Building Acceptance and Adoption of Governance of Enterprise IT
By Bob Frelinger, CGEIT

“Building Acceptance and Adoption of COBIT at Sun Microsystems” is the title of an article published in the ISACA Journal in 2005. Much has happened since then, including the acquisition of Sun Microsystems by Oracle Corp. And, in all that time, the light has kept shining on COBIT, and the COBIT/governance champions have continued to drive the acceptance and adoption of COBIT and the governance of enterprise IT (GEIT).

During that time, the enterprise has enjoyed some successes and learned some valuable lessons along the way. The following are the key lessons learned:

1. **Understand the target.** COBIT is not the target. The target is improved governance and management of the enterprise’s IT. To do so means adopting, leveraging and implementing the industry-accepted concepts and practices that are embedded in COBIT. COBIT provides the overall framework, but when it comes to execution, the enterprise must dive deeper into those concepts and practices.

2. **Use the COBIT umbrella.** COBIT is the end-to-end umbrella framework. The enterprise developed a presentation that showed how the most common industry-accepted frameworks/methodologies/practices complement each other.\(^1\) It is a little dated because of the updates to some of the frameworks that have taken place, but it still tells the story. COBIT goes a long way in harmonizing the many frameworks. This is important and incredibly valuable in dealing with the many IT specialties. Specialists are very good at what they do. Service management professionals manage, and, for most, their preferred guidance is ITIL. Security professionals protect, and, for many of them, the preferred guidance is the ISO/IEC 27000 series. By using a COBIT-inspired model, all groups were able to see how their work fit under an overall umbrella and how their work related to each other’s work.
3. **Stay focused.** Improving the governance and management of enterprise IT is a journey, not a destination. Some enterprises want to focus on the short term. That is fine as long as it is in the context of the longer-term direction. Related to this is the worry among some employees that COBIT will be replaced within the enterprise in a year or so by something else that might be the “hot topic” in the management world. Two things are helping to avoid that. First, the enterprise has a COBIT/governance champion, who keeps an eye on where the concepts in COBIT can add value. Second, the enterprise is not implementing COBIT *per se*, it is implementing improvements to how it governs and manages the IT contribution to the enterprise, and COBIT is the guiding framework.

4. **Use it all.** COBIT and all the COBIT collateral, including Risk IT and Val IT, provide an amazing body of work. There are golden nuggets throughout all of the material. By having someone who has an in-depth understanding of the COBIT material, a COBIT champion, the organization can get really serious about improving governance and management of enterprise IT. For instance, Sun/Oracle has found the mapping documents very helpful when talking about how the various frameworks all fit together. Sun/Oracle embraces ITIL as well, and has had some success using the COBIT *User Guide for Service Managers*.

5. **Avoid common mistakes.** Using the Sun/Oracle experience, and after consulting other organizations that are undertaking implementations of governance of enterprise IT using COBIT, some common reasons that implementations fail have been identified. As may be expected, they fail for many of the same reasons that other transformational change efforts fail.²

The following are some specific examples of how Sun/Oracle has successfully leveraged the concepts in the COBIT-related materials:

1. Sun/Oracle leveraged the IT Assurance Guide: *Using COBIT* to create a discussion worksheet for process health and maturity self-assessments. It is a two-part document. The first part applies to all processes and addresses the six generic process controls. The second part addresses the controls specific to each individual process. Sun/Oracle uses the input and output tables to identify key boundary processes. This ensures that the enterprise has key stakeholders from these processes involved in the discussion. The focus of the facilitated discussion is the process’s current state and the business impact of that state. The discussion of the business impact is influenced by the business objectives. Sun/Oracle uses the goals cascade in COBIT (appendix A and the management guidelines) to help provide a line of sight between its activities and its business goals. The enterprise can then step easily into a maturity assessment of the process using the maturity attributes (figure 15 of COBIT 4.1).³

2. To bring predictability and reliability to how the IT group plans and manages the work across the enterprise, the group leveraged many of the concepts embedded in the COBIT framework portion of the COBIT 4.1 publication. The group needed a way to operationalize the Plan-Do-Check-Act (PDCA) concept at the IT organization level. The enterprise had a corporate planning cycle, and the IT group created the “IT management cycle” to complement that corporate activity. Figure 1 shows how the IT management cycle is represented;
3. It became useful to demonstrate what the enterprise must do to achieve integration and alignment of the governance/management activities. **Figure 2** is a matrix that helped Sun/Oracle do just that. It combines the IT management cycle with the IT governance focus areas. The key message is: Both vertical and horizontal integration and alignment of the activities are necessary.

