COBIT® Focus

Volume 2, April 2013

In This Issue:

Use of COBIT 5 for ISACA Strategy Implementation—A Case Study Excerpt

In 2009, ISACA® developed a strategy focused on becoming the global leader in products and services that support trust in, and value from, information systems. By 2011, having accomplished many of the 2009 goals, ISACA began work on an extension of the 2009 strategy, resulting in an expanded focus on extending ISACA's global leadership in educating and informing individuals and enterprises on the topic of trust in information and information systems. In recognition of the strategy's 10-year horizon for completion, it is referred to as Strategy 2022, or S22, for short.

The strategic aspiration is underpinned by a series of more than 20 initiatives designed to help the association achieve its goals through creating or adapting knowledge, supported by practical guidance, education programs, online opportunities and a variety of other resources. The planned activities are expected to provide valuable products and services for core constituents, while also reaching a bit farther outside that core to make others aware of the importance of embedding trust concepts at all points of the information and information systems life cycle.

The initiatives are ambitious and complex, and contain numerous dependencies. They represent a prime opportunity—and need—for effective governance and management, with special focus on resource optimization, risk mitigation and benefit delivery. ISACA, as the developer of COBIT® 5, became convinced that COBIT's commonsense, business-oriented approach to governance and management would help in addressing the far-ranging and interrelated strategy-specific activities necessary to achieve its aspirational goals. The COBIT 5 framework provided the conceptual underpinning and *COBIT® 5 Implementation* offered the practical guidance for putting plans into execution.

Why COBIT 5?

One of COBIT's strengths, since its first edition, issued in 1995, is its flexibility. It not only accommodates customization to fit the user's needs, it encourages it. Therefore, it easily lent itself to ISACA's planned usage, which did not focus on IT, COBIT's more common milieu. Instead, ISACA's intent was to utilize COBIT® to ensure that the strategic initiatives were undertaken in such a way as to enable the goals cascade, i.e., that the needs of stakeholders (members, certification holders, others in IT trust professions, and enterprises that are dependent on IT, among others) were reflected in appropriate organizational goals, the achievement of which would be enabled by

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 3, 2013: 10 June 2013

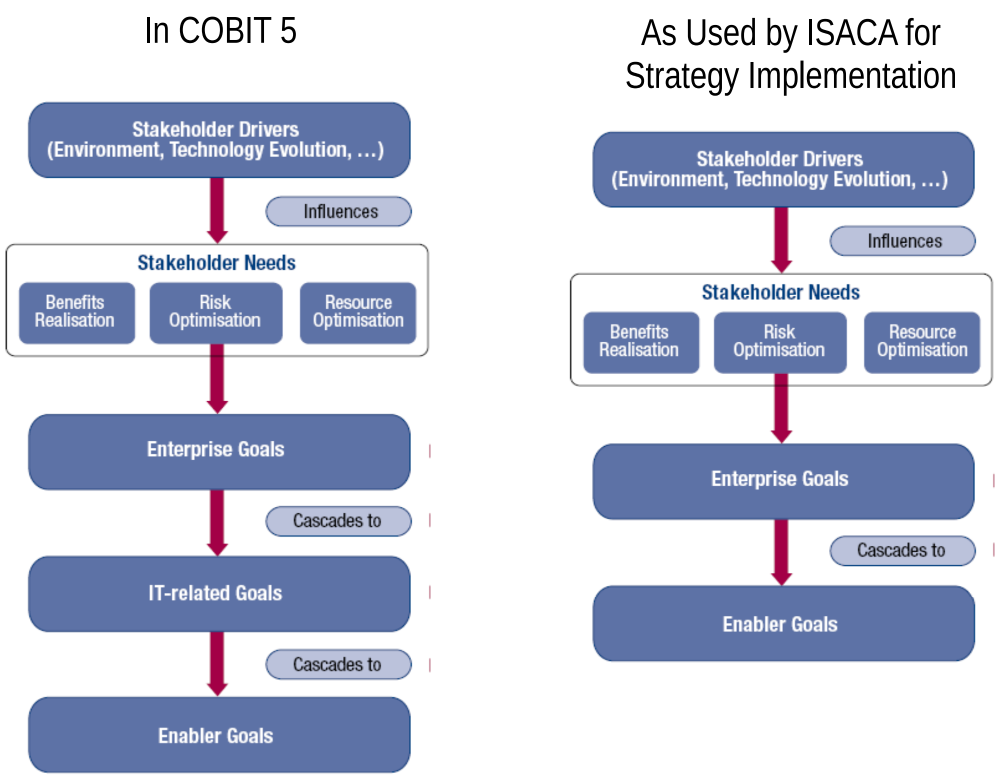
Submit articles for peer review to: publication@isaca.org

Case Studies

Visit the **COBIT Recognition** and **Case Studies** pages to read more COBIT 5 and COBIT 4.1 case studies.

achievement of the goals of the entire strategic portfolio, which in turn would be supported by achieving individual initiative goals. The goals cascade shown in **figure 1** is the COBIT 5 cascade; for purposes of this project, ISACA did not address the IT-related goals, as COBIT 5 was not being applied to an IT project.

Figure 1—COBIT 5 Goals Cascade



Source: COBIT 5

Based on COBIT's methodology, ISACA expected that the use of COBIT would address many challenges inherent in the implementation of the strategy:

- It would help to identify and clarify dependencies among initiatives.
- It would ensure a consistent approach to executing the tactics required to achieve the strategic objectives.
- It would "force" thinking through the issues surrounding each initiative in a logical, reasoned and methodical way, and taking a holistic view resulting from consideration of the seven enablers.
- It would help to establish the scope for each initiative—especially important in ISACA's "try to do all things for all people" culture.
- It would help ensure wise and unified use of limited resources.
- It would help to recognize risk on a timely basis, so it could be mitigated, and it would help ensure realization of the value anticipated from the project.
- It would support the identification of stakeholders, and the subsequent development and implementation of sound value proposition for each, in a coherent way.

