COBIT® Focus

Volume 1, January 2013

In This Issue:

Come join the discussion! Christos Dimitriadis will be responding to questions in the **discussion area of the COBIT 5—Use It Effectively** topic beginning 25 January 2013.

INTRALOT Introduces COBIT 5 in Its Product Line

By Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, ISO 20000 LA

INTRALOT is a leading international supplier of integrated gaming and transaction processing systems, with presence in more than 50 countries on all continents. The diversity of this multinational environment as well as the criticality of integrity, compliance, quality and operational excellence in the lottery sector dictate the implementation and timely adoption of state-of-the-art frameworks in governance of enterprise IT (GEIT).

As a service and technology provider, INTRALOT is constantly searching for ways to improve its product line in a holistic manner, ensuring that all aspects are taken into account systemically. At the same time, the enterprise recognized that its use of multiple frameworks from several fields, such as quality, security and service management, needed to be managed in a simpler and more effective manner. A single systemic and holistic framework that incorporates business thinking would increase effectiveness and optimize investments. To that end, INTRALOT is implementing COBIT® 5.

In adopting COBIT 5, INTRALOT's main goal is to combine multiple frameworks under COBIT 5, which will help reduce complexity, ensure information quality toward decision making, increase the value gained from technology and enable innovation.

Implementing COBIT 5

Prior to the release of COBIT 5 in 2012, INTRALOT was deploying COBIT 4.1 to address compliance requirements and build control frameworks. COBIT 5's principle for separating governance from management, its systemic nature that brings a holistic

Call for Articles

How are you using COBIT® at your enterprise?

We welcome articles on your experiences with this framework. Deadline to submit copy for volume 2, 2013: 8 March 2013

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

Case Studies

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

approach and the means it provides for merging multiple frameworks under a single one, led to the decision to transition to a COBIT 5 adoption.

The implementation of COBIT 5 started in INTRALOT's product line. The value INTRALOT delivers to its clients is closely coupled with the enterprise's strategic goals in meeting stakeholder and customer requirements. COBIT 5's principle in meeting stakeholder needs and its overall business approach provided the opportunity to communicate to senior management specific and measurable benefits from its adoption.

The initial target was the enterprise's Software Quality Assurance and Control Department, which is responsible for assuring a high level of quality through technology solution testing and for supporting clients over multiple jurisdictions in meeting their needs. This department ensures that INTRALOT products are tested and improved, taking into account security requirements (ISO 27001 and World Lottery Association Security Control Standard), control frameworks provided by clients (e.g., ISAE 3402-based frameworks), ISO 9001 requirements and requirements derived from contractual obligations in 50 countries.

With COBIT 5, the management of the departmental activities is being integrated under a single framework, while its activities are being analyzed per the COBIT enablers. The human and cultural aspects are correlated with properties from each enabler, while technology and tools used by the department were also evaluated to maximize value. At the same time, a set of metrics was created to provide measurable results to senior management in a correlated manner. This correlation itself enables the opportunity for innovation by streamlining product testing and improving processes to deliver products to the market with continually increasing levels of efficiency, speed and quality.

INTRALOT is working on the maturation of the COBIT 5 implementation by continually processing feedback from metrics and analyzing effectiveness. At the same time, the company is implementing *COBIT® 5 for Information Security* and looking forward to subsequent COBIT products such as *COBIT® 5 for Risk*.

Conclusion

Through the implementation of COBIT 5, INTRALOT established a single framework for ensuring product quality and related customer support. Departmental activities were directly linked to strategic goals under one common framework, while maturity assessment was unified under a common set of metrics. This gives the opportunity to provide a more comprehensive type of feedback to senior management toward improved monitoring, supporting decision making at the same time. Complexity is gradually being reduced, information quality is improving by taking into account all enabling processes (holistic approach) and, as a result, innovation is being enabled even further.

Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, ISO 20000 LA

Is head of information security at INTRALOT Group. He has been working in the area of information security for 12 years, and has more than 80 publications in the field. Dimitriadis is currently serving ISACA as international vice president. He is a member of the Permanent Stakeholders Group (PSG) of the European Network and Information Security Agency (ENISA), and has been providing information security consulting services to the International Telecommunication Union, European Commission Directorate Generals, Ministries and international organizations.

Research Update

Recently Released COBIT 5 Materials

- ***Securing Mobile Devices Using COBIT® 5 for Information Security***
- ***Securing Sensitive Personal Data or Information Under India's IT Act Using COBIT® 5***
- ***COBIT 5 Foundation Level Training and Certificate***

Upcoming First Quarter 2013 Releases for COBIT 5

- *COBIT® Process Assessment Model (PAM): Using COBIT® 5*
- *COBIT® Assessor Guide: Using COBIT® 5* and Tool Kit
- *COBIT® Self-assessment Guide: Using COBIT® 5* and Tool Kit
- *COBIT® 5 Assessment-level Training*
- *COBIT® 5 Implementation-level Training*

For more information on COBIT publications and training, visit the **COBIT 5** page of the ISACA web site.