4. From time to time, the IT group revisits the components of governance of enterprise IT as described in COBIT: leadership, organizational structures and processes. The enterprise decided to focus on the organizational structures and has found that it has done a pretty good job with the vertical structures (the traditional who reports to whom), but has not focused sufficiently on the necessary horizontal (or lateral) structures. This led us to two new internal rules:
   - Horizontal organizational structures (i.e., a risk council or information security community) must be as deliberately thought through as the vertical structures of the organization.
   - When a decision is made to form a horizontal structure, it must have a well-defined charter that includes the mission or purpose of the group, the composition and the decision rights.

**Bob Frelinger, CGEIT**
Is currently manager of the Process Management Program for Oracle’s Global IT group. Before joining Oracle, he served in a similar position at Sun Microsystems Inc. He is a former board member of the ISACA Denver Chapter, and has served on several ISACA international boards and committees. He has been leveraging COBIT, ITIL, Six Sigma, PRINCE2 and other industry-accepted practices since 2003, and is a strong proponent of drawing on the strengths of each.

**Endnotes**

1. Find a copy of it at [www.isaca.org/Groups/Professional-English/frameworks/GroupDocuments/frameworks_v3_111908.pdf](http://www.isaca.org/Groups/Professional-English/frameworks/GroupDocuments/frameworks_v3_111908.pdf).
2. A copy of the top six reasons is available at [www.isaca.org/Groups/Professional-English/cobit-implementation/GroupDocuments/Why%20IT%20Fail.pdf](http://www.isaca.org/Groups/Professional-English/cobit-implementation/GroupDocuments/Why%20IT%20Fail.pdf).
3. To see an example of the discussion worksheets for problem management, go to [www.isaca.org/Groups/Professional-English/cobit-implementation/GroupDocuments/process_health_and_maturity_assessment.pdf](http://www.isaca.org/Groups/Professional-English/cobit-implementation/GroupDocuments/process_health_and_maturity_assessment.pdf).
Overview of COBIT 5 Public Exposure Commentary
By John Lainhart, CISA, CISM, CGEIT, CRISC, CIPP/G, and Derek Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM

The COBIT 5 development project prepared drafts of COBIT 5: The Framework and COBIT 5: The Process Reference Guide for public review from 27 June to 18 September 2011. The drafts were made available on the COBIT 5 update page on the ISACA web site. Comments were solicited from all interested parties. These comments were collected and analyzed for significant observations that would result in changes to the draft documents.

Feedback was collected in two forms, through an online survey and via a detailed feedback form. Reviewers were able to submit either or both forms of feedback. The results of the survey were further analyzed and quantified. Overall, 79 percent of the reviewers’ ratings were positive.1

The detailed feedback in the comments supported the positive ratings reviewers applied to them. Many reviewers found the material to be initially overwhelming in volume and detail, but in the end rated it favorably. Not surprisingly, where the material was perceived as too voluminous or unclear the content was reported in the comments as incorrect or difficult to assimilate.

Many reviewers reported COBIT 5 as being more comprehensive and tying together issues they struggled with in COBIT 4.x and earlier. Most notably, several reviewers reported that the inclusion of Val IT, Risk IT and BMIS was a welcome improvement. Other reviewers noted that the inclusion of these ISACA products was not done at a sufficient enough level of detail to be useful. As a result, future development proposals are planned for COBIT for security, assurance, risk and value to address this issue. The integrated framework, with Val IT, Risk IT and BMIS tied to COBIT, was not always understood by reviewers, but those who did understand the concept tended to express their approval of its form and content.

Another area that generated several comments was the goals cascade, which presents the relationships among the stakeholder needs, governance objectives, enterprise goals, IT-related goals and enabler goals. Despite its inherent strength and basis in the balanced scorecard, the cascade was perceived as difficult to digest immediately and some reviewers felt it was vague at the level presented.

A few inconsistencies or inaccuracies were reported in the drafts. The issues reported were typically with regard to the connections among the management practices via the input and output tables. A gap was also reported in that COBIT 4.1 had an additional set of control objectives—Application Controls and Process Controls—that did not appear to be treated in COBIT 5.

