Sustainable Security for Infrastructure SCADA

Jason Stamp Phil Campbell Jennifer DePoy John Dillinger William Young

Sandia National Laboratories
Albuquerque, NM 87185-0785

***Abstract* — Modern SCADA systems used in infrastructure are threatened by cyber attack, as a result of their higher visibility in recent years and the conversion of legacy stovepipe implementations to modern information technology (IT) systems. Many contemporary efforts statically address obvious errors in the implementation of these systems, but this approach does not foster effective security because of the fluid IT environment. The problem must be addressed such that SCADA security becomes effective and sustainable for the entire system lifecycle, including design, installation, operation, maintenance, and retirement. Only the implementation of effective security governance for SCADA will meet this requirement. Some approaches for security perform well at linking security investment for information assurance to the business goals of the larger corporation but are not readily translatable into actionable practice. Others excel at defining and enforcing security for implementations and procedures but are weak from the perspective of the larger picture. The strengths of the two groups can be leveraged to create effective security governance for SCADA, reaching across the organizational structure of the company and creating the foundation for sustainable security.**

***Index Terms* — SCADA systems, computer security, data security, management (information systems).**

I. Present and Future Security for Automation Systems

An automation system, often referred to as a process control system (PCS) or supervisory control and data acquisition (SCADA) system, is critical to the safe, reliable, and efficient operation of many physical processes. PCS and SCADA are used extensively in infrastructure like electric power, water, petroleum, and natural gas, as well as in various manufacturing operations. The Sandia interpretation of the terms PCS and SCADA include the overall collection of control systems that measure, report, and change the process. Essentially, any subsystem that electronically measures state, alters process control parameters, presents/stores/communicates data, or the management thereof is subsumed in our consideration of SCADA.

Unlimited release – approved for public release.

Sandia National Laboratories report SAND2003-4670C.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

A. Current SCADA Security Conditions

The present state of security for SCADA is not commensurate with the threat or potential consequences. The industry has generated a large base of relatively insecure systems, with chronic and pervasive vulnerabilities that have been observed during security assessments. Arbitrary applications of technology, informal security, and the fluid vulnerability environment lead to unacceptable risk. [1]

An analogy can be made between security for control systems and fuel economy for vehicles. Until the fuel crises of the 1970s, automobiles were built based on available technology, increasing performance and convenience with small concern for energy efficiency. Once fuel became precious, the design philosophy changed to include efficiency as a design goal, and now it is ingrained as a critical consideration (with a few exceptions).

Similarly, SCADA systems are evolving as new technology is added for performance and convenience, only this time ignorant of security. Unfortunately, the problem is more acute since poor fuel efficiency is only harmful in a circumspect way (pollution, international dependence, etc.) while the possible circumstances from SCADA intrusion are critical [2, 3].

Security for SCADA is typically five to ten years behind typical information technology (IT) systems because of its historically isolated stovepipe organization. However, security can become a design consideration either after some event or before. If one waits until after a cyber attack, then much catching up will be required and the owner starts at a disadvantage (in addition to recovering from the damage caused by the attack). However, prudent investment in system security now reduces risk both immediately and in the future. Possibly, a precautionary company may deter adversaries from targeting it, by identifying and managing risks through an effective security program.

B. Components of Sustainable Security

Security for future SCADA depends on three elements:

- Secure implementations of technology and procedures managed by effective security administration, including enforcement and audit;
- Better security technology, including SCADA-specific

capabilities; and
- Third-party assessment of administration and implementation.

1) Security Administration

Security administration is paramount to manage security risks. Vulnerabilities that may be exploited by an attacker are related to the implementation and operation of a particular SCADA system, managed by people whose actions are defined and controlled by the system's security administration. Realistically, it is impossible that any SCADA operation is free of vulnerability and immune to threat. In the fluid IT environment, changing conditions demand constant vigilance. Only through constant evaluation and maintenance can security be sustained; therefore, effective and sustainable security for SCADA depends on effective security management.

Modern SCADA, or even SCADA in modern times, must be addressed and managed in a style appropriate for a critical IT system. For some time not including the latter part of the twentieth century, SCADA and other automated control systems enjoyed freedom from concern for security, and concentrated their engineering and design to features which thwart non-human adversaries, such as weather, electromagnetic interference, material fatigue, and the like. The rise of the so-called Information Age has introduced the malevolent human threat into a position of prominence, probably permanently. As long as SCADA systems offer the opportunity for manipulation to the benefit of some people to the detriment of others, they must be protected to ensure that their operation is appropriate and according to their design. Commodity trading for energy increases the likelihood for manipulation and illicit gain, while the proximity of SCADA to critical infrastructure affords desirable calamity for the enemies of secular capitalism and the rule of law.

One key element for effective security administration is the need for dedicated security personnel (who are knowledgeable about SCADA and automation systems). Generally speaking, it is an ineffective practice for SCADA system administrators and managers to also bear the responsibility for security. Cutbacks in staff and increasing system complexity in most cases deny adequate attention to security from SCADA operations personnel. The SCADA security staff has a heavy training burden to keep abreast of threat and vulnerability developments; this reinforces the notion that the security officer's attention be uniquely directed to security. Furthermore, the SCADA security administrator must also have clear authority to alter running configurations (subject to reliability concerns) to mitigate vulnerabilities, and that power must derive from clear and direct policy.

During assessment work, many permutations of political interaction among IT and SCADA staff have been observed. Occasionally, there was friction between the corporate IT staff and the SCADA engineering team. A SCADA security officer should necessarily have a background in modern IT security, but should (appropriately) be a member of the SCADA staff. Potentially, this arrangement may foster better cooperation since the SCADA security function relates to both IT and SCADA.

The recommended taxonomy for effective security governance is presented later in this document.