COBIT 5 for Assurance Progress Report, Part 2

By Anthony Noble, CISA

The development of *COBIT® 5 for Assurance* to extend the COBIT 5 family of products is progressing as planned and approved. The project task force is directing and guiding the developers as they build the content for the guide, expanding on the tremendous contributions made by dedicated volunteers during a development workshop held in October 2012.

The objective of the project is to create an assurance view of COBIT 5 that will serve as specific guidance for ISACA's information assurance constituents. The content structure for *COBIT 5 for Assurance* is aligned with *COBIT 5 for Information Security* to allow for efficient use by those professionals using multiple topic focus guides (security, assurance and risk). The draft content items from the workshop are being blended into a consistent form using this structure.

The next step, following the completion of the draft, will be a broader subject matter expert (SME) review. More details about how to get involved with COBIT-related opportunities such as this volunteer SME review (as well as other volunteer opportunities) can be found on the **Volunteering** page of the ISACA web site.

COBIT 5 for Assurance remains on track to be available in early second quarter 2013.

Anthony Noble, CISA

Is the New York-based vice president of IT audit for Viacom Inc. He has 30-plus years of IT experience and 20 years of experience as an IT auditor. He is a member of ISACA's Framework Committee and is the chair of the COBIT 5 for Assurance Guide Task Force. Previously, he was a member of the ISACA Guidance and Practices Committee.

Come join the discussion! Diana Santos and Joao Souza Neto will respond to questions in the **discussion area of the COBIT 5—Use It Effectively** topic beginning 25 January 2013.

Comparison of Enterprise IT Governance Process Assessments Performed With COBIT 5 and COBIT 4.1

By Diana Santos, CAPM, and Joao Souza Neto, Ph.D., CGEIT, CRISC

Having evaluated both at a Brazilian public sector organization, this article presents a comparison between the maturity level evaluation for the ME4 *Provide IT governance* process of the COBIT® 4.1 Monitor and Evaluate domain and the process capability assessment for the governance domain of COBIT® 5. This organization has an IT department of 81 people, structured in four main divisions—operations (including help desk and infrastructure), software development, service delivery and information management—with a US $2.5 million annual budget in 2010 (excluding staff payroll). The organization has been implementing IT governance and IT management best practices, such as a formal IT strategic committee and a project management office (PMO), since 2009, with an 85 percent increase in its IT budget in 2011 followed by a 75 percent cut in 2012.

Methods

The maturity level of the ME4 process was evaluated through self-assessment using the maturity model described in COBIT 4.1. Further, the capability assessment for the governance domain of COBIT 5 was performed using the self-assessment approach described in *COBIT® Process Assessment Model (PAM): Using COBIT® 4.1*,[1] by evaluating process outcomes for capability level 1.

Results

Using the process maturity model provided in COBIT 4.1, the public sector organization achieved maturity level 2 (repeatable but intuitive) for ME4. Nonetheless, on the more detailed vision of COBIT 5 process capability assessment, it was found that 40 percent of the evaluate, direct and monitor (EDM) governance processes were at level 0 (incomplete process), and that processes EDM02 *Ensure benefits delivery* and EDM03 *Ensure risk optimization* are the least addressed ones, as shown in **figure 1**. This is important information for decision makers that was masked in the high-level COBIT 4.1 process assessment.

Figure 1—Assessment for COBIT 5 Governance Processes

Governance Domain		Total of Outputs	N (0%-14%)	P (15%-49%)	L (50%-84%)	F (85-100%)	Results
EDM01	**Ensure Governance Framework Setting and Maintenance**	6				5	**Level 1**
EDM02	**Ensure Benefits Delivery**	6	0				**Level 0**
EDM03	**Ensure Risk Optimization**	8	1				**Level 0**
EDM04	**Ensure Resource Optimization**	8				8	**Level 1**
EDM05	**Ensure Stakeholder Transparency**	5			4		**Level 1**

Thus, there is a significant difference between these assessment models. Although they were both performed as high-level assessments, measuring capability level 1 provided more detailed information since all governance processes outcomes were explicitly gauged.

It is worth noting that the average capability level of the COBIT 5 governance processes should not be considered the global governance domain capability level in order to directly compare it to the single ME4 process. This would create a distortion as PAM was not meant to assess a domain. Instead, a safer comparison would be taking a look at the highest levels achieved using PAM and note that they are all lower than the maturity level of ME4. “In general, scores will be lower with COBIT 5 process capability model…. In the COBIT 4.1 maturity model, a process could achieve a level 1 or 2 without fully achieving all the process’s objectives; in the COBIT 5 process capability level, this will result in a lower score of 0 or 1.”[2] This was expected and empirically confirmed.

As of now, there are no publicly available benchmarks for COBIT 5 assessments; however, governance processes in level 0 are a matter of concern as fragilities in IT governance processes reflect negatively in IT performance.

