In This Issue:

- COBIT 5: Enabling Information Progress Report
- Integrating COBIT 4.1 Into the Internal Audit Function
- COBIT 5 for Risk Progress Report
- COBIT Maturity Assessment and Continual e-Health Governance Improvement at NHS Fife
- COBIT 5 for Assurance Progress Report

COBIT 5: Enabling Information Progress Report

By Steven De Haes, Ph.D.

The objective of the COBIT® 5: Enabling Information 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. The guide should be considered the information equivalent of the COBIT 5: Enabling Processes publication.

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 recently. This project is now moving forward under the direction of a task force that is guided by the ISACA Framework Committee and Knowledge Board.

The proposed content includes:

- Elaboration of the COBIT 5 goals cascade, expanding on the information enabler goals
- Clarification of the information model with examples and explanations
- Examples of how to apply the COBIT 5 information enabler model to information governance and management issues
- Examples of how the information model can be applied to specific, selected information items (items will include business-related and IT-related examples)

A plan has been established to progress the project, including a content development workshop and a broader subject matter expert review. The product is anticipated to be available in the second quarter of 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 the COBIT 5 Task Force and currently serves as the chair of the Information Reference Model Task Force.
Integrating COBIT 4.1 Into the Internal Audit Function

By John Panopoulos, CISA

TT Hellenic Postbank S.A., in Athens, Greece, is a publicly traded bank in the Athens Stock Exchange, a member of the Hellenic Banking Association, the European Savings Banks Group and the World Savings Banks Institute. Today, TT Hellenic Postbank is a modern bank with a wide depositor base and a healthy loan book, enjoying the required potential and financial background to provide substantial support to the Hellenic economy and society.

The bank’s IT audit management recognized that a new methodology was required for the assessment of the effectiveness and efficiency of the bank’s IT internal control environment. Moreover, IT audit management decided to establish a standardized and well-defined method of planning and implementing IT audits; thus, the bank decided to consider widely accepted control-based frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework and COBIT® 4.1.

Comparing the two aforementioned frameworks, the IT audit management concluded that COBIT 4.1 was the best solution for its needs, due to its comprehensive coverage of IT controls and its straightforward link with business objectives, as opposed to COSO, which it found to be very high level and not IT-specific. COBIT 4.1’s good practices contribute to aligning IT and business objectives, introduce a generally accepted process model, and define a list of control objectives for each process. By means of the maturity model and the detailed control objectives, there is a clear understanding about the current level of efficiency and control over IT processes. Also, COBIT can be easily customized to support the needs of each organization and mapped with other commonly accepted assurance frameworks. As a result, COBIT 4.1 was utilized to define the IT audit universe, create tactical (annual) and strategic risk-based audit plans, and standardize the audit process.

Implementation

COBIT 4.1 implementation took place at TT Hellenic Postbank in 2008 and was focused on the following areas:

- **Defining the IT audit universe**—The IT governance framework diagram (figure 1) was created, outlining the current IT operations, and was used as the foundation of the audit universe. At that point, the 34 COBIT 4.1 processes were mapped under those operations (figure 2); for example, the DS5 and DS9 processes were mapped under Security Configuration Management. Subsequently, all high-level IT operations were assessed and an initial maturity level was assigned to them: 0 (for nonexistent) or 1 (for initial/ad hoc). Accordingly, IT resources (applications, information, infrastructures and people) were assigned under each IT operation, and after every change in the IT environment, the audit universe was updated.

- **Creating a risk-based audit plan**—A methodology was created to rank the IT processes according to residual risk. Initially, IT audit management collaborated with IT management to assess the inherent risk of IT processes, taking into consideration risk factors such as financial and operational risk. After that, the current maturity level was taken into consideration and the residual risk was calculated. The inherent risk has been reassessed on an annual basis, and the highest ranking processes according to this methodology are included in the audit plan.

- **Setting the scope of audit engagements**—Internal policies and procedures, legislation and regulations as well as the COBIT 4.1 process control objectives were combined to define the scope of the audit engagements. In the scope of those engagements, the most critical IT resources were also included.

- **Scoring the process**—COBIT 4.1’s Process Maturity Model (PMM) was used for scoring IT operations. Initially, a maturity level value of 0 (for nonexistent) or 1 (for initial/ad hoc) was assigned to each IT operation. Consequently, after the completion of an audit engagement, the operation’s maturity level was updated to reflect the current state.