The COBIT 5 Development Team has digested all of the feedback from the public exposure and has been working diligently to incorporate the significant observations. The completion of the Framework and Process Reference Guide are on schedule and both will be published in March or April 2012, along with COBIT 5: The Implementation Guide, which is intended to assist stakeholders in implementing COBIT 5 for governance and management of enterprise information and technology assets.

1. "Reviewers’ ratings were positive."
John Lainhart, CISA, CISM, CGEIT, CRISC, CIPP/G
is the IBM Global Business Services global security and privacy service area leader and public sector cybersecurity and privacy service area leader. He represents IBM on the American Institute of Certified Public Accountants (AICPA) Assurance Services Executive Committee’s Data Integrity Task Force and the Strategic Advisory Council for the Center for Internet Security. Currently a member of ISACA’s Framework Committee and a cochair of the COBIT 5 Task Force, Lainhart has held numerous positions with ISACA and the IT Governance Institute (ITGI), including international president.

Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM
is the chief executive officer of UK-based audit consultancy Ravenswood Consultants Ltd., which he founded in 1995, and is an information audit and security specialist with 30 years experience, working on audit, security and governance projects throughout Europe. He is a chartered fellow of the British Computer Society, a fellow of the Institute of IT Service Management and a member of the Institute of Information Security Professionals. Oliver is regarded internationally as an expert in information governance, audit and security and has spoken at international conferences on various information security and audit topics. Oliver is cochair of the COBIT 5 Development Task Force and a member of the ISACA Framework Committee and Cloud Security Task Force.

Endnotes

1 When reviewing the responses, the top two of the five possible responses were viewed as positive ratings.

Risk IT Framework for IT Risk Management: A Case Study of National Stock Exchange of India Limited

By Sunil Bakshi, CISA, CISM, CGEIT, CRISC, CISSP, ABCI, AMIIB, MCA, PMP

National Stock Exchange (NSE) is the largest stock exchange in India catering to 1,200-plus members. Globally, NSE has been ranked second in stock index options and third in single stock futures and stock index futures. The business processes of NSE are heavily dependent on IT. Average daily turnover of trades processed by NSE are INR 1,441,010.1 At a national level, NSE is a critical organization for the Indian economy and is identified as one of its most sensitive organizations.

The criticality of business operations required NSE to focus on risk management as an integral element of its day-to-day business processes. Up until this new focus, the existing risk management process mainly focused on addressing business risk. The IT risk assessment method was complementary to the business risk processes, and the approach adopted was periodic assessment (once a year), which until now was considered adequate.

However, during the review of risk assessment, it was observed that the dynamic nature of the business environment had been prompting frequent changes in IT infrastructure. These changes constituted not only changes in hardware, but also included revamping applications and identifying new service delivery channels. This prompted the decision to revisit the IT risk management approach.

IT Risk Management Project

The IT risk management project was initiated with a primary objective to ensure that ongoing risk assessment was an integral part of IT operational and governance processes. Milestones and deliverables for this project are listed in Figure 1.

<table>
<thead>
<tr>
<th>Project Step</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Define the risk management framework by considering available global standards.</td>
<td>IT risk framework, risk evaluation criteria and risk response policy</td>
</tr>
</tbody>
</table>
2. Implement the framework uniformly across the IT organization. Identifying stakeholders and risk champions in each process area (e.g., applications, operations, network, databases, system administration)

3. Conduct risk identification workshops to confirm existing risk and identify new risk. Risk register for each process area

4. Use framework to assess identified risk and develop risk response options. Updated risk register and control catalog based on response

5. Build a risk register and link it with the control catalog. Analyzing risk register and control catalog to identify control gaps

6. Develop a process for risk aggregation and developing the risk profile. Risk register for the organization and the risk profile, showing inherent, current and residual risk

7. Establish communication channels to communicate the risk profile. Identifying stakeholders and communicating the risk profile and results of the risk management process

8. Link IT risk management with governance process. Definitions of key performance indicators (KPIs), key risk indicators (KRIIs) and establishment of monitoring process