Discussion

The assessments made are based on facts that were reported exclusively by IT managers, which constitute a limitation of this work as the participation of business managers would be important to ascertain the delivery of the desired outcomes. Therefore, it is possible that the IT respondents skewed toward the higher end of the scale and reported on what they wanted to or what they expected to achieve soon, as opposed to what they had actually achieved. In this scenario, governance processes at the assessed organization reached an alarmingly low level. To ascertain the validity of this hypothesis, an increase in the rigor of the assessment and the inclusion of the process practices and the work products would be necessary.

The main benefit perceived in the COBIT 5 process capability assessment was the detailed analysis of the process being evaluated, assessing whether the process achieves its goals and produces the required outcomes. Using the maturity model provided in COBIT 4.1 makes it relatively easy and fast to perform a process assessment, but it will be based on a broad consensus rather than measurable and repeatable components. COBIT 5, on the other hand, provides a process capability approach, with generic process capability attributes that use the information for the work products, base practices and process outcomes as performance indicators for capability level 1. This assessment process takes more time to carry out, and may result in a higher assessment cost, but it is more precise.

Expertise in the organization’s processes under scrutiny is required for both assessment approaches, but ISO-based methodology expertise is an additional requirement for a COBIT PAM assessment. Managers were briefed on the *COBIT 5: Enabling Processes* publication during the questionnaire application as part of the assessment process. If the respondents are beginners on the IT governance and management subject and they are not familiar with COBIT 4.1, it would not be

recommended to do such a briefing during the session, because it will demand a longer explanation time. Nevertheless, it worked just fine with skilled participants.

Conclusion

Processes are one of the seven governance and management enablers proposed in COBIT 5, and the scope of this article considered only one process from COBIT 4.1. Therefore, this type of evaluation, which is focused only on governance processes and is a limited sample, does not provide enough information to make definitive conclusions about the governance of this organization.

Nonetheless, results using the COBIT 5 PAM showed two governance processes in level 0—very useful information that the COBIT 4 model did not provide. The COBIT 4 model provides a quick scan that is not fully accurate and the COBIT 5 PAM takes more time but provides a much more precise and fact-based view of the process.

The COBIT 5 process capability assessment of the governance processes of other Brazilian federal government agencies related to the judiciary is a matter for future research.

Diana Santos, CAPM

Is chief of the information systems division at a Brazilian federal government agency related to the judiciary, and she has collaborated on IT governance and the implementation of COBIT processes. She is a member of the ISACA Brasilia (Brazil) Chapter.

Joao Souza Neto, Ph.D., CGEIT, CRISC

Has more than eight years of experience in IT governance, applying COBIT within Brazil Post. He is also responsible for the IT governance research area in the Universidade Catolica de Brasilia. He is founder and educational director of the ISACA Brasilia (Brazil) Chapter.

Endnotes

[1] The *COBIT® Process Assessment Model (PAM): Using COBIT® 5* is in development and expected to be available in first quarter 2013.

[2] ISACA, **COBIT 5**, USA, 2012, p. 43-44

Come join the discussion! Myles Suer will respond to questions in the **discussion area of the COBIT 5—Use It Effectively** topic beginning 25 January 2013.

COBIT 5 Uses Balanced Scorecard to Drive and Demonstrate Performance Improvement

By Myles Suer

COBIT® 5 should be a big deal for all practitioners of IT management. There are moments in IT management when a practitioner may feel like the Scarecrow in The Wizard of Oz who so desperately wants a brain. COBIT 5 is like adding that much-needed brain. Specifically, it adds the level of governance needed to ensure that benefits are delivered, risk is reduced, resources are optimized and, most important, stakeholder transparency is established. While the governance function does have process goals and metrics for measuring success, the most important element of driving transparency in COBIT 5 is that it embraces an updated version, compared to COBIT 4.1, of the balanced scorecard (BSC) methodology for structuring and communicating performance measurement and places it more prominently at the front of the framework in the goals cascade. This approach enables IT organizations to establish a culture of performance management and accountability.

Why Is the Balanced Scorecard Approach Important?

The original balanced scorecard was developed by David Norton and Robert Kaplan in the mid-1990s. It aimed to move

enterprises away from looking only at short-term lagging indicators, namely current period financials, in evaluating an overall enterprise performance. After all, most investors are long-term investors and, as such, are buying discount future performance as much as current performance. “According to the Balanced Scorecard Collaborative, no less than 60 percent of Fortune 500 companies use the balanced scorecard in some form.”[1] Yet, there is one enterprise department that historically has not actively managed performance to a balanced scorecard: IT. This is because IT measures integrated performance 60-120 days after the first data points were created. This needs to change for IT organizations to get a seat at the business table.