- **Audit reporting**—COBIT 4.1 provided a way of matching IT processes to IT goals and IT goals to business goals. This matching has been used to present the benefits of taking corrective actions to senior management more efficiently. In the case of the security configuration management audit, IT audit management was able to present, in the same context, technical issues, compliance issues and contractual obligations that needed to be observed.
Benefits
Integrating the COBIT framework into the IT audit function has resulted in the following positive impacts:

- The development of a well-defined, standardized methodology of planning and implementing IT audits. In this way, audit budgets have involved more projects and audit resources have been properly utilized.
- There has been better alignment among audit, IT and business goals.
- A common language for IT, audit and C-level management has been established.

At this point, COBIT has only been used by TT Hellenic Postbank’s IT audit team. Eventually, the bank’s IT audit management envisions the acceptance of COBIT as an IT governance framework for the entire organization, as it has improved the quality of the audit work and has proven the importance of the adoption of a common framework.

John Panopoulos, CISA
Is the head of IT audit at TT Hellenic Postbank in Athens, Greece. Previously, he was a senior software engineer and an IT consultant. Panopoulos can be contacted at j.panopoulos@ttbank.gr.
Endnotes

1 IT Governance Institute (ITGI), *COBIT Mapping Overview of International IT Guidance, 2nd Edition*, USA, 2006
2 The Institute of Internal Auditors (IIA), *Global Technology Audit Guide (GTAG): Developing the IT Audit Plan*, USA, 2008
3 ISACA San Francisco Chapter, “Integrating COBIT 4.1 Into the IT Audit Process (Planning, Scope Development, Practices),” PowerPoint, California, USA, 2006
4 Bank of Greece Governor’s Act 2577/2006
COBIT 5 for Risk Progress Report
By Steven Babb, CGEIT, CRISC

The objective of the COBIT 5 for Risk project is to create a risk view of COBIT 5, which will serve as specific guidance for ISACA’s risk-focused constituents. The resulting publication will be the risk management equivalent of the recently published, security-focused COBIT 5 for Information Security.

The project to develop the COBIT 5 for Risk publication to extend the COBIT 5 family of products was approved by the ISACA Board of Directors recently. This project is now moving forward under the direction of a task force that is guided by the ISACA Framework Committee and Knowledge Board.

COBIT 5 for Risk will replace ISACA’s previous framework on IT risk management, Risk IT, which was last updated in 2009 and has successfully driven improvements in how enterprises manage their IT risk exposure.

COBIT 5 for Risk builds upon this and will:
- Provide an explanation of how the COBIT 5 enablers can be used to support the activities and needs of risk professionals
- Enhance the COBIT 5 framework capability in the area of information risk and link it with third-party guidance (e.g., ISO 31000, COSO Enterprise Risk Management—Integrated Framework, ISO 27005) and risk governance and management techniques, as appropriate
- Address business and IT risk integration by ensuring that COBIT 5 for Risk facilitates and promotes this alignment, with the understanding that IT risk is business risk
- Address how the overall control concept is embedded into COBIT 5 for Risk. This is aligned to the changes made in COBIT 5, where business objectives are now used instead of control objectives and governance and management practices and activities are used instead of control practices and activities.

A plan has been established to progress the project, including a small content development workshop and a broader subject matter expert review. The product is anticipated to be available in the second quarter of 2013.

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.
COBIT Maturity Assessment and Continual e-Health Governance Improvement at NHS Fife

By Elena Beratarbide, CISA, Pablo Borges and Donald Wilson

The NHS is the National Health Service trust that provides public health care services across the UK. NHS Fife is the corresponding public health care provider within the Fife region in Scotland, UK, covering a range of services from primary care to acute services, involving community hospitals across the region.

NHS Fife began working with COBIT® in 2007, led by the need to ensure that its e-health services were aligned with NHS’s national and local strategies, along with internal pressures to improve security, audit outcomes and compliance with recognized standards.

Until 2007, NHS Fife had been focused on Information Technology Infrastructure Library (ITIL) as a best practice standard for IT service management. ITIL v2, the version available at the time, lacked the overall vision of a continual improvement process—something that COBIT provided. This vision incorporated all relevant processes from the service strategy to operations, establishing the improvement cycle in terms of level of maturity, how to progress within the improvement path for processes and activities, and how to measure progress.

NHS Fife understood that COBIT provides a higher-level framework that allows for working with a process vision, encompassing some IT governance processes not covered by ITIL, such as strategic planning, risk management, quality management and internal control. The decision to integrate the organization’s previous efforts with ITIL with the COBIT framework allowed for a more efficient management of resources, particularly in a climate of greater-than-ever efficiency-savings pressures and increasing clinical and non-clinical e-health demand.