Although ISACA is the organization responsible for COBIT's development and continued enhancement, that work is carried out by ISACA volunteer members. Therefore, while the staff members who worked with the volunteers on the COBIT development projects were intimately familiar with COBIT's concepts, most staff was not. In other words, ISACA came to a COBIT implementation as would any typical small to medium enterprise, facing a similar degree of understanding, challenges and questions. It quickly became clear that a first step would need to be building a level of COBIT understanding among staff, so that its general concepts could be applied to specific strategic activities.

Getting Started

Training

The need for training to support the initial baseline activities was identified early in the process. Each of the strategy's 24 initiatives was managed by a staff team representing various functional areas (e.g., research, finance, certification, marketing/communications, membership) that would be needed to deliver on the purpose of the initiative. Therefore, the initiative team leaders were treated to a training session conducted by one of the staff COBIT experts.

The training covered the basics of COBIT 5—principles, enablers, goals cascade, etc.—and then addressed COBIT 5 as applied to ISACA strategy. Considerable discussion took place about the identity and roles of ISACA stakeholders. It was concluded that the most succinct way to identify them was to determine who bears the risk, who gets the benefit and who provides/is a resource.

Project Management

Typical of any enterprise implementing COBIT, ISACA began its application of COBIT concepts to strategy execution in midstream. Very few enterprises have the luxury of using COBIT at the beginning of an entirely new project, applying COBIT concepts from the outset. ISACA was no different. Some work had already begun on outlining and scheduling tasks necessary to progress the initiatives. A project management resource had been added to staff to help organize the portfolio and program and schedule each project, and various schedules, timelines and stage-gates had already been established. One of the tasks that had to be included in applying COBIT to each initiative was incorporation, accommodation and/or revision of already-existing project plans.

Setting Up Teams

This case study has mentioned the creation of teams for the purpose of ensuring effective implementation of S22. It was recognized that the teams that arose on somewhat of an *ad hoc* basis, or the individuals assigned specific responsibilities, needed to be formalized, with clear roles and responsibilities assigned.

Governance

Before the teams could begin work in earnest, some governance issues arose that had not heretofore been articulated or addressed. Among these—specifically, the monitoring activity—was how to report properly. Governance cannot effectively monitor without the information provided in succinct, pertinent reports. COBIT 5 does not prescribe how to report, so it was necessary to develop a process that served the needs of the ISACA Board of Directors and the Strategic Advisory Council (SAC). Templates were created for each group. Both templates are considered "living documents" and will undoubtedly undergo revision as lessons are learned about reporting needs and preferences.

Conclusion

To learn more details about the initial steps and implementation process, read the full case study ***COBIT Case Study: Use of COBIT 5 for ISACA Strategy Implementation*** on the ISACA web site.

The work to use COBIT 5 as a strategy implementation tool goes on—in keeping with S22's 10-year horizon. Now that the first governance review has taken place for each initiative, progress on the remaining phases will continue and tangible results are expected to ensue. Measures will be developed to gauge achievement against objectives, and monitoring will be maintained.

There is no question among those working on the S22 initiatives that using COBIT 5 has enabled a more productive outcome to date. The rigor required by starting with defining stakeholders, their drivers and their needs, then proceeding to describe the as-is and to-be states, has sparked a deeper analysis of each initiative.

Based on the success of using COBIT to implement strategy, ISACA is applying COBIT 5 to other specific activities as well. Gradually, the intent is to expand COBIT's scope to cover broader enterprise issues. After years of developing COBIT, writing about it, offering education and training on it, and incorporating it into certifications, ISACA has found it a rare privilege to apply it to the association's own environment.

COBIT 5: Enabling Information Progress Report, Part 2

By Steven De Haes, Ph.D.

The project to develop the *COBIT® 5: Enabling Information* publication to extend the COBIT® 5 family of products was approved by the ISACA® Board of Directors in 2012. This project progressed during 2012 and into 2013 under the direction of a task force that is guided by the ISACA Framework Committee and Knowledge Board. This task force organized multiple development workshops to build new expertise around this knowledge area.

The objective of the project is to create an innovative reference guide for the information enabler for governance and management of enterprise IT (GEIT). This guide will further explain the information model included in COBIT 5 (based on the generic enabler model) and provide some examples of fully elaborated information entities (e.g., customer data, IT strategic plan). The guide will be the information equivalent of the *COBIT® 5: Enabling Processes* publication.

Proposed content includes:

- A definition of information management and information governance
- Elaboration of the COBIT 5 goals cascade, expanding on the information enabler goals
- Explanation of the COBIT 5-based information model with examples
- Several examples for applying the COBIT 5 information enabler model to information governance and management issues (e.g., big data)

The next step in the development plan is a subject matter expert review, which is expected to begin before the end of April 2013. The publication is anticipated for release in early third quarter 2013.

Steven De Haes, Ph.D.

Is associate professor information systems management at the University of Antwerp—Faculty of Applied Economics and at the Antwerp Management School. He is actively engaged in teaching and applied research in the domains of IT governance, IT strategy, IT performance management, IT management, IT assurance, IT business value and strategic alignment. He was a member of ISACA's COBIT 5 Task Force and serves as the chair of the Information Reference Model Task Force.