Choosing a Guiding Risk Management Framework

As a first step to achieving the objective, a comparative study of available standards and frameworks was performed to identify a framework that would meet NSE’s IT risk management requirements. The criteria used for evaluation is described in figure 2.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The framework should integrate with IT operational processes.</td>
<td>Risk evaluation is an ongoing process, and it is necessary to integrate the risk evaluation process as part of normal IT operations.</td>
</tr>
<tr>
<td>The framework must be linked with the control environment/framework.</td>
<td>NSE needs to implement controls that will help in mitigating identified risk.</td>
</tr>
<tr>
<td>The framework should provide for the monitoring of risk and help in identifying parameters for monitoring.</td>
<td>Risk monitoring refers to monitoring of related scenarios that will enhance the risk materialization.</td>
</tr>
<tr>
<td>The framework must provide for a governance process.</td>
<td>Risk management shall continue to work in silos unless linked with business objectives. Governance framework should include a risk monitoring process.</td>
</tr>
<tr>
<td>The framework must be flexible and should integrate easily with the business processes.</td>
<td>IT risk, if materialized, impacts the business objectives/operations; hence, it must be able to link with business objectives.</td>
</tr>
</tbody>
</table>

After thorough review, NSE chose the Risk IT framework as the benchmark for NSE’s creation of its risk management framework. The following are the main reasons for selecting Risk IT:

- Risk IT provides granular guidance on risk management processes in the three major areas required—Risk Evaluation, Risk Response and Risk Governance—covering all traditional risk management processes, including risk identification, risk assessment, risk response, risk treatment and risk monitoring.
- Risk IT focuses on linking IT risk with business objectives rather than IT assets.
- It is the only framework that provides detailed processes for IT risk governance.
- Risk IT is focused on building risk scenarios (also provide list of generic scenarios) that help in directly linking risk management with business processes.

NSE’s Risk Management Framework

Following this study, NSE’s risk management framework has been developed based upon Risk IT (figure 3).

NSE’s high-level objectives for each area of the framework are:

1. Risk Governance:
   - Maintain a common view—Maintain standard risk register to provide a risk update in business terms.
   - Define the organization structure—Define roles and responsibilities across the organization to review and maintain IT risk profile.
   - Make risk-informed decisions—Provide IT risk dashboard to IT management to enable risk-informed strategic decisions.
2. Risk Evaluation:
   • Collect data—Prepare risk scenarios, conduct risk-identification workshop, establish process touch points for risk updating and link the impact assessment with the business impact analysis (BIA).
   • Analyze risk—Use a standard table for defining likelihood and Impact. Use the Delphi technique\(^5\) wherever required.
   • Maintain risk register—Update and maintain the risk register to develop the risk profile by aggregating departmental risk.
3. Risk Response:
   • Articulate risk—Establish a process for defining risk response and communicating to stakeholders.
   • Manage risk—Maintain a control catalog with risk mapping, and define the review process.
   • React to risk events—Establish a link to incident management, change management and operations management to review risk.

NSE’s Business and IT Mapping

NSE provides IT-based services to members and brokers for trading in securities on behalf of their clients and investors. There are multiple different market segments.

Each market segment has four major processes: trading (consisting of placing orders by members that are matched by matching engine and confirmed), risk management (online monitoring of activities), surveillance (online pattern matching to identify out-of-turn trades to restrict malpractices), and clearing and settlement (involving delivery of securities), in addition to various supporting processes.

Figure 4 depicts the mapping of risk management processes covering these high-level IT processes.
Implementation Approach

The implementation approach for the risk framework at NSE is described in figure 5.

<table>
<thead>
<tr>
<th>Activities</th>
<th>Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select applicable risk scenarios for IT applications, process and projects.</td>
<td>All possible risk scenarios based on the perceived risk to the IT universe</td>
</tr>
<tr>
<td>Identify various, applicable areas of risk.</td>
<td>The internal and external environment</td>
</tr>
<tr>
<td>Identify the business impact (financial and nonfinancial) and the likelihood.</td>
<td>BIA reports, audit reports, and IT and business teams</td>
</tr>
<tr>
<td>Identify existing controls.</td>
<td>Input from IT teams</td>
</tr>
<tr>
<td>Validate the results with IT teams.</td>
<td>IT teams review of data collected</td>
</tr>
<tr>
<td>Validate risk registers with IT teams.</td>
<td>Input from IT teams</td>
</tr>
<tr>
<td>Validate risk and impact with business teams.</td>
<td>Input from business teams</td>
</tr>
<tr>
<td>Finalize risk registers.</td>
<td>-</td>
</tr>
<tr>
<td>Ensure continuous monitoring, reporting and communication.</td>
<td>Result of risk assessment</td>
</tr>
</tbody>
</table>

The implementation of risk management was conducted at two levels:
1. Develop risk register for business functions.
2. Define aggregation process to arrive at an organization-level risk profile.