NHS Fife supported the implementation of COBIT with the Meycor COBIT® Suite, which was particularly helpful for establishing a baseline, developing improvement plans, selecting metrics and tracking the improvement cycles designed for each targeted process.

In 2008, the NHS Fife initiative evolved into an e-health COBIT demonstrator project, which aimed to show results after applying COBIT to three different NHS boards in Scotland and the UK, and to present conclusions and recommendations to the e-health directorate of the Scottish government for consideration across other NHS boards.

To get support from the Scottish government (e-Health Programme), NHS Fife needed to demonstrate results achieved from the earliest stages. In 2005, NHS Fife started restructuring the IT department based on ITIL recommendations, which included implementing clear service delivery, service support functions and managers for key ITIL processes, while maintaining infrastructure support teams. In 2006, a new IT change support manager, who already worked with COBIT, was appointed and introduced the framework into NHS Fife. The quick results related to IT change management convinced the head of the department to extend the improvement model to other key processes, and within a year, a further two NHS boards joined the project, which aimed to demonstrate results and to develop a set of recommendations for other NHS boards facing the same challenges and considering the adoption of e-health governance best practices.

From the NHS Fife perspective, the targets for a COBIT implementation were to:

- Understand the priorities toward establishing a mature process for e-health to engage and align with the NHS Fife strategy
- Reduce risk and improve security
- Improve internal and external audit outcomes
• Establish a continual improvement model of working that is sustainable, and demonstrate results
• Achieve COBIT level 3 maturity for all key processes within a year

The implementation of COBIT was divided into two phases. Phase one involved training the key process owners from the e-health team on IT governance, COBIT® 4.0 and Meycor COBIT tools. Phase two involved:
• Raising awareness of IT governance across the e-health team
• Further training on the COBIT framework and Meycor COBIT tools
• Identifying all relevant process owners and responsibilities (figure 1)
• Reviewing in-depth the existing processes, producing a baseline of the current situation
• Selecting pilot processes according to the priorities for the organization. This selection was based on a heat map of critical processes from the NHS Fife priorities perspective (figure 2), including the expected value of improving the process for NHS Fife, audit recommendations, risk and the results of the assessment baseline (figures 3 and 4).
• Developing improvement plans. Each process owner was in charge of producing improvement plans, with further assistance provided by a COBIT expert. The latter was only required during the initial training—until the method was established in the team.

### Figure 1—Example of Adapted RACI Chart

<table>
<thead>
<tr>
<th>COBIT PROCESS</th>
<th>CONTROL OBJECTIVE</th>
<th>COBIT ACTIVITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS8</td>
<td>1.2</td>
<td>Create classification (severity and impact) and escalation procedures (functional and hierarchical)</td>
</tr>
<tr>
<td>DS8</td>
<td>2.1/2.2</td>
<td>Detect and record incidents/service requests/information requests</td>
</tr>
<tr>
<td>DS8</td>
<td>2.3</td>
<td>Classify, investigate and diagnose queries</td>
</tr>
<tr>
<td>DS8</td>
<td>3.1/3.2 4.1/4.2</td>
<td>Resolve, recover and close incidents</td>
</tr>
<tr>
<td>DS8</td>
<td>1.3/5.1</td>
<td>Produce management reporting</td>
</tr>
</tbody>
</table>

Source: NHS Fife. Reprinted with permission.

### Figure 2—Value Analysis: Heat Map Based on Aggregated IT and Business Goals Importance

| Value contribution to IT Goals (Weighted value, max importance of IT Goal contributed) |
|-----------------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|--------------------------------|
|                                        | High contribution (values 31-50)| ME1 (32)                       | ME4 (32)                       | PO6 (48)                        | DS5 (42)                       | Al7 (36)                       |
|                                        | Medium contribution (values 16-30) | PO10 (24)                       | PO5 (20)                       | PO8 (20)                        | DS2 (24)                       | DS4 (30)                        |
|                                        | Low contribution (values 0-15) | PO4 (18)                       | PO9 (16)                       | DS1 (24)                        | DS6 (20)                       | ME2 (30)                        |
|                                        |                                 | AI4 (18)                       | AI9 (18)                       | DS11 (17)                       | DS10 (16)                      | DS13 (28)                       |
|                                        |                                 | PO7 (19)                       | DS7 (14)                       | PO2 (13)                        | DS8 (22)                       |                                 |
|                                        |                                 | PO3 (4)                        | DS9 (10)                       |                                 |                                 |                                 |
|                                        | Medium Importance Goals (2-3-4) | AI5 (14)                       | AI1 (12)                       |                                 |                                 |                                 |
|                                        | High Importance Goals (1)       |                                 |                                 |                                 |                                 |                                 |
|                                        | Very High Importance Goals (0)  |                                 |                                 |                                 |                                 |                                 |