Research Update

Recently Released COBIT 5 Materials

- ***COBIT® Process Assessment Model: Using COBIT® 5***
- ***COBIT® Assessor Guide: Using COBIT®* 5 and Tool Kit**
- ***COBIT® Self-assessment Guide: Using COBIT® 5* and Tool Kit**

Upcoming Second Quarter 2013 COBIT 5 Releases

- *COBIT 5 for Assurance*
- COBIT 5 Assessor-level Training and Certificate
- COBIT 5 Implementation-level Training and Certificate

Additional COBIT 5 Initiatives in Development

- *COBIT 5: Enabling Information*
- *COBIT 5 for Risk*
- COBIT 5 Online

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

Come join the discussion! Jeff Curtis will respond to questions in the discussion area of the COBIT (4.1 and earlier)—Use It Effectively topic beginning 22 April 2013.

Sunnybrook Health Sciences Centre Case Study

By Jeff Curtis, CISSP

Sunnybrook Health Sciences Centre (Toronto, Ontario, Canada) is one of the largest academic teaching hospitals in Canada. Its 10,000 staff, physicians and volunteers provide care to more than one million patients each year. Over the past 60 years, Sunnybrook has evolved from its original role as a veterans' hospital into a centre for acute patient care, education and research. Today, it specialises in caring for Canada's war veterans; high-risk pregnancies; critically ill newborns, adults and elderly; and treating and preventing cancer, cardiovascular disease, neurological disorders, orthopaedic and arthritic conditions, and traumatic injuries. Sunnybrook is fully affiliated with the University of Toronto and provides learning opportunities for more than 2,000 students annually. As a research-focused hospital, each year Sunnybrook's 600-plus scientists conduct CAN $100 million of breakthrough research.

Sunnybrook's Need for IT Governance

IT governance is an integral part of enterprise governance and consists of the leadership, organisational structures and processes that ensure that Sunnybrook's information services group sustains and extends Sunnybrook's enterprise strategies and objectives. At an annual IT planning retreat, Sunnybrook's chief information officer (CIO) expressed the need for increased focus on technical and process risk management within the IT management team following several years of increasing operations, project incidents and disruptions. At the same time, the CIO was being asked to present IT value and risk management activities to the audit committee of the board.

The audit committee had been previously unaware that a standards-based governance framework existed specifically for IT and was, therefore, immediately supportive of the IT governance programme proposal because it aligned with the emerging corporate enterprise risk management (ERM) and value-focusing efforts for hospital clinical care delivery. Members of IT management also appreciated the opportunity to structure, define and measure value and risk considerations within their respective IT strategic programmes, recognising that they could not commit to every project request going forward and were increasingly managing and competing for limited development resources.

An IT governance programme was, therefore, formally introduced as one of five IT strategic goals in Sunnybrook's 2012 IT Strategic Plan (**figure 1**).

Figure 1—Sunnybrook Information Services Strategic Goals

Goal 1: Sunnybrook will be the national leader in the development of personal health records through expansion of the MyChart^{TM} programme.[1]

Goal 2: Sunnybrook will lead in the design and build of innovative health care solutions.

Goal 3: Sunnybrook will use information systems and technologies to improve the integration of care across health care providers.

Goal 4: Sunnybrook will lead in the development of real-time information management tools and implement clinical data warehouses for health services research.

Goal 5: Sunnybrook will implement an IT governance framework.

The strategic goals correspond to three resulting IT strategic programmes, with director accountability for each programme's value and risk performance: MyChart (Sunnybrook's personal health record), SunnyCare (its next generation, in-house developed clinical management system) and the information management programme (providing real-time data management dashboards and reporting). Each of these programmes is required to account for corporate value and risk management within

Sunnybrook's IT balanced scorecard.

Sunnybrook's IT governance framework is based on COBIT® 4.1, a core set of managerial-level IT process controls, combined with two complementary enterprise-level IT governance frameworks:

- **COBIT 4.1** provides the essential managerial process control framework for day-to-day IT service creation and delivery.
- **Risk IT** provides risk assessment and risk mitigation across all IT services.
- **Val IT™** provides IT project, programme and portfolio value management objectives and controls.

These three ISACA frameworks[2] combine to provide an overall IT governance programme that is fully complementary with existing best practices for IT service delivery and provides both managerial and board-level visibility and control over the performance of Sunnybrook's IT strategic programmes.

Sunnybrook's IT Governance Areas of Focus and Balanced Scorecard Development

Whether at the management or board level, IT governance is fundamentally concerned with two primary outcomes: IT value delivery and the mitigation of IT-related risk. These are enabled by ensuring the strategic alignment of IT services with Sunnybrook's business goals, the availability and management of appropriate IT resources, and the measurement and management of IT process performance. The resulting IT governance programme is focused on the application of five governance areas that are common to all enterprise governance frameworks and are applied to Sunnybrook's IT management, specifically:

1. **Strategic alignment**—Ensuring linkage between Sunnybrook's corporate and IT strategic plans
2. **Value delivery**—Ensuring information services' value proposition throughout the IT delivery cycle and across IT programmes, projects and operational areas
3. **Risk management**—Ensuring risk awareness and active mitigation of risk by senior corporate officers and IT management
4. **Resource management**—Ensuring optimal investment in, and the proper management of, critical IT resources
5. **Performance measurement**—Monitoring the achievement of IT strategic goals and objectives including value and risk management, project completion and success, IT resource usage, and IT process performance and service delivery, using balanced scorecards that translate strategy into action

For performance reporting purposes, these areas of focus have been translated into a four-quadrant IT balanced scorecard that is reportable to the board and is composed of selected IT objectives and associated process and outcome measures, which reflect the IT governance goals for each quadrant:

1. **Corporate perspective:** Delivering value and managing risk
2. **Learning and growth perspective:** Ensuring IT sustainability
3. **Internal (operations) perspective:** Achieving operational excellence
4. **Customer perspective:** Exceeding customer expectations

The measurement and management of the associated IT balanced scorecard indicators ensure visibility and accountability for both the IT strategic programme and the operational goals and objectives.