Real Time Vs. Historical View—Time Value of Information

IT organizations are operational reporting focused in a day-by-day or sometimes minute-by-minute fashion. Holistic IT measurement occurs only on a quarterly basis with the oldest data being as old as 120 days. Simply put, IT leadership can report but not manage. “Control is different than ‘reporting’ in that it implies the possibility for management intervention if things go out of control. Control implies feedback in which management is actively involved. Reporting, on the contrary, is passive. For control to be effective, therefore, data must be timely and provided at intervals that are effective for intervention.”[2]

Put even more simply, IT leaders cannot be held accountable when they do not have the information available to take corrective actions. They need to see that they are at risk of missing a goal or, if they have already missed it, they need to see how to take corrective action.

How a Balanced Scorecard Is Used With COBIT—Overall Governance Layer, Personas and Disciplines

In COBIT 5, generic scorecards have been created for the enterprise and IT as a whole. Both ask end-to-end questions about IT from a horizontal dimension. Obviously, a scorecard applied to an organization will have business- and industry-specific key performance indicators (KPIs) added. Additionally, organizations need scorecards that go after more than one IT persona or IT leadership role. Cascaded scorecards need to exist for key IT personas, such as vice president of applications, vice president of operations, chief information security officer and so on. Obviously, these need to fit the structure of the organization.

The quality of the IT disciplines also needs to be judged using the BSC framework. Scorecards may be built for numerous IT disciplines, including IT service management, project and portfolio management, quality management, automation management, and security management. In all cases, the scorecard allows IT management to show the value and improvement driven by investment in each IT discipline.

For example, in a balanced scorecard around managing service requests and incidents, one wants to measure the number and percent of incidents causing disruption to business-critical processes. This number should go down over time as things improve.

At one financial services firm after implementing a BSC like this, everything was seen to be moving in the opposite direction. In October, their incident volume was 20,000 per month, and for November through February, incident counts jumped to more than 65,000 per month—a more than threefold increase. The number of incidents that could be solved in a day dropped by 75 percent and core system failures skyrocketed. When analyzing these numbers, the firm realized that it had delivered end-of-year changes and projects as expected, but in doing so, it had brought core systems to their knees at a time (year-end) when people tend to access their money.

Why is measuring KPIs like this so important? Because COBIT 5 charges IT organizations with creating predictable quality for the solutions and services that they enable. As stated in the Manage Quality section of COBIT 5, IT organizations need to “ensure consistent delivery of solutions and services to meet the quality requirements.” The financial services firm in the previous example failed to look at the whole picture when it was managing changes and projects to their completion.

Goals and Metrics From COBIT: Extending Disciplines and Measuring Perception

COBIT 5, like COBIT 4.1 that preceded it, has the process goals and metrics for measuring all layers of the IT stack. This includes looking at the organization from the chief information officer (CIO) level to the persona to the discipline. As important, COBIT 5 focuses equally on customer perception and on analytic measurement in its selection of KPIs. At the same time, COBIT 5 creates more business-oriented measures, rather than just measuring what is easy to do from an IT tool set. In several cases, COBIT 5 extends the definitions of disciplines beyond how practitioners define them today. The best example of this is quality. When discussing quality, most people will talk about testing. However, COBIT 5 talks about services as much as it discusses projects, and it has KPIs such as the number of service level agreements (SLAs) that include quality-acceptance criteria or the number of processes with a formal quality requirement.

Measuring Customer Perception and Producer Reality

For the management of the IT portfolio, a metric of measurement is the degree to which enterprise management is satisfied with IT's contribution to enterprise strategy. Clearly, this can be measured by a survey. In the areas of quality, metrics provided are the average stakeholder satisfaction with solutions and services and the percent of stakeholders satisfied with IT quality. This means COBIT wants both reality and perception measured.

Linking IT to Business

COBIT 5, as did COBIT 4.1, challenges those in IT to move beyond tool-oriented measures to those that are oriented to the business. It is easy to measure things such as the percent of activities that are on time; however, it is harder to measure the percent of activities aligned to scope and expected outcomes. This leads to an interesting business question: Do the activities invested in actually conform to the scope and expected outcomes of stakeholders? The organization needs to verify that each investment achieves its specified business goal.

Extended Definitions of Disciplines

For most people in the software business and within IT shops, quality equals testing. However, in manufacturing, for example, this is not the case. In IT, there is a hard silo wall between development and operations. COBIT 5 defines quality as the process that aims to define and communicate quality requirements for all processes, procedures and related outcomes. This includes controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts. This makes the wall between development and operations artificial. In fact, the first goal shown for quality is that stakeholders are satisfied with the quality of solutions and services. Three COBIT 5 metrics are used to measure success of this goal: average stakeholder satisfaction with solutions and services, percent of stakeholders satisfied with IT quality, and number of services with a formal quality management plan. This definition of quality is very different from most people's concept of quality in software development or IT management.

Conclusion

COBIT 5 is a great starting point for any organization and maturity level. While it is comprehensive and demanding at the highest level of maturity, it does not preclude one from starting by measuring what is easiest to measure. An organization can simply create a scorecard and start to improve. For its part, COBIT provides an easily navigated yet exhaustive set of goals that can be measured in flight for any state of maturity. It gives users the ability to consider where they want to go and how they will measure to get there.