Business processes were categorized in the following areas:
- Most critical (core production)
- Critical (production)
Support functions
For each business function, the following activities were performed:
- Conduct risk evaluation facilitated workshops.
- Generate risk profile for inherent risk (risk without considering controls).
- Determine response options.
- Identify and assess controls from control catalog.
- Identify positive (excess) and negative (missing) control gaps.
- Define a plan for closing control gaps.
- Finalize the risk register.
- Obtain confirmation from risk owner (department heads).

For aggregation of the risk profile at the organization level, the following activities were performed:
- Build a matrix for all identified risk.
- Collect department-wide data, and build the matrix.
- Add weightage of criticality for each department.
- Arrive at organization-level risk profile.
- Review and sanitize the risk profile by eliminating mathematically inappropriate impacts and likelihood.
- Present risk profile to board and senior management.

Risk Management Processes
NSE concluded that changes in risk need to be tracked on an ongoing basis and identified the following triggers as having an impact on risk status: incidents, events, changes in IT and business environment, and procurement based on strategic IT decisions. **Figure 6** shows the risk updating process based on these identified triggers.

A uniform scale for quantifying the likelihood and qualitative impact assessment was defined for use across the organization.

Conclusion
Use of the Risk IT framework helped NSE in building a uniform structure and view of IT risk across the organization. The Risk IT framework helped NSE in:
- Presenting a uniform view of IT risk to stakeholders
- The use of scenarios and avoiding jargon encouraged stakeholders to participate in the process

**Figure 6—Risk Updating Process Based on Identified Triggers**
• Defining a monitoring process for continuous updating of changes in the risk profile
• Acceptance by risk owners

An Excel-based tool that automatically updates the risk profile is being used to track and maintain risk changes. The risk profile is presented in three stages:
• Inherent risk (total risk without controls)
• Current risk (overview of current risk based on existing controls)
• Residual risk (risk after applying control gaps)

The residual risk is arrived at after considering the impact of implemented controls over inherent risk. Considering the future road map and alignment of the Risk IT framework with COBIT, COBIT 4.1 control objectives were used to identify control gaps and to assess the impact of controls on the risk profile.

Sunil Bakshi, CISA, CISM, CGEIT, CRISC, CISSP, ABCI, AMIIB, MCA, PMP
Is a consultant and chief information security officer for NSETECH (NSE Infotech Services limited). A gold member of ISACA, he is a member of the CRISC Test Enhancement Subcommittee. Bakshi has previously worked in various capacities with the State Bank of India, the Enterprise Risk Services Group of Deloitte Touche Tohmatsu, India Private Limited, and Wipro Consulting Services.

Endnotes

1 National Stock Exchange, Highlights of NSE Newsletter, November 2011
2 Ibid.
3 The evaluation process of the various standards is out of scope for this article.
4 ISACA, Risk IT, USA, 2009, www.isaca.org/riskit
5 Delphi technique is a method to get an opinion of experts for arriving at consensus by asking uniform questions. In risk assessment it is used by asking the experienced judgment on the likelihood and impact of risk to users who are associated in the risk evaluation process to arrive at consensus on measures of likelihood and impact of identified risk.

COBIT and the Cloud
By Marc Vael, CISA, CISM, CGEIT, CISSP, ITIL-SM

The phenomenon known as cloud computing has emerged as one of the most important evolutions in IT in the last three years and is changing the way enterprises handle information and computing power to accomplish their business objectives. As business executives look for innovative ways to save money and increase the trust and value in their information systems, cloud computing can and should be considered as an attractive option. Some of the benefits that cloud computing promises include:
• Rapid, elastic and transparent scalability of IT power for clients
• Transitioning of capital expenses to operating expenses (from CAPEX to OPEX)
• Shorter life cycle development of new applications or deployments
• Shorter time requirements for new business implementations
• Optimized computing utilization
• Automated monitoring, measuring and logging of IT services

As cloud computing evolves in importance worldwide, it is important that enterprises understand how to handle the paradigm change in business operations that the cloud presents in an effective and efficient manner. This level of understanding will enable enterprises to maximize the benefits and opportunities that cloud computing offers, while simultaneously addressing its unique and emerging threats and vulnerabilities in an intelligent manner.

