Chapter 5
IT-Assurance with CobiT

Martin Fröhlich
PricewaterhouseCoopers AG, Germany

Wolfgang Johannsen
it’s okay Lt. & Co. KG, Germany

Karsten Wilop
PricewaterhouseCoopers AG, Germany

ABSTRACT

Strategic IT management is increasingly concerned with requirements from regulatory bodies. This conformance part of IT management complements the classic performance side. Ideally both are integrated into IT Governance of an enterprise or organization. With the need to prove compliance with a wide diversity of laws and rules for IT systems (technology, processes, rules) the demand for proven support methods grows. Specifically best practice models are beginning to gain awareness and acceptance for IT Audits and for the less formal IT Assurance projects. The Control Objectives for Information and Related Technology (CobiT) reference model is increasingly being discussed as a framework of choice for IT Audits and IT Assurance. This chapter introduces requirements for IT Audits and IT Assurance projects and discuss the boundaries of applying the CobiT IT Assurance Guide in such environments.

INTRODUCTION

In this article the goals and procedures showing different characteristics of IT-Assurance projects will be presented and the adequacy of the CobiT Reference Model for these projects discussed.

First we need to differentiate between IT-Assurance and IT-Audit. While IT-Audit requires a bounded and more formal framework, IT-Assurance projects can basically be defined and designed openly. IT-Audits are generally more shaped in their completion through legal and other requirements as well as specific qualification profiles (e.g. financial auditors).

As a reference model for performing the IT-Assurance the, IT Assurance Guide using CobiT (ITGI, 2007a) was re-published last year. After a short description of the basic characteristics of this guide, a presentation of its usableness in a proprietary framework for IT-Audits follows. Finally we will discuss the boundaries of using the IT-Assurance Guide.
GOALS OF IT-ASSURANCE

For IT-Assurance the following common understanding has emerged: through an “act of assuring” an independent Assurance-provider assures the receiver, that the Assurance-object does or does not fulfill a warranted property. According to the definition of the IT-Governance Institute (ITGI) Assurance covers five components (ITGI, 2007a):

1. A defined relation between three parties: a) the one responsible for an Assurance-object, b) an Assurance-provider and, c) the one(s) interested in an Assurance-result,
2. A specific Assurance-object,
3. Criteria, which an Assurance-object has to meet and which are accepted by all parties,
4. A defined Assurance-process,
5. An assessment, if the criteria are fulfilled by the Assurance-object.

In this context we understand IT-Assurance as a special process, which makes a statement in the result, if selected parts of IT or IT as a whole can cope with a specific catalogue of criteria.

In case that IT-Assurance is given by financial auditors within the scope of the annual audit, we call it IT-Assurance in a narrower sense or “IT-Audit” due to the particular existing direction to the financial reporting. On the other hand we call audits performed by internal auditors or by governmental bodies like the German Federal Office for Information Security (BSI) IT-Assurance in a wider sense or IT-Assurance, as their evaluation focuses on sections beyond financial reporting.

The common basis of IT-Audit and IT-Assurance are the auditor’s independence and criteria accepted by all parties such as financial accounting and financial reporting standards for financial auditors or standards and best practices for designing control- and security-systems (COSO, CobiT, ISO 2700X).

Therewith IT-Assurance and IT-Audit processes differ from an expert opinion, as the latter predominantly adducts subjective experience gathered in the evaluation process.

The different goals of IT-Audit and IT-Assurance are illustrated in the following Figure 1.

The picture illustrates the different levels of an IT-system holistically. This covers the IT processes and IT Infrastructure with hardware, operating systems, network and IT Processes, the IT Applications that are applied supporting the operational tasks in an organisation and the Business Processes that employ IT resources for their processing. The co-operation of these levels is determined by the control environment, in which the operational and organisational structure, the organisation’s strategy, human resources management, etc are linked up (see also Figure 1).

As illustrated by the dark toned bar in the picture, IT-Audits generally allude to all areas of an IT system (business processes, IT applications, IT processes and infrastructure). In the focus of an IT-Audit only those elements that have direct and indirect influence on the financial reporting of the organisation are considered. Therefore IT-Audits in the context of the annual audit address only those areas of an IT system, from which risks for the financial reporting could arise.

On the other hand IT-Assurance in a wider sense is expandable to any other areas in IT systems. The spectrum can range from the whole IT to focused security audits of single components. As examples for IT-Assurance a certification according to ISO 27002 or a data center security audit are presented in the figure as oval forms (see also Figure 1).

PERFORMING IT-ASSURANCE

Standards vs. Best Practice

Standards are documents which are created in the context of a consensus and audited by an accepted body. They offer rules and guidelines for activities, methods, procedures, etc. and are binding