Myles Suer

Is a senior manager at HP for IT performance management. In this capacity, he works with customers and partners on their performance management needs. Prior to this, Suer headed the product management team responsible for HP's IT Financial Management and Executive Scorecard products. This included interviewing chief information officers (CIOs) regarding their needs around balanced scorecard requirements. He has 20 years of experience leading new product initiatives at start-ups and large companies. He is also adjunct faculty at the John Sperling School of Business at the University of Phoenix (Arizona, USA).

Endnotes

[1] de Koning, Guido M.J.; "**Making the Balanced Scorecard Work (Part 1)**", *Gallup Business Journal*

[2] Abell, Derek; *Managing With Dual Strategies*, The Free Press, 1993, p. 275

The COBIT Assessment Programme—COBIT 5-based Guidance Coming Soon

By Steven Babb, CGEIT, CRISC

The COBIT® Assessment Programme is a COBIT-based approach that enables the evaluation of select IT processes. The assessment results provide a determination of process capability and can be used for process improvement, delivering value to the business, supporting the achievement of current or projected business goals, providing consistent reporting, and

enhancing organizational compliance.

Later this quarter, ISACA® will issue new publications to support the assessment of enterprise IT-related processes as defined in COBIT 5. There will be three volumes: *COBIT® Process Assessment Model (PAM): Using COBIT® 5*, *COBIT® Assessor Guide: Using COBIT® 5* and *COBIT® Self-assessment Guide: Using COBIT® 5.*

These volumes add to the guidance already available to support such assessments using the **COBIT® 4.1 process reference model**.

COBIT PAM has been reworked to incorporate the relevant process materials from *COBIT® 5: Enabling Processes*. The *Assessor Guide* has been enhanced to provide additional guidance on the available assessments using this approach and the value they deliver to the enterprise, as well as to enable those applying the approach to better understand and communicate effectively the limitations and potential expectation gap risk of the approach to the assessment sponsor.

In addition, ISACA is working to develop and deliver related training that will lead to a certification in performing COBIT 5-based assessments using this approach. Since the approach stresses the need for competent assessors, such a certification will support assessment sponsors in identifying competent assessors. More news will be available regarding this new opportunity soon.

Finally, having established a market capability for COBIT-based process capability assessments, in 2013, ISACA will examine market needs and opportunities to establish a COBIT-based enterprise certificate similar to other enterprise certifications (e.g., the CMMI SCAMPI, AICPA HITRUST assessment, ISO standards compliance reports). Further details will be announced once plans have been confirmed.

Steven Babb, CGEIT, CRISC

Is head of information and technology risk for Betfair, one of the world's largest international online sports betting providers. Babb manages a team of security and risk professionals covering Australia, Europe and the US. Prior to this, he was head of technology risk in the UK practice of KPMG's Risk Consulting team. He has more than 16 years of consulting and assurance experience covering areas such as information systems governance, IT risk and control, service management, and programme and project management, gained across the public and private sectors. Babb chairs ISACA's Framework Committee and the COBIT for Risk Task Force, sits on the Knowledge Board, and previously was a member of ISACA's Risk IT and COBIT 5 task forces.

Come join the discussion! Yuichi (Rich) Inaba and Hiroyuki Shibuya will respond to questions in the **discussion area of the COBIT (4.1 and earlier)—Use It Effectively** topic beginning 25 January 2013.

Executive Management Must Establish IT Governance: Tokio Marine Group

By Yuichi (Rich) Inaba, CISA, and Hiroyuki Shibuya

Tokio Marine Group is a global corporate group engaged in a wide variety of insurance businesses. It consists of about 70 companies on five continents, including Tokio Marine and Nichido Fire Insurance (Japan), Philadelphia Insurance (US), Kiln (UK) and Tokio Marine Asia (Singapore).

In addition to Tokio Marine and Nichido Fire Insurance, which is the largest property and casualty insurance company in Japan, Tokio Marine Group has several other domestic companies in Japan, such as Tokio Marine and Nichido Life Insurance Co. Ltd, as well as service providers, such as Tokio Marine and Nichido Medical Service Co. Ltd. and Tokio Marine and Nichido Facilities Inc.

Implementing IT Governance at Tokio Marine Group

Tokio Marine Holdings, which is responsible for establishing the group's IT governance approach, observed that the executive management of Tokio Marine Group companies believes that IT is an essential infrastructure for business management, and it hoped to strengthen company management by utilizing IT. However, some directors and executives had a negative impression of IT—that IT is difficult to understand, costs too much, and results in frequent system troubles and system development failures.

It is common for an organization's executive management to recognize the importance of system development but to put its development solely on the shoulders of the IT department. Other executives go even further, saying that the management or governance of IT is not anyone's business but the IT department's or chief information officer's (CIO's). This line of thinking around IT is similar to the thought process that accounting is the job of the accounting department and handling personnel affairs is the role of the human resources department.