ISACA has developed several governance and management tools to assist executives and managers to integrate and align their use of information and technology into the primary business focus of the enterprise:
• COBIT—The global comprehensive and integrated IT governance and management framework that addresses every aspect of IT and IT controls
• Val IT—The governance framework that focuses on value delivery and ensures that IT-enabled investments are managed through their full economic life cycle
• **Risk IT**—A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk

• **Business Model for Information Security (BMIS)**—A holistic model for managing information security that takes a business-oriented approach

While these tools have not been designed specifically for cloud computing environments, the principles are applicable as such. In fact, cloud computing may amplify the importance these tools have in any enterprise as the impact from cloud computing on any business may change its business processes. In traditional IT environments, everyone in the business has to go to the IT department to obtain IT-related services; with cloud computing capabilities, employees can go straight to a cloud service provider (CSP) to acquire IT and business services online. This elevates the enterprise’s level of risk and opportunity. Having tools such as the aforementioned ISACA frameworks will help any enterprise to implement repeatable processes and appropriate control levels, taking maximum advantage of the opportunities while minimizing the related risk.

The COBIT framework offers potential cloud computing users valuable benefits as it produces a summary assessment of the business risk and achieved business value of an application, and can help practitioners evaluate many risk, resource or value issues.

When enterprises decide to utilize cloud computing services for some or all IT services, their business processes are impacted, making (IT) governance more outspoken than ever. Following are just a few reasons why enterprises should implement and maintain a sound governance of enterprise IT (GEIT) program:

• To effectively manage increasing risk, including security, compliance, projects and partners
• To ensure continuity of critical business processes that extend beyond their own data center
• To communicate clear organization objectives internally and to all relevant third parties
• To adapt easily. Flexibility, scalability and services are changed in a cloud computing environment, enabling the organization and business practices to adjust to create new opportunities and reduce cost.
• To facilitate continuity of IT knowledge, which is essential to sustain and grow business
• To handle the myriad of rules and regulations

For organizations to gain maximum benefits from the use of cloud computing, a clear governance and management framework and supporting plans and practices must be developed, approved, executed and monitored. The governing stakeholders should set the proper direction and objectives for cloud computing within the enterprise.

There are many variables, risk areas and values in any cloud opportunity or program that affect the decision of whether a cloud computing application should be adopted from a risk/business-value standpoint. Each enterprise has to weigh those variables to decide for itself if cloud computing is an appropriate solution for its current challenges.

**Editor’s Note**

For additional information, consider reading the ISACA publication *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud.*

**Marc Vael, CISA, CISM, CGEIT, CISSP, ITIL-SM**

Is chief audit executive at Smals, a Belgian not-for-profit IT company with more than 1,800 employees working exclusively for the Belgian Federal Social Security Institutions. Vael has more than 20 years experience in risk and security management, business continuity management, privacy, outsourcing, and IT audit in private and public enterprises. He is a director on the ISACA Board of Directors, and chairman of ISACA’s Knowledge Board and of ISACA’s Cloud Computing Task Force.
Using COBIT to Aid in Hospital Risk Management

By Masatoshi Kajimoto, CISA, CRISC

In medical institutions, IT can be a double-edged sword: It can mitigate risk and, yet, be a big risk factor. Without appropriate operational risk management, IT risk management will fail. Based on this author’s experience, COBIT is an essential approach for medical institutions to implement total hospital information systems and manage operational risk. This article will explain how COBIT was utilized for this purpose at Takeda General Hospital, which is located in Aizu-Wakamatsu, Fukushima Prefecture, Japan.

First, a hospital information system (HIS) implementation project process, based on the COBIT approach, was successfully completed and appropriate controls were implemented.

As many COBIT users have realized, identifying the appropriate and necessary COBIT controls can be a high hurdle to overcome. In this case, the organization found that it was easy to identify the necessary COBIT controls after completing the identification of the subjects of control activities.

This article describes this first stage, which is based on the descriptions in the COBIT framework and appendix 1 of COBIT 4.1. Following this guidance, the organization began by utilizing the IT balanced scorecard approach.

The IT balanced scorecard approach works closely with COBIT and is evaluated against the defined business objectives. The COBIT process provides a track from generic business goals to IT goals to IT processes. This results in a set of metric indicators with which to monitor and evaluate IT performance.

