives. Risk IT extends and enhances COBIT, so there is no requirement to reinvent

existing IT information and governance frameworks.

Do Not Forget the Need for a Reality Check

Nature has a habit of disrupting day-to-day business: Destructive weather, earthquakes, volcanic ash, for example, periodically test and potentially jeopardise business operations, and humans continue to contribute to the risk mix through fraud, theft, acts of terrorism and, in rare cases, all-out war.

So, risk and cost must be balanced, along with theory vs. practice. Likelihood plays a significant part. In fact, likelihood is *key* to effective and realistic risk management. How likely is it that a devastating risk will actually manifest itself, really? Be honest. And, even once manifested, what will the impact on the business be? Is it truly likely to threaten the business? Most of the time, the actual impact is not a worst-case scenario at all.

However, the impact on the organisation must be carefully considered. Media outlets run daily stories on IT risk-related scenarios (e.g., identity theft, e-espionage, data loss, significant fraud cases, disgruntled employees running amok), so security professionals no longer need to paint their own risk scenarios and put forward worst-case scenarios to senior executives—they get it! Only by considering real risk factors and environmental risk factors can a balanced and credible view of overall enterprise risk be delivered.

In short, risk management needs an injection of reality, and fast! Scenario planning is a way to deliver that injection. Without scenario planning to insert that realism—theoretical risk explained in easy-to-understand business terms, with credible risk definitions, impact assessments, likelihood statistics and monetary values reflected in risk scores—the information security, risk management and compliance communities will continue to fail in getting their messages to senior management and ensuring that IT risk is always connected to business objectives.

Open Up Communication Channels

Risk must be explained in plain language, with the cost of risk mitigation stated clearly, alongside the projected cost impact of manifested risk. This is not complicated to do.

For example, marketing people understand brand value; risk people understand the potential for reputational damage caused through security breaches. Bolting these two understandings together creates the foundations for realistic risk vs. cost analysis. This reality injection helps promote fair and open communication of IT risk throughout the enterprise and ensures that staff understands that this is a continuous process and an important part of daily business activities. Are there any additional, associated ethical and moral issues that could cause further—in rare cases, irreparable—brand damage? Here is another simple example: How much would sales be impacted if a web site were to be defaced or taken down during a high-profile marketing campaign? How much would it cost to secure that web site against such attacks? Subtracting one of the monetary values from the other will clearly indicate how much funding needs to be set aside to implement those precautionary methods.

It also helps to focus on the business data, rather than the ‘IT clutter’ around it: Lost customer data can lead to lost revenue, which is simple to understand. Corrupted data can also lead to lost revenue—also simple to understand. Data not being available when the business needs them is perhaps the easiest to explain in terms of lost revenue.

Risk Management Integration

All that is required is a way of calculating rough figures for revenue losses. This process cannot be fully automated, as up-to-date environmental risk data must be fed in and considered in all cases. Rather, trained, certified and experienced professionals must be utilised to help form a balanced view. In the author’s experience, self-created tools and spreadsheets, and even some off-the-shelf applications, while helpful, quickly reveal a critical missing ingredient if used on their own: the human factor.

Risk IT (now incorporated in to COBIT 5) provides tools and techniques to help understand and communicate tangible risk to business operations, as opposed to generic checklists of controls or compliance requirements. Once key enterprise stakeholders have been engaged, IT-related business risk management can be truly integrated into overall ERM.

Risk IT enables enterprises to understand and manage all significant IT risk types. The Risk IT framework provides an end-to-end, comprehensive view of all risk related to the use of IT, as well as a similar view of risk management. The framework fills a gaping hole between generic risk management frameworks (e.g., COSO Enterprise Risk Management and ISO/IEC 31000) and detailed (primarily security-related) IT risk management frameworks.

The key message here is: IT risk *is* business risk—the two can no longer be thought of and treated separately.

Mike Gill, CISA, CISM, CISMP, ISO 27001 LA, PCIRM
is managing director of HQ Risk Management Ltd., a company he established in 2005 to help organisations pragmatically translate information security requirements into realistic, achievable and sustainable controls. Gill works with large, multinational corporations in the automotive, media and telecommunications sectors. He can be contacted via LinkedIn at **http://www.linkedin.com/pub/mike-gill/1/435/48b** or at **mikegill@hqrm.com**.

Come join the discussion! Erik Guldentops will be responding to questions in the **discussion area of the COBIT (4.1 and earlier)—Use It Effectively** topic beginning 23 April 2012.

Between Fear and Greed, IT Value Is Losing Out!

