Using COBIT to Support IT Risk Management

By Paul Lokuciejewski, Ph.D., Karsten Wilop, CISA, CGEIT, CRISC, and Werner Syndikus, CISA, CGEIT, CRISC

IT plays a vital role in today’s business world. Crucial incidents in IT substantially impact business processes and can result in loss of revenue and image damage. The increasing relevance of IT moves IT risks and their detection and handling into the focus of those responsible for IT. Furthermore, legal and regulatory requirements for operational risk management are growing, demanding proactive risk management with an early warning system.

IT risk management is described in conventional standards and best practice frameworks as a cyclical process (figure 1).

Regulatory requirements, standards and frameworks provide differing levels of detail for the practical deployment and execution of this process. For this reason, a group of experts in Germany formed the IT Risk Management With COBIT group with the objective of developing practically oriented tools for the substantive deployment of IT risk management.

Goals and Approach
The starting point for the IT Risk Management With COBIT group was a collection of questions arising in the context of a practical deployment of an IT risk management process. The following essential questions were identified:

- How can a comprehensive inventory of generic risks be defined to prevent overlooking fundamental risks in the course of developing enterprise-specific risk scenarios?
- What key indicators can be used to measure vulnerabilities, and which key indicators can be utilized to support the implementation of an early warning system?
- How can suitable countermeasures for risk treatment be identified?
- How can risk impact be represented to IT management and business in particular?

Based on these issues, the objective of the IT Risk Management With COBIT group was formulated as follows: development of tools for the
practical issues raised previously that can be provided to the relevant target group (e.g., IT supervisors, risk managers and line supervisors) in the form of a practical guideline.

The group first carried out a general analysis of COBIT to determine whether and how information could be derived from this framework to provide answers for the questions posed previously and to create the planned guideline. In parallel, a wide range of other IT risk management standards and frameworks (e.g., ISO/IEC 27005:2011 Information technology—Security techniques—Information security risk management, ONR 49000 Risk management for organizations and systems—Terms and basics—Implementation of ISO 31000, Risk IT, etc.) was analyzed to check whether they contain answers to the identified issues, which would make the planned guideline superfluous.

Although the analyzed standards/frameworks all present good approaches to the methodical deployment of IT risk management, only a small number of practical aids was found to resolve the identified issues. In particular, none of the standards/frameworks contained extensive information on the creation of a "comprehensive risk inventory" for risk scenario development.

In contrast, the general analysis of COBIT showed that COBIT, as a comprehensive framework for IT processes, offers a high potential for the derivation of such a risk inventory because it covers all relevant IT control areas. Furthermore, COBIT’s control objectives implicitly cover areas of IT that inherently entail risk. COBIT also provides a wide range of auxiliary information, e.g., goals and metrics at the IT, process and activity levels.

Based on the results of the general analysis, a systematic and detailed analysis of COBIT was performed to extract useful components of the framework for a substantive deployment of an IT risk management process. The following conclusions were drawn:

- To provide an initial basis for scenario development, the inventory of generic risks should be formulated as an inversion of the detailed control objectives that indirectly represent vulnerabilities.
- Early-warning indicators should be derived from COBIT’s goals and metrics and then allocated to the respective risk areas.
- Information on risk treatment should be derived from COBIT’s maturity model.
- The mapping of IT processes to the IT objectives and business objectives contained in COBIT should be exploited to explain the impact of the detected risks to IT management and business.

Results and Outlook

The detail analysis showed that valuable information on the substantive deployment of IT risk management can be derived from the information in COBIT. These essential results were formulated in the following work packages (WPs):

- **WP1: Derivation of IT vulnerabilities from control objectives**—COBIT states that IT processes have to be managed in a proper way to achieve business objectives. This implies that missing or poorly managed IT processes endanger business objectives and, thus, represent a vulnerability (leading to a risk). Based on this assumption, vulnerabilities from all control objectives were systematically derived, resulting in a risk inventory containing 222 vulnerabilities that represent a starting point for scenario development.
- **WP2: Identification of risk indicators from goals and metrics**—For each identified vulnerability, goals and metrics of the corresponding processes were analyzed to see whether they were suitable as risk indicators. As a result, goals and metrics were allocated directly to a specific vulnerability. Goals and metrics were indirectly allocated to the vulnerabilities at the process level due to their higher abstraction level.
- **WP3: Derivation of risk treatment countermeasures**—Countermeasures for a systematic treatment of the identified vulnerabilities were extracted from the maturity model in connection with the requirements from control objectives.
- **WP4: Derivation of risk impacts on IT and business objectives**—The COBIT tables, the mapping of IT processes to IT objectives and business objectives were exploited to represent the impacts of the identified risks on business objectives.

The complete approach of the detail analyses, including all of the results, is currently being compiled by the IT Risk Management With COBIT group in a comprehensive guideline. In parallel to the creation of the guideline, the expert group is developing a tool in which the information from the WPs are centrally collected and evaluated.

Paul Lokuciejewski, Ph.D.

is a consultant at PwC in Dusseldorf, Germany. He has several years of experience in technology consulting, internal and external audits in the financial sector, and software development.
Karsten Wilop, CISA, CGEIT, CRISC
is a senior manager at PwC in Dusseldorf, Germany. He has more than 10 years of experience in the areas of IT compliance, internal and external audits, and IT consulting within the financial sector.

Werner Syndikus, CISA, CGEIT, CRISC
has 10 years of experience as a software developer and 10 years of experience as head of IT in the wholesale industry.

Endnotes

1 The group includes the following members: Mohammad Hamidi, Ralf Herter, Paul Lokuciejewski, Ph.D., Heinz-Dieter Schmelling, Ph.D., Werner Syndikus, Martin Urban and Karsten Wilop.

2 Risk IT provides a clear framework for implementing an IT risk management process. This article demonstrates how COBIT 4.1 can be used to build upon Risk IT’s series of generic scenarios to identify a more detailed set of IT risk scenarios in support of IT risk management.