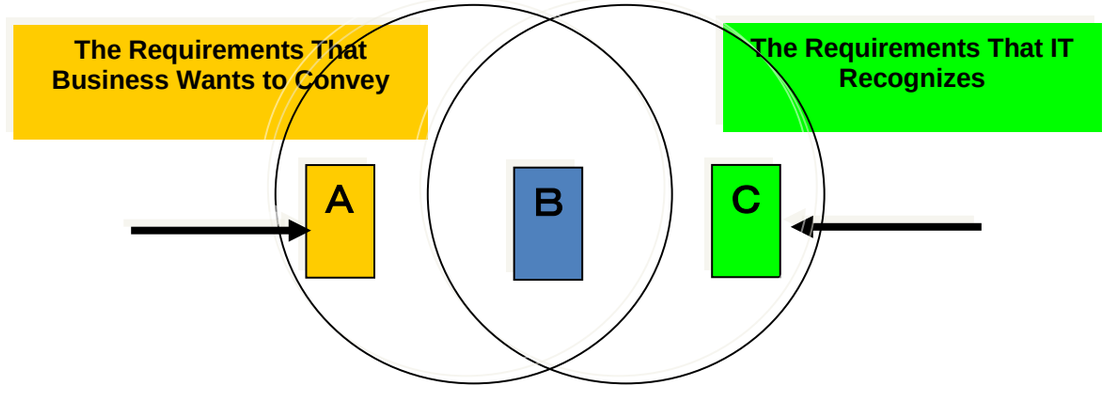
These are typical behaviors of organizations that fail to implement IT governance systems. Tokio Marine Holdings' executive management recognized that IT is not for IT's sake alone, but is a tool to strengthen business.

Tokio Marine Holdings' management recognized that there were various types of system development failures (e.g., development delays for the service-in date, projects being over budget). Even more frequently, the organization was finding requirement gaps—for instance, where after building a system, the business people say, "This is not the system that we asked you to build" or "The system that you built is not easy to use. It is useless for the business."

Why the Requirement Gaps Occur

The process of system development is similar to that of a building's construction. However, there is a distinct difference between the two: system development is not visible, whereas building construction is. Therefore, in system development, it is inevitable that there are recognition and communication gaps between business and IT (**figure 1**).

Figure 1—The Requirement Gap



Tokio Marine Group's Solution for System Development Success

To fill these gaps, business and IT must communicate enough to minimize the gaps of A and C in **figure 1** and maximize a common understanding of B. The road to success for system development is to improve the quality of communication between business and IT.

Such communication cannot be reached or maintained in a one-sided relationship. Ideal communication is enabled only with an equal partnership between business and IT with appropriate roles and responsibilities mutually allocated.

This is the core concept of Tokio Marine Group's Application Owner System.

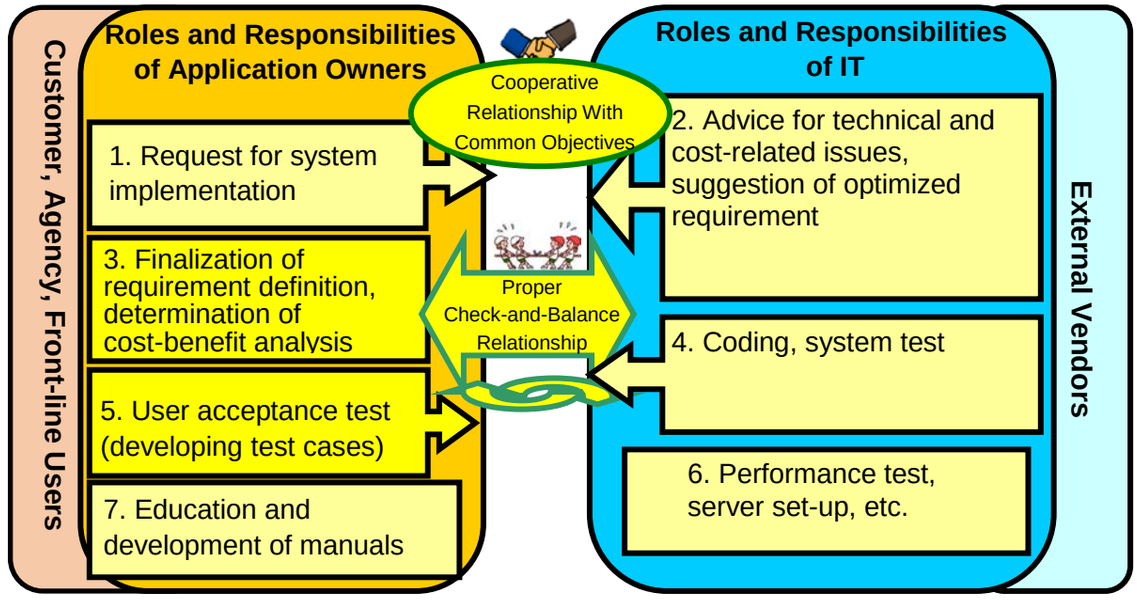
Implementing the Application Owner System

Tokio Marine Holdings decided to implement the Application Owner System as a core concept of the Group IT Governance System. Tokio Marine Holdings believes it is essential for the group companies to succeed in system development and to achieve the group's growth in the current business environment.