By Erik Guldentops

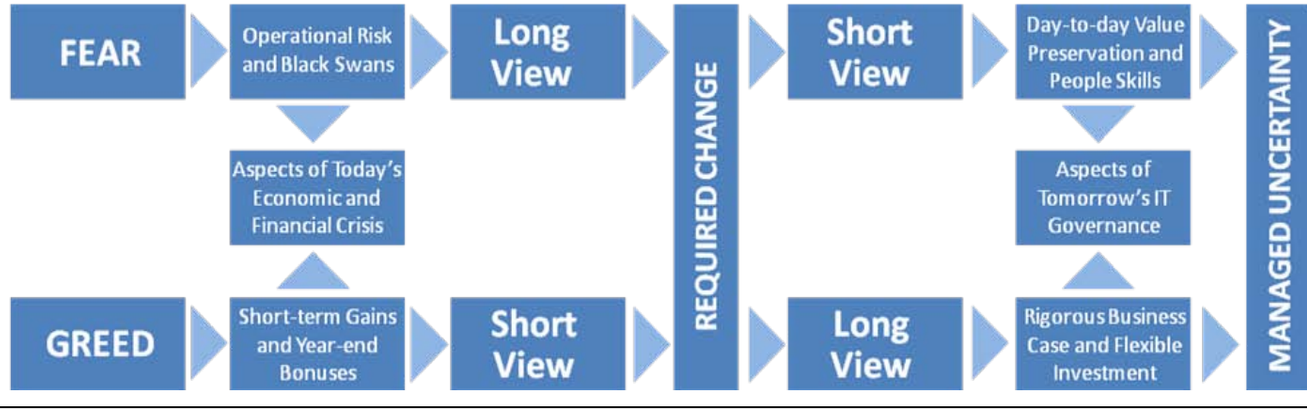
When asked why he was pushing the adoption of COBIT as the IT governance framework for his enterprise, the chief executive officer (CEO) of a large savings bank in Asia reminded me that people are driven by two things: fear and greed! He played upon greed by picturing the value that would be created by adopting the framework, value in which all would share. And, he played upon fear by pointing out that if insufficient value was being created, all would suffer. When thinking about the current economic and financial crisis and its parallels with the risk and value debate in IT governance, I was reminded of this encounter, which happened several years ago. I was especially reminded of the way we usually deal with short- and long-term views.

Fear makes us take the long view of big IT risk (also known as Black Swans[1]), whereas we should maybe first focus on short-term day-to-day IT value erosion. Greed makes us take the short view of quick returns and year-end bonuses, whereas we should take the long view of creating sustainable enterprise value with IT investments.

Rather than looking for short-term gains (while not excluding them), we need to focus more on IT investments by rigorously following the business case and increase or stop our investments when assumptions or conditions change. This is a key message from Val IT: Based on COBIT.[2] We have to be flexible and accept uncertainty of value outcome, but also change our attitudes and practices to better deal with uncertainty. One of these tough changes is accepting that stopping a project in time is a success!

Rather than exclusively focusing on major, expensive and long-term contingency plans for big and improbable IT risk, we also need to focus on the short-term day-to-day value erosion of spam, malware and improper use of enterprise IT. This is a key message from Risk IT: Based on COBIT. For the long term, we need equally to be flexible and accept uncertainty of risk outcome, but deal with it by increasing awareness and building skills, attitudes and capabilities that enable us to deal with the unexpected. One of these tough changes is to focus more on general people skills and a bit less on specific contingency plans because things will not go as expected—especially in a contingency. See **figure 1**.

Figure 1—Fear and Greed: The Need to Switch Management Focus



When remembering that it is attitude governed by greed that put us in the current financial crisis and thinking about the fear that it will get worse before it gets better, we realize the uncanny parallel with the current challenges of governing IT value and IT risk.

And, it does require a major change. Let's begin with accepting uncertainty and deal with it! But, also, let's work on suppressing this urge for short-term gain and the unnecessary fear of the unexpected. Let's focus on the day-to-day erosion of IT value and also on applying business cases rigorously for IT value creation. That's how we beat fear and greed.

Erik Guldentops

Is a lecturer at the Management School of the University of Antwerp, Belgium. He worked for many years at SWIFT (Society for Worldwide Interbank Financial Telecommunication), where he held the positions of inspector-general and director of information security and worked with its board and executive management on the subjects of governance, risk, security and control. He held several positions in ISACA and the IT Governance Institute® between 1989 and 2007 and was instrumental in the development of COBIT and Val IT. He recently chaired a panel of professors that reviewed the master of IT audit programmes in four universities in The Netherlands.

Endnotes

[1] Until the discovery of Australia in the latter part of the 18th century, scientists could never have predicted nor believed the existence of black swans. That is why totally unexpected events are called black swans; it is a metaphor that encapsulates the concept that an event is a surprise (to the observer) and has a major impact. After the fact, the event is rationalized by hindsight. The theory was developed by Nassim Nicholas Taleb. One can argue that the attacks on the US on 11 September 2001 or the current financial crisis were not totally unexpected, but they were certainly not on the list of most (if not all) risk managers.

[2] The scope of governance and management of enterprise IT (GEIT) practices addressed in Val IT and Risk IT are now an integral part of COBIT 5 (**www.isaca.org/cobit**), such that COBIT 5 can act as the framework by which enterprises can identify the GEIT needs of all stakeholders and balance short- and long-term enterprise goals effectively.

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.