Maximum Importance of IT Goals contributed (MAX)

Source: NHS Fife. Reprinted with permission.
Applying an IT department user-satisfaction survey to demonstrate changes in perceptions through a series of improvement cycles

Carrying out an assessment after three, six and 12 months, which involved measuring the achieved level of maturity and putting on a series of lessons-learned workshops with key stakeholders and process owners

Disseminating the results

In 2010, the change management process was externally audited, showing an achievement of a high, level 3 (incipient level 4) maturity. This result represents one of the highest scores and quickest improvements obtained for processes externally audited within the e-health practices at NHS Fife.
The improvements to the change management process also resulted in a series of improvements in linked processes, e.g., service desk and incident management, change and configuration, service level management, security management, and business continuity.

Since 2010, NHS Fife’s e-health infrastructure achieved ISO 27001 certification (in January 2012) and developed a corporate framework for IT governance, which involves a recognition of the importance of IT governance regardless of whether the IT service is provided by the e-health infrastructure department or another department (currently within NHS Fife there is a federated archetype). E-health governance is positively influencing the expansion of the use of COBIT across other processes linked to e-health services within NHS Fife, but residing outside of the e-health infrastructure team, e.g., within the e-Health Programme, information services and other federated IT services.

Looking Forward
At the present time, the e-health infrastructure team is focused on consolidated metrics and establishing relevant dashboards suitable for specific needs, particularly support team management (e.g., service desk, desktop, systems, applications, network, general practitioners IT support, telecommunications), but also dashboards for specific process management service level agreements (SLAs) and security. This constitutes a step toward level 4 maturity in other critical processes.

With the release of COBIT 5 and an especially challenging e-health delivery programme for the forthcoming years in NHS Fife, the organization is focusing even more intently on meeting stakeholders’ expectations and reviewing the e-health governance structure of NHS Fife to ascertain how to make the best use of the additional features, especially the principle of meeting stakeholder needs.

Elena Beratarbide, CISA
Is an experienced IT consultant and security auditor for Touché & Ross (Deloitte), KPMG and Fujitsu. Beratarbide is the e-health manager for the National Health Service (NHS) in Fife, Scotland, UK. She is also an active e-health researcher in collaboration with the computer science department of St. Andrews University (Scotland, UK), the Business Management Department—DOE of the Polytechnical University of Valencia (Spain), Capella University (USA), Middlesex University (UK) and the NHS.

Pablo Borges
Is an experienced IT consultant, working in IT governance projects across the Americas and Europe since 2006. Borges leads multidisciplinary teams to drive improvement in IT processes aligned with best practices, combining frameworks such as COBIT and ITIL with quality standards, such as ISO 27001, to design tailor-made solutions that suit business needs. He specializes in continual improvement projects and provides support in areas including information security, risk management, business continuity, major incidents and change management.

Donald Wilson, CITP
Is head of e-health and has served the NHS in Fife, Scotland, UK, for 15 years. He began his career in the electronics and computer technology field with Scottish Water and Motorola. Wilson is an active member of the e-Health Leads Group, which provides a link between NHS Boards and the Scottish Government e-Health Programme at a management level, and is key to the successful implementation of projects at the NHS board level.

Endnotes

1 NHS Fife web site
COBIT 5 for Assurance Progress Report

By Anthony Noble, CISA

The objective of the COBIT 5 for Assurance project is to create an assurance view of COBIT 5, which will serve as specific guidance for ISACA’s information assurance constituents. The guide should be considered the assurance equivalent of the recently published, security-focused COBIT 5 for Information Security.

The project to develop the COBIT 5 for Assurance publication to extend the COBIT 5 family of products was approved by the ISACA Board of Directors recently. This project is now moving forward under the direction of a task force that is guided by the ISACA Framework Committee and Knowledge Board.

The proposed content includes an:

- Explanation of how the COBIT 5 enablers can be used to support the activities of information assurance professionals
- Explanation of how information assurance professionals can provide assurance over the COBIT 5 enablers for the governance and management of enterprise IT (GEIT)
- Exploration of relationships between COBIT 5 for Assurance and relevant major assurance standards
- Introduction of a new ISACA audit program format that will be used going forward. This format will address all of the COBIT 5 enablers and other components necessary to support assurance assessment, evaluation and conclusion reporting. One or two example programs will be included.

A plan has been established to progress the project, including a small content development workshop and a broader subject matter expert review. The product is anticipated to be available in the second quarter of 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 currently 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 for two years.