

SCC VOICE

Thoughts and ideas from The Systems Consulting Consortium

How COBIT, ITIL and ISO 17799 Can Help Your Compliance Efforts

Regulatory compliance is having a profound impact on how organizations manage risk and exercise due care. For many, the administrative burden is unbearable. In the last five years, we've observed substantial discussions on the impact of regulations, driven largely by the U.S. Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002. Other regulations with a significant impact include:

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act,
- The Gramm-Leach-Bliley Financial Services Modernization Act,
- The New Basel Capital Accord (Basel II),
- Title 21 Code of Federal Regulations (21 CFR) Part 11, and
- The Health Insurance Portability and Accountability Act (HIPAA).

For organizations in highly regulated industries such as financial services, healthcare and telecommunications, managing compliance with diverse regulatory requirements from a number of national and international sources is extremely expensive and is starting to affect the available budget for legitimate business opportunities that can help the organization compete more effectively within its industry.

Holistic Approach To Compliance Challenges

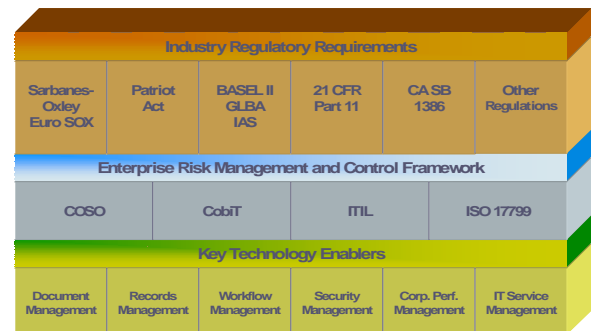
Complying with regulatory requirements does not have to be a burdensome one off activity. There are a number of common themes that run through most regulations. By using a "Compliance Management Architecture" (CMA) framework organizations can save significant time and energy in meeting their compliance objectives.

According to Gartner, "by 2006, public companies that do not adopt a compliance management architecture will spend 50 percent more annually to achieve SOX compliance (0.8 probability). Companies that choose one-off solutions to each regulatory challenge they face will spend 10 times more on compliance projects than their counterparts that take a proactive approach (0.9 probability)."

Compliance Management Architecture Overview

Compliance Management Architecture is a set of internal controls for managing organizations. CMA focuses on IT and technology controls. There are four compatible frameworks within the Architecture:

- **COSO** (Committee of Sponsoring Organizations' Enterprise Risk Management Framework) – Scope is organization wide controls,
- **COBIT** (Control Objectives for Information and Related Technologies) – Satisfies and extends COSO controls related to Information Technology,
- **ITIL** (Information Technology Infrastructure Library) – Satisfies and extends COBIT controls relating to IT Service Management (Problem Management, Change Management, Release Management, etc.),
- **ISO 17799** – IT Security Controls to meet and extend COBIT Security.



Compliance Management Architecture, NAI © 2005

The benefits of an Architectural approach include a common approach to security and privacy requirements, implementation of tried and tested industry best practices and availability of off-the-shelf support material.

[Author: Hamid Nouri, President, Nouri Associates Inc. (NAI), ©SCC, Inc.; October 2005]

Mr. Nouri has over 25 years of experience in the IT industry and has held senior leadership positions at Gartner and Countrywide Funding. He is certified at the Masters level in ITIL and is a Certified Information Systems Security Professional (CISSP).



The Systems Consulting Consortium, Inc.
 P.O. Box 519, Orinda, CA 94563
 888-418-1200 ofc, 925-254-8524 fx
 info@scc.cc (email), www.scc.cc (website)