One of the most challenging issues in developing the balanced scorecard has been selecting indicators for quadrant 1, the *corporate perspective*, where value and risk indicators should be reflective of enterprise health care delivery goals and objectives. In consultation with senior clinicians and information systems directors, for example, work has begun on a number of indicators that reflect value delivery in terms of clinical management system access, efficiency, effectiveness, client centredness and safety.[3] These clinical value dimensions are appropriate in a hospital setting where IT's core purpose is to ensure that IT systems deliver information to patients, clinicians and managers where and when it matters most.

The following are samples of the resultant value indicators applicable to SunnyCare. Management discussion is underway regarding the best way to measure certain indicators where, for example, clinical effectiveness or efficiency outcomes may not be directly observable without significant commitment and support for data gathering. Other value indicators reflective of patient and administrative value dimensions are also in development for both the MyChart and information management programmes, respectively.

SunnyCare clinical value dimensions are:

- **Access:** Reducing waits and sometimes harmful delays for both those who receive and those who give care; *key indicators:* number of unique users; number of clinical programmes with active users
- **Efficiency:**[4] Minimising waste, including waste of time, equipment, supplies, ideas and energy; *key indicators:* user

survey results reflecting clinician efficiency improvements
- **Effectiveness:** Providing services based on scientific knowledge to all who can benefit, and refraining from providing services to those not likely to benefit; *key indicators:* in development
- **Client centredness:** Providing a product that is respectful of and responsive to client preferences, needs and values, and ensuring that client values guide all design decisions; *key indicators:* client usability and satisfaction scores
- **Safety:** Avoiding injuries to patients from the care that is intended to help them (Safety value can be realized by reducing errors that have the potential to cause harm.); *key indicators:* in development

Sunnybrook is committed to developing and measuring these indicators for the next year of its IT governance programme implementation in order to assess the feasibility of further refining and building similar measures for all IT strategic programmes and services going forward. As noted, the need for value and risk measurement has prompted much discussion regarding the feasibility of measurement and the meaningfulness of the resulting indicators. These are ongoing discussions that are continuing to refine Sunnybrook's balanced scorecard as the organisation goes forward. Through the promotion and use of an IT balanced scorecard, the audit committee has commended the IT group for its introduction of the COBIT framework and for, thereby, putting IT on the measurement track to ensure value and risk visibility for both the board and management.

Jeff Curtis, CISSP

Is the chief privacy officer (CPO) for Sunnybrook Health Sciences Centre (*www.sunnybrook.ca)*, a 10,000-plus employee acute care, research and teaching hospital in Toronto, Ontario, Canada. Curtis is a director in the hospital's information services group responsible for information privacy assurance, freedom of information compliance, IT risk management and corporate strategic planning activities. He has worked in the information technology sector for the past 20 years and is a doctoral candidate undertaking his DBA in information security research at the Henley Business School, University of Reading, UK.

Endnotes

[1] **www.mychart.ca**

[2] In 2012, ISACA released COBIT® 5, in which the Risk IT and Val IT frameworks are now included.

[3] Adopted from National Research Council, 'Crossing the Quality Chasm: A New Health System for the 21st Century', The National Academies Press, USA, 2001

[4] Etchells, E.; M. Slessarev; T. MacMillan; The Effects of Duplication of Redundant Information Between Paper and Electronic Records on Efficiency, Document Completeness, Safety and User Satisfaction of General Internal Medicine Admission and Discharge Processes, working paper, 2012

How COBIT 5 and ITAF Relate

By Anthony Noble, CISA, and Ian Sanderson, CISA, CRISC, FCA

The IT Assurance Framework™ (ITAF™) from ISACA® is a comprehensive and good-practice-setting IS audit and assurance model that:
- Organizes standards that address the IS audit and assurance professional's roles and responsibilities, knowledge and skills, and audit performance and audit reporting requirements
- Defines terms and concepts specific to IS audit and assurance engagements
- Provides guidance to help the IS audit and assurance professional implement the standards

ITAF provides a single reference source through which IS audit and assurance professionals can find standards and guidance, research policies and procedures, identify relevant audit and assurance programs, and develop effective reports. The ISACA IS Audit and Assurance Standards that form the basis of the ITAF guidance were updated and subjected to public exposure in late 2012, resulting in feedback from more than 1,100 contributors. The updated standards will be made available in June 2013 and effective September 2013. The IS Audit and Assurance Guidelines, which help users to apply the standards, are currently being revised and updated with public exposure planned as the updates are completed.

While ITAF organizes the ISACA IS Audit and Assurance Standards and Guidelines, it has been designed to be a living framework. As new standards and guidelines are developed and issued, they will be indexed within the framework and made available to ISACA members.

