

Compliance module - Importance and applicability

by Geraldo Ferreira - May 23, 2007

The scene has changed radically. Ten years ago, security professionals had no literature on which to base their work. Today, there is a profusion of security requirements (laws, regulations and guides) that must be followed by organizations (Figure 2). Some of these are mandatory, like the Federal Laws, while others are conditional and should be implemented according to the organization's location and sector (government, financial, telecommunications, and others). And there are also optional frameworks, representing international security standards organized into codes of practice.

• Figure 1: surviving the storm!



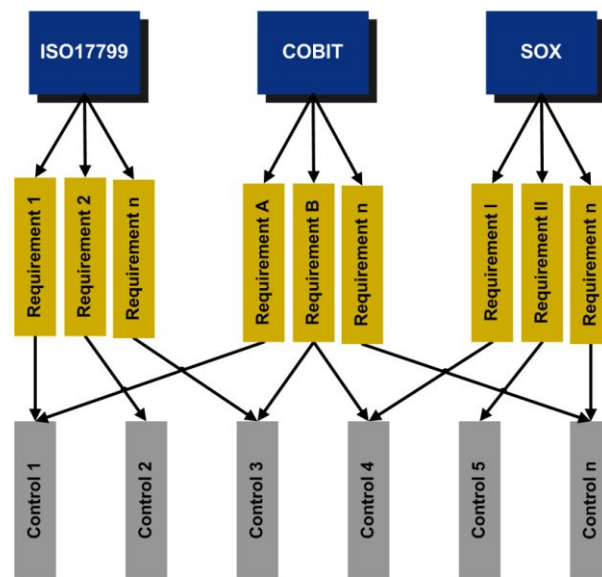
• Figure 2: security requirements (USA).

SECURITY REQUIREMENTS (USA)			
Mandatory	Conditional		Optional
Federal Laws	Industry regulations		Codes of practice
	Government and public administration	Banking and Finance	
Law		Regulation	
Orientation		Orientation	
USA Patriot Act (USAPA) PCOAB SAS 94	Federal Information Security Management Act (FISMA) National Strategy to Secure Cyberspace	Basel II Sound Practices of Operational Risk Gramm Leach Biley (GLBA)	ISO17799 (ISO) COBIT (ISACA)
.	.	.	.
.	.	.	.
.	.	.	.

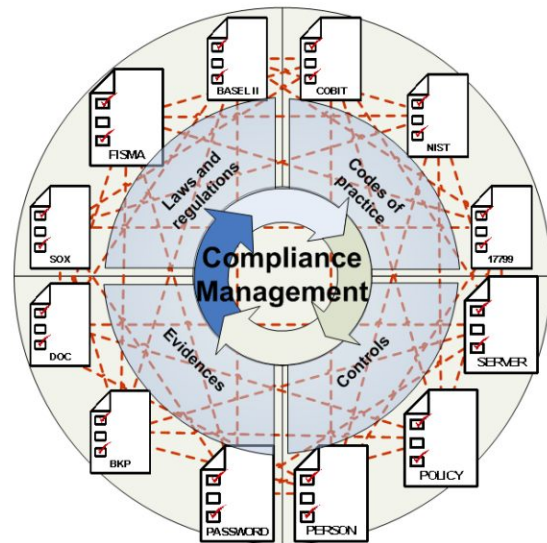
Security managers are responsible for understanding and complying with the frameworks, identifying the requirements to be implemented and providing the necessary means to ensure compliance. The main challenge in this work lies in the complexity generated by independently treating each framework, since each one uses a different type of language, organizes requirements in a different way, requires evidence to be registered differently, and uses different audit processes to prove compliance. And all of these processes take place at different moments and document results in different ways!

However, in spite of the diversity, security controls are often the same (Figure 3). The security manager therefore needs to apply a larger cycle to compliance management, since he or she needs to understand the laws, find out which are the most compliant frameworks, implement the corresponding controls, and record evidence of each control demonstrating compliance with each law applied (Figure 4). All this

• Figure 3: similar controls for different requirements.



• Figure 4: compliance management.



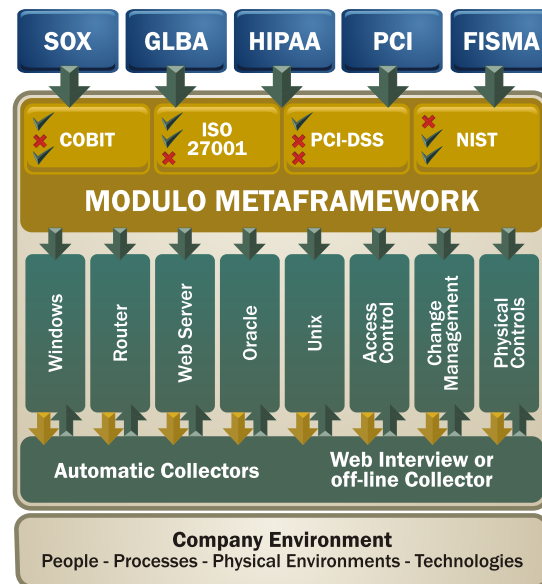
has to be carried out independently and with no integration between the different frameworks, which creates a set of N:N relationships that renders management extremely complex. In order to make this task easier, several attempts have been made by specialists to create a "common language" for all frameworks. Presently, however, a great part of the compliance effort still has to be conducted manually by the security manager. This situation tends to unnecessarily drain the organization's resources, for the company has to bear the high cost of maintaining compliance in a scenario of multiple audits.

The best solution for the security manager would be to deal with the implementation of all the necessary controls and recording of evidence to demonstrate compliance in one single process, automatically organized according to the framework analyzed.

The compliance module was included in Risk Manager 4.1 in view of this scenario. It operates based on a set of frameworks previously registered with the system (called Metaframework™) and uses the entire potential of the risk assessment module to evaluate controls and to record evidence. All this information is organized automatically. Therefore, from one single risk assessment, the system can present the level of compliance with all frameworks on the database. By using this new feature, the security manager will be able to:

- Conduct more efficient audits with lower costs, freeing resources to be used in other important activities;
- Manage security requirements in multiple audits, eliminating redundant costs and unnecessary controls;
- Clearly demonstrate security performance by means of economically feasible actions, in conformity with applicable laws, regulations and standards.

Modulo MetaFramework



The compliance module has registered three frameworks (ISO17799:2005, COBIT 4.0 and PCI/DSS) and other frameworks are to be included in the new versions. It merges Modulo's extensive security knowledge base with the best frameworks in the market, thus creating a powerful tool for security managers.