Risk factors in medical institutions include medical (e.g., medical mistakes, hospital infections, errors), financial (e.g., uncollected payments, shortened hospital stays, cost management) and regulatory (e.g., acceptance of interns, electronic statements). To manage the risk and implement a total HIS, a top-down approach is needed. That is where COBIT comes in.

Of course, in Japan, as in most countries, personal data protection is a very important issue, especially in the health care industry, which is governed in this area by Japan’s data protection law as well as an earlier established law relating to medical care record protection. Storing medical care records at external locations is strictly prohibited. Also, medical care record-related systems (network) cannot connect with outside networks (only a closed network is permitted). Furthermore, transfer of data for remuneration for medical treatment can be done only by electronic media, dedicated line or closed network. Therefore, data-protection-related risk is a matter of course in Japan and, thus, was not a key initiative in this project. That said, other health care organizations taking on a similar initiative may need to consider this issue in greater detail during their review of risk and control.

Begin With a Balanced Scorecard

First, the organization strategy was defined, followed by defining the total IT strategy, broken down into great detail. From the first stage, the hospital’s IT risk, including existing risk, risk tolerance levels and risk acceptance levels, was examined. When defining strategy, it is important to keep in mind that a target of value management will support the achievement of business goals; a target of risk management will prevent the achievement of business goals. Using a traditional balanced scorecard approach, the HIS implementation steering committee, which was established by the hospital president, discussed risk factors with the hospital’s senior management.

The vision and mission statement of senior management are very important in a total HIS, as in any industry. If a total HIS cannot support the top management’s vision and mission statement, the system is of no use. The team determined the following goals for the total HIS, in keeping with top management’s vision:

- Maintain a high level of security and personal information data protection.
- Raise and maintain a high level of medical services.
• Minimize medical mistakes (malpractices).
• Rapidly respond to the medical needs of the community.
• Improve information sharing between the hospital and the community.
• Raise the staff’s skills and knowledge.
• Identify and address new challenges.
• Implement cooperation among each facility.
• Establish total support systems for health care, treatments and nursing care.
• Establish a better environment for doctors’ research activities, and improve medical care in the hospital and related facilities.

Strategic Alignment With Customer Satisfaction
For a hospital, the customers are the patients as well as the communities it serves. The next step was to define customer satisfaction performance indices, or value and risk scales. If the established level is higher than the current level, it will be value creation. If the established level is lower than the current level, risk may be actualized. The team identified the following areas to evaluate on value and risk scales:

- **Improvement of patient satisfaction**—Quick response, shortening of period of treatment, wide selection of methods of treatment, completeness of informed consent forms and better disclosure of information
- **Improvement of cooperation between hospitals and clinics in the same community (medical care zone)**—Quick information sharing, an excellent medical information center, cooperation with the local government where necessary, adherence to the local community’s standards of health care, and improved response from the emergency medical service
- **Improvement of the general public’s satisfaction**—Better disclosure of medical information and better services for healthy people to maintain their health

Strategic Alignment With Finance
With regard to financial issues, the team identified the following areas to evaluate on value and risk scales:

- **Growth**—Accuracy of the request to the health insurance society for remuneration for medical treatments, improvement of profit and appropriate capture of billable medical practice items
- **Profitability**—Effect of cost-reduction activities and capture of information about items that can be cost analyzed
- **Liquidity**—Analysis of factors that determine cash flow worth and better control of equipment and facilities that are counted fixed assets
- **Stability**—Better control of personnel expenses (labor cost)

Strategic Alignment With the Internal Process
When considering the internal process, there are many risk factors and hurdles. Problems related to personally identifiable data (PID) are also hidden here. The team considered:

- **Improvement of the quality of medical service**—Substantial standardized medical treatments, substantial clinical paths and application of them, and substantial medical research and study environments for doctors
- **Medical risk management**—Tracking of medical practices, detailed tracking of medicines from procurement to administration, minimizing medical mistakes (e.g., errors, malpractices) and problem analysis
- **Improvement of business process**—Simplification and speed-up of processes and separation of professional processes and standardized processes
- **Utilization of information**—Expansion of information and knowledge sharing environment (based on “need to know, need to do”) and promotion of end-user computing (EUC) utilization

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

ISACA’s Licensing Program
Expanded course delivery options include classroom-based training and online and blended course offerings. Current company and/or individual licensees are posted on the Training page of the ISACA web site.