The ITAF Standards are categorized into:

- 1000—General standards (e.g., Professional Independence, Audit Charter, Proficiency)
- 1200—Performance standards (e.g., Planning and Supervision, Audit Materiality, Audit Evidence)
- 1400—Reporting standards (e.g., Reporting, Follow-up Activities)

The ITAF Guidelines directly support the standards and are categorized into three related series:

- 2000—Guidelines supporting general standards
- 2200—Guidelines supporting performance standards
- 2400—Guidelines supporting reporting standards

The ITAF Tools and Techniques provide additional examples an assurance professional could follow when performing IT assurance work. The Tools and Techniques are not contained directly in the electronic ITAF document, but are referenced online to ensure that the IS audit and assurance professional utilizes the most current ISACA guidance. Tools and Techniques include:

- Reference series (books)
- Audit programs
- White papers
- *ISACA® Journal* articles

Additional Tools and Techniques are in development.

The COBIT® 5 framework scope encompasses assurance activities—related to all of the seven governance and management enablers—within it, as appropriate. These include management assurance or self-assessment activities and arrangements, as well as those focused on ITAF, that relate to independent assurance functions such as internal audit, external audit or other assurance providers following professional standards. Management's monitoring of controls is relevant to most activities within COBIT 5 while the independent assurance activities are focused on the Monitor, Evaluate and Assess (MEA) processes domain.

The newly refreshed ISACA IS Audit and Assurance Standards and Guidelines referenced in the updated ITAF have been mapped to the relevant COBIT 5 framework components in the upcoming *COBIT® 5 for Assurance*.

The *COBIT 5 for Assurance* publication will provide valuable guidance to IS audit and assurance professionals in two key areas: how to use the COBIT 5 approach in planning and performing audit and assurance assignments, and how to leverage the COBIT guidance when assessing governance of enterprise IT (GEIT) topic areas. This publication also introduces a new format for future ISACA audit programs, which are designed to support IS audit and assurance professionals in obtaining maximum value from the COBIT 5 framework approach.

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.

Ian Sanderson, CISA, CRISC, FCA

Is a member of ISACA's Professional Standards and Career Management Committee and the specialist information systems auditor to the International Board of Auditors for the North Atlantic Treaty Organization (NATO).

COBIT 5 Training and Accreditation Program

ISACA has joined together with APMG-International to provide a COBIT 5 training and accreditation program that allows individuals to obtain the highest quality training through accredited training organizations and trainers.

Accreditation is a method of assessing the technical competence and integrity of training organizations offering COBIT. By taking training through an accredited training organization or trainer, you can:

- Ensure confidence in the value and knowledge acquired
- Save time and cost when choosing accredited training organizations and trainers
- Demonstrate your competencies and strong knowledge of COBIT
- Get an advantage in career development

Visit the **COBIT Training Providers** page of the ISACA web site for a list of accredited trainers and to learn more.

Come join the discussion! **Olabode Olaoke** will respond to questions in the **discussion area of the COBIT (4.1 and earlier)—Use It Effectively** topic beginning 22 April 2013.

Gaining Control of IT With COBIT—A Case Study

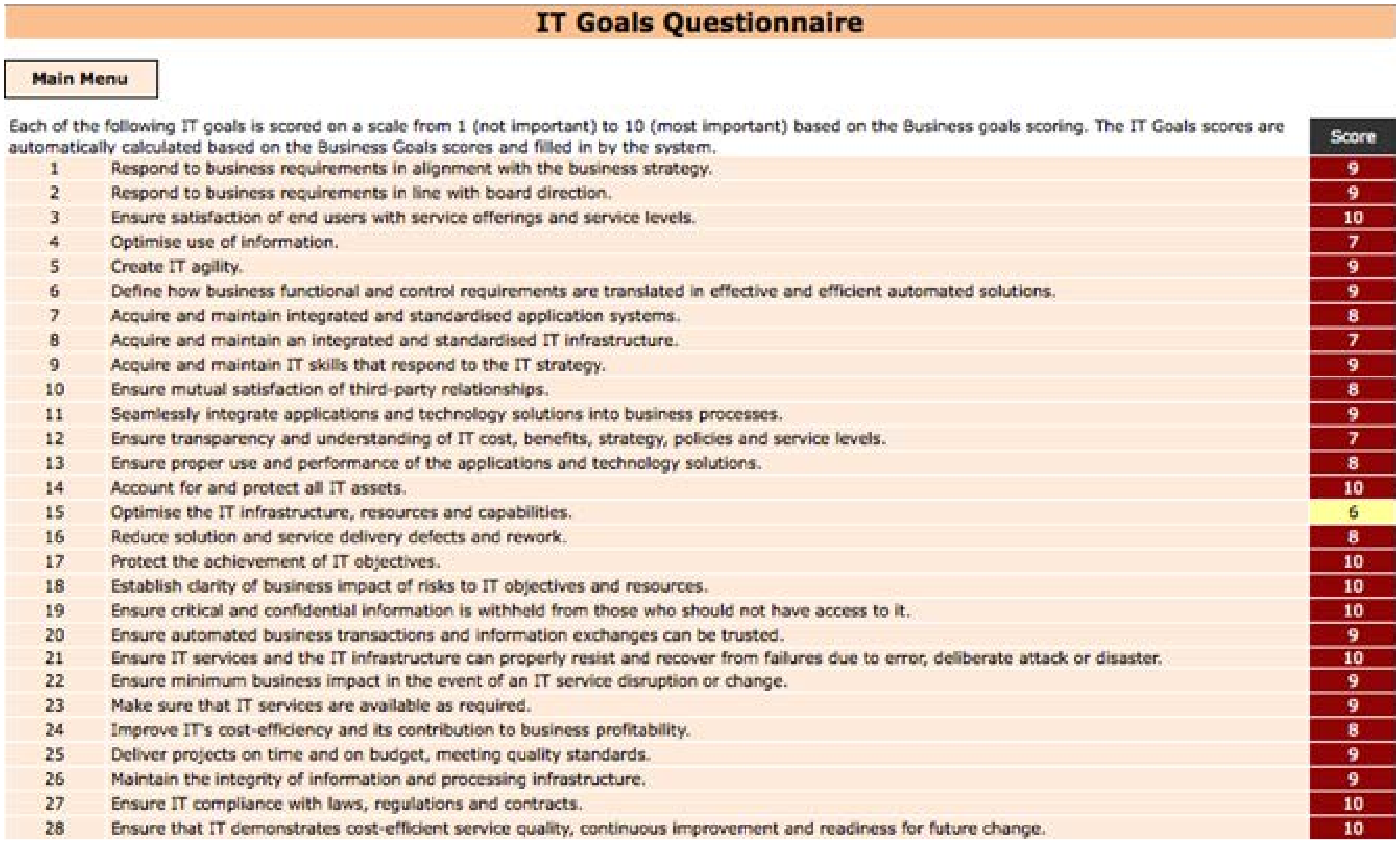
By Olabode Olaoke, CISA, ISO 27001 LI, ITIL, P2P

