

The Compliance Challenge in Information Technology

By Caroline Simões e Leonardo Freitas - October 6, 2006

The term Compliance means "conforming to, obeying, abiding by". In information technology (IT), being compliant means conforming to rules, regulations, or best practices.

There are currently several standards of best practices in the IT area, which are adopted by managers in the process of implementing internal controls and managing IT-related risks.

Below we present summarized descriptions of two of the main standards used in the IT area:

CobiT

CobiT (Control Objectives for IT and related Technologies) is a set of good practices focusing on IT governance. It was developed by the IT Governance Institute - ITGI (www.itgi.com) to define standards for guiding and controlling information technology in organizations. It is composed of 34 processes, divided into 218 control objectives. Structurally, CobiT consists in a set of 34 processes, which are divided into 218 control objectives for IT.

ISO/IEC 17799

ISO/IEC 17799 is an international standard focusing on information security. It is based on the first part of the British standard, BS7799, and was developed by the international group JTC1/SC27, which is formed by the ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) organizations. ISO/IEC 17799 is currently the main reference in information security standards. It is structured into 11 sections (first level controls), containing altogether 39 control objectives (second level controls) and 135 third level controls.

The existence of so many best practice standards, which complement each other in some areas and delve deeper into others, increases the complexity of the task of defining priorities regarding actions to be taken by managers when implementing internal controls.

Risk Manager's Compliance Module

Modulo is aware of this need, and has therefore incorporated a new feature into the Risk Manager IT risk assessment and information security knowledge management tool. This feature supports managers in the challenge of adhering to these best practice frameworks using the controls in the Risk Manager knowledge base.

The Compliance Module provides the client with information on the relationship between each of the requirements in the frameworks and the controls presented in Risk Manager. The image below

represents the way this information is made available in Risk Manager.

Let us suppose, for example, that after conducting a risk assessment process, a manager has to identify the controls needed for implementing a specific requirement. (In the image above, item 5.1.1 of ISO/IEC 17799). Without using the tool, he or she will take a long time to identify these controls, since the relationship between controls and requirements is by no means trivial.

Using the Compliance Module, at the end of the assessment process the manager will be able to identify the controls that are related to the specific requirement and, of these, which have been implemented and which still need to be implemented. Risk Manager allows this analysis to be performed in the scope of the entire framework.

Through the indexes presented in the report (compliance index and security index), the manager can develop an organized and prioritized action plan to meet the necessary requirements. This reduces the amount of both resources and time required to implement the frameworks.