COBIT Information

Control Objectives for Information & Related Technology

Overview information

COBIT is a generally applicable and accepted standard for good information technology security and control practices. It is intended to provide a reference framework for IS management, security administrators, system users, and professionals who provide IS audit/control/security services to enterprises.

COBIT standards have been developed, maintained, and disseminated by the Information Systems Audit and Control Association (ISACA); click **here** to see their web site.

The standards include 34 information technology processes together with suggested approaches to sustain effective management control over each process. COBIT also provides audit guidelines for information technology assessments plus over 300 detailed control objectives.

Implications for IT management

COBIT "good practices" represent the consensus of international IT experts. Just as Generally Accepted Accounting Principles (GAAP) form the worldwide basis for practice in the accounting profession, so COBIT's "generally applicable and accepted" standards define professional practice expectations for IT management. Those good practices:

- Will help your enterprise optimize the return on it's IT investment, and ….
- Will serve as the yardstick with which IT management performance will be measured when something goes haywire in the organization.

It is therefore prudent to: i) identify distinctions between COBIT standards and your enterprise's current policies, procedures, and practices, ii) avoid problems by erasing as many distinctions as possible, and iii) regularly assess risks associated with any surviving/emerging distinctions. Those steps form the foundation of management control. COBIT defines "control" as:

> *"The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."*

How Unbeaten Path can help

- ☑ **Bill of Health**™ provides 50 robust assessment reports describing your iSeries security status together with a competent prescription to address each identified vulnerability.
- ☑ **Stitch-in-Time**® **Data Integrity Software** quickly and decisively responds to audit challenges about the security of your data. If an unauthorized change was executed in a critical file, Stitch-in-Time provides comprehensive information to enable analysis of that change.
- ☑ **Stocking Stuffers**™ **for SOX** are a collection of products designed to work with BPCS software that can help auditors gather evidence about the integrity of your internal control environment.

Looking at COBIT from a lower altitude

COBIT provides **Management Guidelines** which respond to management's need for control and measurability of the information technology function. COBIT suggests tools to assess and measure the enterprise's IT capability for each of the 34 COBIT IT processes. The tools include, for example, a list of critical success factors that provide succinct, non-technical best practices for each IT process.

COBIT guidance provided to audit professionals is comprised of these three general elements: Standards, Guidelines, and Procedures:

Standards *define mandatory requirements/expectations for IS auditing and reporting by professional IS audit practitioners.*

Guidelines *provide guidance to IS auditors on how to apply the audit standards for each control area so as to competently evaluate each control, assess compliance, and measure the risk of controls not being met. To date, twenty-six guidelines have been issued..*

Procedures *provide examples of methods or processes an IS auditor might follow in an audit engagement.*

Even more details about COBIT standards

Here is the full text of the COBIT standards entitled "IS Standards, Guidelines and Procedures for Auditing and Control Professionals." The document is accessible from the ISACA web site and the most recent update of the publication is dated March 24, 2004. Brace yourself for a single-spaced, 161 page .pdf download. **go-see-it**

Not every one of the 161 .pdf pages has enthralling content. A two-page extraction of very interesting information about risk assessment, vulnerability analysis, audit evidence, assessment documentation, and penetration testing has been prepared. **go-see-it**

Return to IT Security Assurance page