The IT organization of X-Bank (original name withheld) was facing a great deal of challenges with day-to-day IT service delivery. While critical activities, such as end-of-day, backup and restore functions, and scheduled server reboot for certain critical servers were documented on paper for regulatory compliance reasons, most processes were at best documented in individual employees' heads.

There was poor change control; something broke every other day and it was perfectly acceptable to have unplanned downtime of banking services for a few hours every month. Often, the unplanned downtime was due to, for example, failed system upgrades or security configuration modifications by the security administrators without proper impact assessments. Fortunately, the enterprise's internal control department had some oversight over the critical banking infrastructure; otherwise, banking operations could have suffered a total systemic failure.

In the marketplace, relatively smaller banks were recording better performance and were perceived as more reputable than X-Bank. Within the bank, the business executives did not trust IT's ability to effectively and efficiently support business objectives, and IT was obviously overwhelmed with the challenges.

Figure 1—Business Goals Questionnaire



IT Goals Questionnaire

	Each of the following IT goals is scored on a scale from 1 (not important) to 10 (most important) based on the Business goals scoring. The IT Goals scores are automatically calculated based on the Business Goals scores and filled in by the system.	Score
1	Respond to business requirements in alignment with the business strategy.	9
2	Respond to business requirements in line with board direction.	9
3	Ensure satisfaction of end users with service offerings and service levels.	10
4	Optimise use of information.	7
5	Create IT agility.	9
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	9
7	Acquire and maintain integrated and standardised application systems.	8
8	Acquire and maintain an integrated and standardised IT infrastructure.	7
9	Acquire and maintain IT skills that respond to the IT strategy.	9
10	Ensure mutual satisfaction of third-party relationships.	8
11	Seamlessly integrate applications and technology solutions into business processes.	9
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	7
13	Ensure proper use and performance of the applications and technology solutions.	8
14	Account for and protect all IT assets.	10
15	Optimise the IT infrastructure, resources and capabilities.	6
16	Reduce solution and service delivery defects and rework.	8
17	Protect the achievement of IT objectives.	10
18	Establish clarity of business impact of risks to IT objectives and resources.	10
19	Ensure critical and confidential information is withheld from those who should not have access to it.	10
20	Ensure automated business transactions and information exchanges can be trusted.	9
21	Ensure IT services and the IT infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	10
22	Ensure minimum business impact in the event of an IT service disruption or change.	9
23	Make sure that IT services are available as required.	9
24	Improve IT's cost-efficiency and its contribution to business profitability.	8
25	Deliver projects on time and on budget, meeting quality standards.	9
26	Maintain the integrity of information and processing infrastructure.	9
27	Ensure IT compliance with laws, regulations and contracts.	10
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	10

A turning point came when the chief executive officer (CEO) was stranded in the UK on a business trip. His debit card did not work for the entire three days that he was away nor did those of the other senior executive who had accompanied him. Unfortunately, it was the policy of the bank that middle to senior management staff were not permitted to hold bank accounts with other financial institutions; thus, they were stranded with little means to help themselves.

On return, the CEO initiated a process that resulted in the hiring of a chief information officer (CIO)—a very experienced CIO. His objectives were very clear:

- Stabilize the IT organization to effectively and efficiently support the business objectives.
- Minimize business disruptions caused by unplanned IT operations.
- Justify any (every) further investment in IT.