The basic idea of the Application Owner System (**figure 2**) is:

- Mutual cooperation between business and IT with proper check-and-balance functions, appropriately allocated responsibilities and shared objectives
- Close communication between business and IT, each taking their own respective roles and responsibilities into account

Figure 2—The Application Owner System in Tokio Marine Group

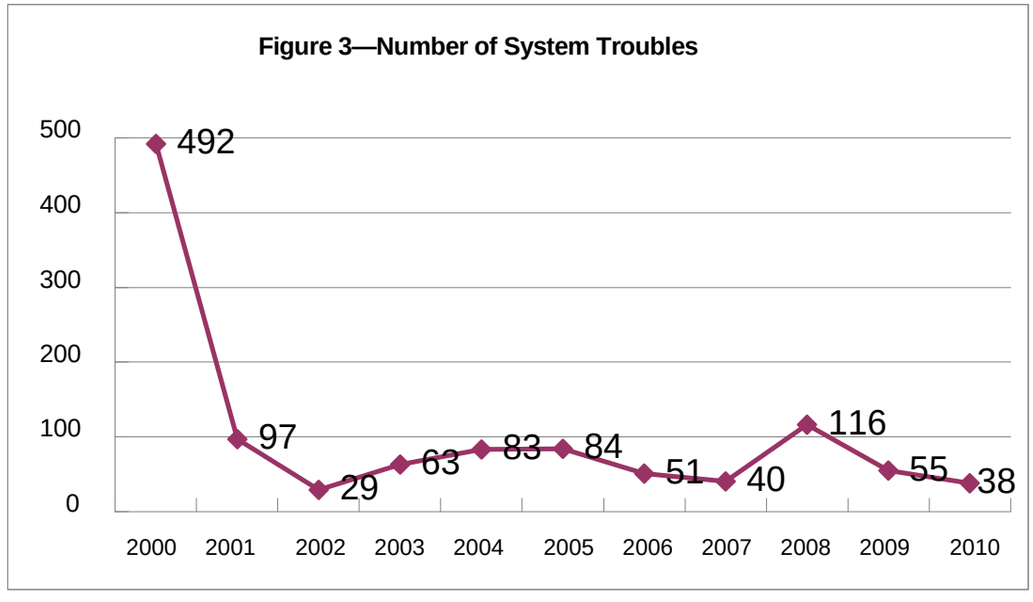


Early Success in Tokio Marine and Nichido Fire Insurance

Tokio Marine and Nichido Fire Insurance Co. Ltd., the largest group company, implemented the Application Owner System in 2000. Implementation of the Application Owner System immediately reduced system troubles and problems by 80 percent (**figure 3**).

Tokio Marine Group is now implementing the system across the group companies.

Figure 3—Number of System Troubles



Mind-set of IT

Tokio Marine's mind-set is that only executive management can establish the enterprise's IT governance system. Thus, IT governance is the responsibility of executive management.

Furthermore, the organization is of the mind-set that all employees, not only executive management, should understand the principle that strong IT systems cannot be realized by the IT department alone but require cooperation between business and IT. It is important that all employees recognize IT matters as their own, not as the matter of the IT function.

Establishing such a mind-set within the enterprise is a role of executive management.

Tokio Marine Group's IT Governance System

Characterized by the Application Owner System, Tokio Marine Holdings has introduced an IT governance framework, focused on the COBIT 4.1 framework, specifically the Plan and Organize (PO) domain.

The main goals of the IT governance framework are:

- **Establishing basic policies for IT governance**—Tokio Marine Holdings established the Basic Policies for IT Governance as the policies for the group's IT governance framework.
- **Establishing guiding principles for IT governance**—Tokio Marine Holdings defines seven principles as the guiding principles (**figure 4**). These cover the five focus areas defined in the *Board Briefing on IT Governance*, particularly focusing on strategic alignment and value delivery. The seven principles are included in the Basic Policies for IT Governance. Tokio Marine Holdings thinks that the most important principle is the Application Owner System, which is stated as follows:

  > *In implementing the plan, it is important for the IT unit and the application owner units to cooperate with each other with proper check-and-balance functions. Management shall clearly determine the appropriate sharing of roles between the IT unit and application owner units, secure human resources of adequate quality in both units, and establish a management system to assure that each unit will execute the plan according to its responsibilities.*