COBIT Training Week Course
The 2012 COBIT training dates have been set. COBIT: Strategies for Implementing IT Governance is a comprehensive COBIT training program highlighting IT issues, governance concepts, risk management and control. Register now to attend a scheduled course or visit the On-Site Training page of the ISACA web site for more information about bringing COBIT training to your location.
Learning and Growth

The last BSC area involves “what we can learn and how we can grow.” This area may appear easy, but there can be profound problems. New roles and responsibilities require staffing, and there can be apprehension from personnel (e.g., “This is not my job. Someone else should do this.”). This area strongly depends on senior management’s intentions. And, all staff must remain knowledgeable about medical treatments and regulatory issues. The team focused on:

- **Improvement of professionalism of staff**—Professional knowledge sharing and electronic information gathering and analysis environment
- **Optimization of roles and responsibilities**—Support and optimal roles and responsibilities assignment, and appropriate information security environment
- **Continuing education**—Status of knowledge management implementation, sharing know-how within the hospital, increasing learning opportunities, and flexibility and quick response to environmental changes

Risk Management

To establish appropriate risk management, the preparation phase is very important. The following activities are indispensable:

- **Standardization of wording (name or abbreviation of disease)**—Medical wording was different for each medical department. For example, “HT” could mean “hypertension” (high blood pressure) or “hypotension” (low blood pressure).
- **Change to globally standardized disease name**—This seems easy, but adjustments among many medical divisions can be very difficult. Using a globally recognized standard is essential.
- **Standardization of medical process**—Each medical department operated independently and used its own customized medical process. All need to use a standardized process.
- **Unification of patient case records**—At first, the team found that each medical department managed its own medical record for each patient, creating too many patient case records for one patient. The record should be unified.
- **Standardization of medicine name**—There are different medicines for the same disease and medicines of very similar names. For example, for breast cancer, there is Taxol (paclitaxel) and Taxotere (docataxel). Standardization will reduce confusion.

If standardization of wording is not performed, the dictionary of electronic medical chart systems cannot be implemented, and can become the cause of medical errors. In which case, disease name and appropriate care does not correctly correspond in the system. If standardization of medical processes is not performed, the HIS becomes very complicated and needs many customizations. Such system will be costly and become the cause of human errors. These activities are effectively controlled by PO6, PO7, PO9 and the application controls in COBIT.

Understanding IT

Of course, IT can mitigate risk, such as the interdependency check of diseases, contraindication of medicines, customer/patient satisfaction, medical mistakes, and tracking of wrong medicine and operating costs. But what about other IT risk factors? For example, can terminals (PCs) be sterilized in boiling water? (Only recently have some medical vendors begun providing terminals that can be sterilized.) If a terminal is contaminated by MRSA, what will happen? Electromagnetic Wave (Wi-Fi) may interfere with delicate medical equipment. If local area network (LAN) cables are used for a terminal, such cables may be contaminated. If a power failure occurs, what will happen? Stealing of paper-based patient records is very difficult, but electronic medical chart data are easy to steal for internal (authorized) personnel.

Further, if a doctor cannot utilize a PC quickly, what will happen? If a doctor inputs a wrong disease name or other data, what will happen? If an appropriate recovery process of the system does not exist, what will happen? For IT, 24 hours per day, 365 days per year, operational risk management is a matter of fact.

Conclusion

IT risk and operational risk have interdependencies. And, IT can be a double-edged sword—mitigating risk and, yet, being a risk factor. IT, business processes and human factors all must be considered at the same time. Additionally, if one wants to increase value, risk will increase. If a sound risk management environment is established, value will be created. Separating risk and value is impossible.

This article described the identification of subjects that need appropriate controls; the next phase is identification of controls based on COBIT. Please watch for a future article, expected in volume 2, 2012, of COBIT Focus, covering this phase of the project.
Masatoshi Kajimoto, CISA, CRISC

Is an IT auditor and independent consultant providing services in BPR, HRM, 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 GRA Subcommittee Area 1 and is a member of the GRA Committee.

Endnote

1 www.slideshare.net/MichaelSim/cobit-val-it-balanced-scorecards-presentation

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.

© 2012 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Please contact Julia Fullerton at jfullerton@isaca.org.

Framework Committee

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

Editorial Content

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

©2012 ISACA. All rights reserved.