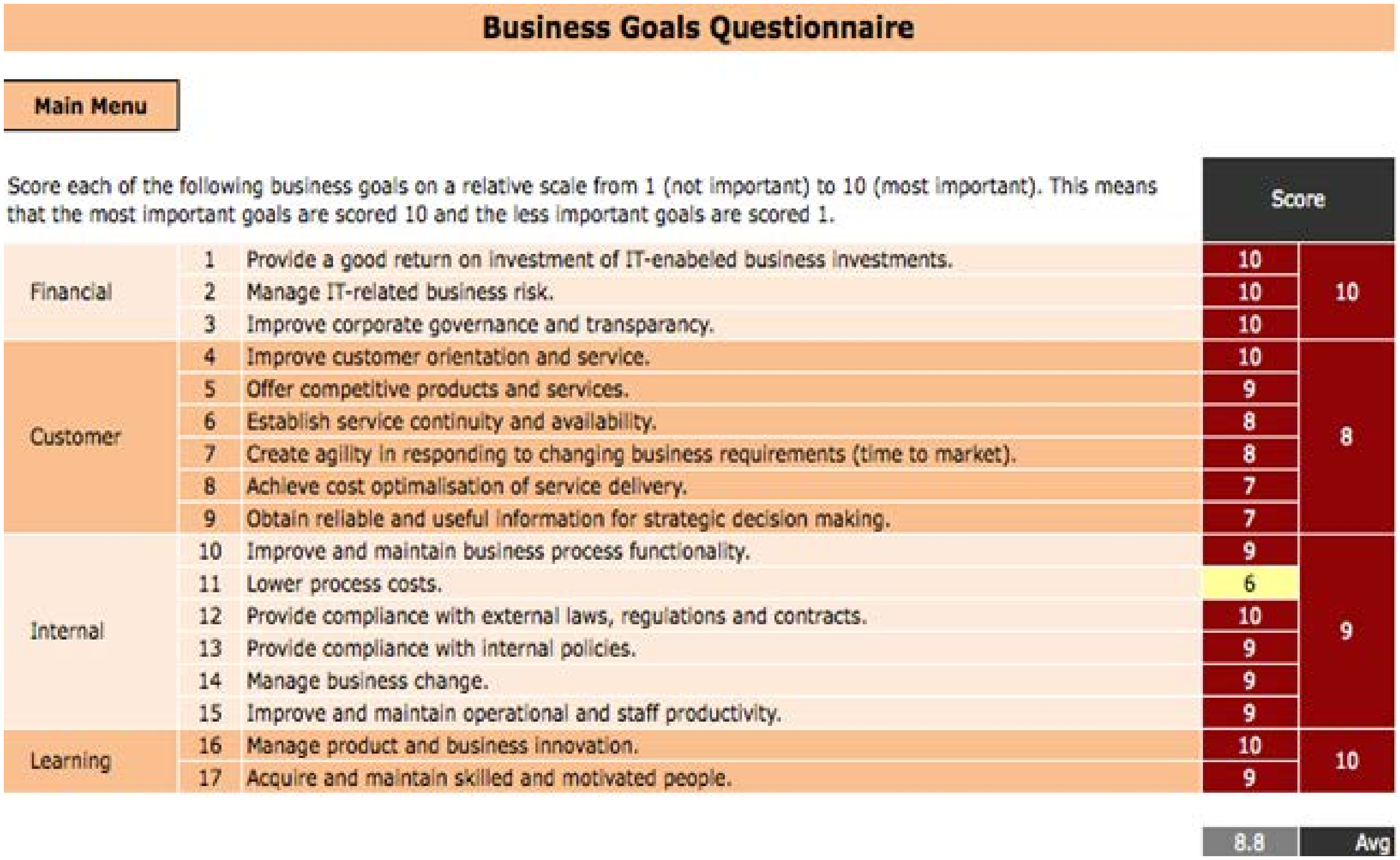
The CIO commenced meetings with new and existing consultants of the organization, the outcome of which culminated in the selection of COBIT® 4.1 as the most rounded approach to achieving the desired outcomes. Additionally, the project was bundled with a security assessment exercise.

The CEO was clear on the results he desired and why he hired a CIO so he was taken by surprise when, after committing to giving whatever was required as a sign of support, the first thing the CIO asked for was his *active participation* in the transformational changes in the IT organization. The lesson was: *Active and sustained* senior management commitment is very important for the successful implementation of the desired organizational changes.

The Assessment

The project kicked off with interview sessions to clearly document senior business management's view and expectations of IT, followed by similar sessions with the CIO and IT management, to get IT goals and a view of the IT organization. These were documented using the COBIT 4.1 Implementation Tool Kit as shown in **figures 1 and 2**.

Figure 2—IT Goals Questionnaire



Business Goals Questionnaire

Score each of the following business goals on a relative scale from 1 (not important) to 10 (most important). This means that the most important goals are scored 10 and the less important goals are scored 1.

			Score	
Financial	1	Provide a good return on investment of IT-enabeled business investments.	10	10
	2	Manage IT-related business risk.	10	
	3	Improve corporate governance and transparancy.	10	
Customer	4	Improve customer orientation and service.	10	8
	5	Offer competitive products and services.	9	
	6	Establish service continuity and availability.	8	
	7	Create agility in responding to changing business requirements (time to market).	8	
	8	Achieve cost optimalisation of service delivery.	7	
	9	Obtain reliable and useful information for strategic decision making.	7	
Internal	10	Improve and maintain business process functionality.	9	9
	11	Lower process costs.	6	
	12	Provide compliance with external laws, regulations and contracts.	10	
	13	Provide compliance with internal policies.	9	
	14	Manage business change.	9	
	15	Improve and maintain operational and staff productivity.	9	
Learning	16	Manage product and business innovation.	10	10
	17	Acquire and maintain skilled and motivated people.	9	
			8.8	Avg

Following the determination of business and IT goals, the core of the gap assessment exercise commenced. The focus was on the 34 processes, not on the 210 controls. Several interviews and process review sessions then followed from Plan and Organize (PO) all the way to Monitor and Evaluate (ME), although not necessarily in order as sessions were based on available resources.

Process Spotlight: PO9 Assess and Manage IT Risks

A good example was the risk management process (PO9), which was assessed as *nonexistent*, even though there was an operational risk (Ops Risk) department in place with a well-developed financial risk management practices around credit, loans, etc. The issues found included:

- No risk assessment framework in place
- No definition of impact ratings nor probability ratings
- No risk rankings
- No periodic risk assessment exercises as part of the organizational culture. IT managers generally used high, medium and low informally in approval memos.