Figure 4—Seven Guiding Principles

No.	Guiding Principle (Summary)	Focus Area
1	Establish an IT strategic plan that enables management to achieve its business strategic plan, build the business processes for it, and develop an execution plan.	Strategic Alignment
2	In executing the plan, ensure that the IT unit and the application owner units cooperate with each other with proper check-and-balance functions.	Strategic Alignment
3	In the development or implementation of information systems, ensure that management scrutinizes the validity of the project plan from the standpoint of quality assurance, usability, commitment to service-in date, appropriate cost estimation and matching to the human resources availability.	Value Delivery
4	Ensure that the information systems are fully utilized by all staff in the company in order to achieve the objectives for the development or implementation of the information systems.	Value Delivery
5	Conduct appropriate IT resource management, including computer capacity management and human resources management.	Resource Management
6	Conduct appropriate risk management and information security management, and establish contingency plans for system faults in consideration of the accumulation of various risk factors in IT, such as high dependency of business processes on IT, centralization of important information and threats from wider use of the Internet.	Risk Management
7	Encourage the transparency of IT operations to be improved, and monitor their progress, which includes, for example, the progress of projects, the usage of IT resources and utilization of information systems.	Performance Measurement

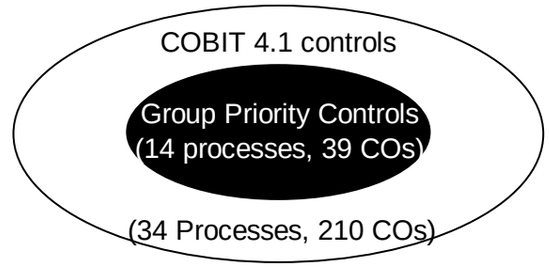
- **Establishing a governance and management system for Tokio Marine Group**—Tokio Marine Holdings defines the governance and management system to be implemented in the group companies. It covers five domains and consists of

three major components: establishment of the organizational structure, establishment of policies and standards, and execution of the plan, do, check and act (PDCA) cycle for improvement. The governance and management system required for Tokio Marine Group companies is detailed in the Group IT Governance Standard.

- **Establishing an IT governance standard** (the definition of Tokio Marine's priority processes)—Tokio Marine Holdings has decided to utilize COBIT 4.1 to define the management system. However, the organization recognizes that it is difficult for relatively small group companies to implement matured processes for all 34 COBIT 4.1 processes. To handle this concern, the organization focused on the minimal set of processes or more detailed control objectives, which are essential for its group business in terms of IT governance and the most important controls for Tokio Marine Group.

In the IT Governance Standard, Tokio Marine Holdings defined the IT controls outlined in **figure 5** as priority for the Tokio Marine Group. The priority IT controls are defined as five domains,14 processes and 39 control objectives, which are selected processes from the 210 control objectives of COBIT 4.1.

Figure 5—Tokio Marine Group's Priority Controls



	Domain Name	Id	Process Name
a.	Planning and organization	a1	Annual IT planning
		a2	Definitions of roles and responsibilities of the IT unit and application owner units
		a3	Establishment of an IT steering committee
b.	Projects management	b1	Management of development and implementation projects
c.	Change management	c1	Change control
d.	Operations management	d1	Incident/problem management
		d2	Vendor management
		d3	Security management
		d4	IT asset management
		d5	Computer capacity management
		d6	Disaster recovery and backup/restore
e.	Monitoring performance and return on investment	e1	Annual IT review
		e2	Monitoring the IT steering committee
		e3	Monitoring project management, change management, and systems operation management

The group companies are required to improve the priority controls to reach a maturity level 3, according the COBIT Maturity Model, and report the progress of improvements to Tokio Marine Holdings.

Toward the Future

Since the establishment of the IT governance system for Tokio Marine Group, Tokio Marine Holdings has extensively communicated not only with the CIOs but also with chief executive officers (CEOs) and executive management of the group companies to ensure that they understand, agree on and take leadership for IT governance implementation.

Through these activities, the organization is confident that the core concept of IT governance has become better understood by management and good progress is being made as a result of the implementation of the application owner system in group companies. Tokio Marine Holdings will continue its evangelist mission to the group companies, realizing the benefit for the group business and giving value to stakeholders.

Yuichi (Rich) Inaba, CISA

Is a senior consultant specialist in the area of IT governance, IT risk management and IT information security in the Tokio Marine and Nichido Systems Co. Ltd. (TMNS), a Tokio Marine Group company. Before transferring to TMNS, he had worked in the IT Planning Dept. of Tokio Marine Holdings Inc. and had engaged in establishing Tokio Marine Group's IT governance framework based on COBIT 4.1. His current responsibility is to implement and practice Tokio Marine Group's IT governance

at TMNS. Inaba is a member of the ISACA Tokyo Chapter's Standards Committee and is currently engaged in translating COBIT 5 publications into Japanese.

Hiroyuki Shibuya

Is an executive officer in charge of IT at Tokio Marine Holdings Inc. From 2000-2005, he led the innovation project from the IT side, which has totally reconstructed the insurance product lines, their business processes and the information systems of Tokio Marine and Nichido Fire Insurance Co. Ltd. To leverage his experience from this project as well as remediate other troubled development projects of group companies, he was named the general manager of the newly established IT planning department at Tokio Marine Holdings in July 2010. Since then, he has been leading the efforts to establish IT governance basic policies and standards and to strengthen IT governance throughout the Tokio Marine Group.

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.