In line with the COBIT guidelines, the first line of action to address these issues was to review the available options for risk management frameworks (for ease of standardization). NIST Risk Management Framework was identified and readily adopted.

The organization focused on the primary goals of *confidentiality, integrity and availability* as well as one important secondary goal: *reliability*.

Within four weeks, the organization had concluded a comprehensive risk assessment exercise, had a clear view into the organization's information risk posture and had easily adopted the parameters used by the Ops Risk department. Risk management started influencing change management and information security controls implementation (two high-risk areas identified during the risk assessment exercise).

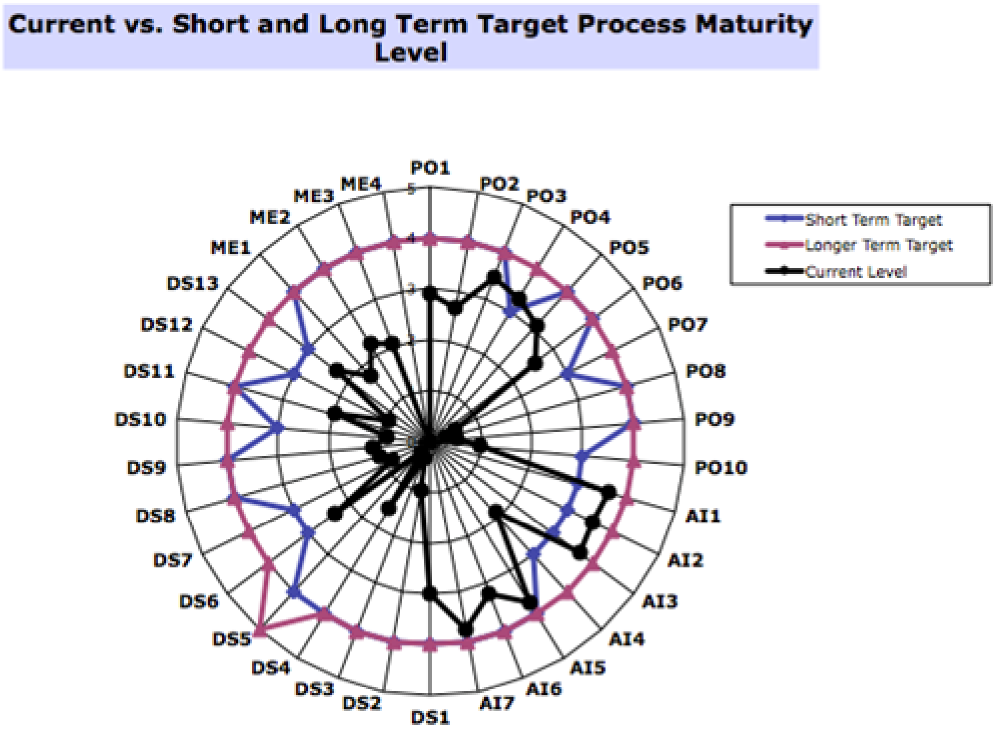
The assessment resulted in implementation of some quick-win initiatives, starting with instituting and enforcing a formalized change management process (COBIT 4.1 AI6) to move from maturity level 3 to maturity level 4.

Measurements and metrics were set and business units were mandated to be formally involved in the change management process.

The business units immediately felt some benefits. The resulting change accountability and communication made the business even more interested in other COBIT initiatives. And, the business unit heads felt a great deal of ownership, as the changes were occurring only with their consent.

By the time the exercise was concluded, the enterprise had good insight into its maturity for all 34 COBIT processes plotted against short- and long-term goals, as shown in **figure 3**.

Figure 3—COBIT Assessment Results for X-Bank (34 Processes)



Observations and Recommendations

It was a little challenging to get the noncore IT areas (e.g., procurement, financial control [responsible for budget], human resources [HR]) to understand the importance of their functions to the success of the IT organization. As part of PO7 (*Manage IT human resources*), HR, as a case in point, did not consider IT resource career paths and training requirements as important enough; hence, IT trainings were often cancelled for cost savings or resource demands. This disconnect was initially extended to the COBIT implementation exercise and it required some escalation to the CIO to get HR to cooperate with the assessment exercise.

Prioritizing and Plans of Action

Once the assessment exercise was concluded, the enterprise set out to commence remediation initiatives. Activities were prioritized according to three categories:

1. **Quick wins**—Achievable within one month and with minimal/no budgetary implications
2. **Key business goal initiatives**—Initiatives aligned with achievement of business goals rated seven to 10 in **figure 1**.
3. **Other gap items**—All other gap items that could be delayed until completion of those items in categories 1 and 2.

Monitoring and Measuring

Responsible, Accountable, Consulted and Informed (RACI) charts were developed for all 34 processes, and the CIO was not willing to accept excuses for noncompliance to newly developed practices. Metrics and measurements were evolving and these were aligned with performance metrics and appraisal systems for the entire IT organization.

Initiatives such as updating scorecards to reflect performance metrics and IT organizational key performance indicators (KPIs), as well as rewards and sanctions, were key to getting operational staff to accept the cultural changes that came with the remediation activities.

Within 18 months, the results were clearly visible; as such, it was not difficult for X-Bank to achieve ISO 27001 certification status shortly thereafter (though as a separate initiative).

Olabode Olaoke, CISA, ISO 27001 LI, ITIL, P2P

Is an information systems security and governance consultant at Digital Jewels Limited (DJL). Olaoke currently leads the information security and IT service management practices at DJL with several standards implementation exercises including ISO 27001, ISO 20000, Payment Card Industry Data Security Standards (PCI DSS) and BS 25999.

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.

Editorial Content

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