2) Improved Technology

In light of the paramount importance of administration for sustainable security, it is critical to also embrace the role of technology to achieve overall security for future SCADA. The development of secure technology, protocols, and standards will equip SCADA security personnel with necessary tools for secure implementation, both now and in the future. Unfortunately, the primary reaction to insufficient security across the SCADA industry has been that improved technology is the answer for the malaise, apparently at the expense of effective security administration. The correct tradeoff between technology and administration at organizations using SCADA should be that investment is primarily directed at the development of effective administration, while for public research outlays funding should be appropriately directed toward programs for sustainable security as well as investments in technology. Some desirable advancement include secure protocols, low-cost encryption for serial SCADA, application-layer stateful inspection for SCADA firewalls, accounts and logging for remote telemetry units (RTUs), etc. On their part, vendors and integrators will react favorably to industry desire for SCADA security when the opportunity to gain competitive edge through security capability becomes apparent, and already some are pursuing security programs. Standards bodies can facilitate security amelioration by educating stakeholders, in addition to influencing efforts within and across industries to leverage investment and improve cohesion.

3) Third-Party Assessment

While internal auditing and assessment of security administration and system implementation are essential for security, regular external evaluations are also critical to catch residual problems perhaps caused by the organization being too close to issues or unaware of new tactics and tools. Unfortunately, contemporary security assessments may or may not be helpful to organizations with nascent security programs. To their own misfortune, many companies contract for a security audit to meet internal or regulatory pressures only to be presented with results from penetration tests and vulnerability scans, which are less than helpful to say the least. Even if each of the discovered vulnerabilities were addressed, the organization has not received any guidance that could help them build a sustainable security program, and it is likely that significant problems will crop up and remain unaddressed because the security culture did not change. Likewise, standard red team engagements do not discover all vulnerabilities, and may only hint at managerial issues that lie at the root of insecure and flawed implementations. (Often, red teams are used as brute force tools against internal

political barriers, with flaws in security implementations as only a secondary priority.)

For now, an assessment process that focuses primarily on security management and organizational culture while addressing only glaring vulnerabilities in implementation is the best balance for most SCADA systems. In the future, when an organization demonstrates administrative maturity in their security program, then independent analysis by third-party red teams and vulnerability analysis perform an important role in discovering lapses and flaws. Until then, however, the results from these types of audits must be carefully used and interpreted.

II. Recommendations for Effective Security Administration

Two categories of security management are available. The first group relates security and IT risk management in general to the business cycle, and the second establishes a family of management documentation to guide security.

Balance among these creates the optimal situation for security administration, where all levels of personnel (from upper management to SCADA technicians) coordinate to instantiate and practice effective security administration across the entire breadth of the lifecycle (design, implementation, operation/maintenance, and retirement).

A. IT Control Framework

The most comprehensive approach for IT systems management integrates elements of IT control into the business cycle. Security is addressed as part of the company's comprehensive risk management program, and as such may be considered in terms of investment and return subject to requirements for public protection (which is particularly important for infrastructure). Coupling the need for security to the organization's business model is the most direct way of evaluating security investment.

A recent article defines policy as "the set of business rules that represents the enterprise's tolerance for risk and the security measures that enforce that stance" (Broadbent) [4]. The study advocates the use of industry standards:

> *"Policies should be based on industry standards, such as COBIT or ISO 17799, because they lay out security program criteria and the basis for comprehensive security assessment and administration."* (Broadbent) [4]

For the particular purpose at hand CobiT [5] has the best balance among breadth, depth, and prospects for future maintenance. CobiT is properly called a control framework, defined below. There are alternatives, such as SysTrust and the Information Technology Control Guidelines, among others. A survey of these is available [6].

The value of CobiT is in its comprehensiveness, which is a balance amongst risk identification and its management through administrative and technical controls. CobiT is maintained by the IT Governance Institute (ITGI). As the name of the maintaining organization implies the goal of CobiT is to provide better IT governance [7]. Security, as it is usually understood, is a proper subset of governance.

The concepts of control and control objective are central to CobiT:

> *"Control: The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."* (CobiT) [8, page 12]
>
> *"Control Objective: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."* (CobiT) [8, page 12]

Using the two definitions above, a control framework is defined as a taxonomy of control objectives. CobiT is a partitioning of industry's current estimation of a complete set of control objectives.

CobiT consists of a three-tiered hierarchy: control objectives grouped into processes, grouped in turn into domains. There are 318 control objectives grouped into 34 processes grouped into the following four domains:

- Planning & Organisation
- Acquisition & Implementation
- Delivery & Support
- Monitoring [5]

The hierarchy is clearly visible in the tag for each control objective. For example, "PO2.3" would be the third control objective in the second process in the PO domain ("Planning & Organisation"):

> *"PO2.3. Data Classification Scheme (control objective): "A general classification framework should be established with regard to placement of data in information classes (i.e., security categories) as well as allocation of ownership. The access rules for the classes should be appropriately defined."* (CobiT) [8, page 37]

A common complaint about the use of control frameworks for IT administration is that the expression of the controls that realize and enforce the control objectives is not as straightforward as most expect. Indeed, the unease with the link from control objective to the control may be the primary reason that tools such as CobiT are not readily applied. One solution is to use industry standard structures for security administration to enforce control objectives derived from CobiT, thus retaining the unique strengths of the control framework approach.

Related to SCADA security administration, the control framework provides a starting point for the business administration of the enterprise employing SCADA. **The business leadership employs the CobiT control framework for the development of control objectives that accurately relate security to the business goals of the enterprise.** The tools used to enforce the control objectives are the SCADA security policy, security plans, implementation guidance, configuration management, and auditing/assessment (see Figure 1).

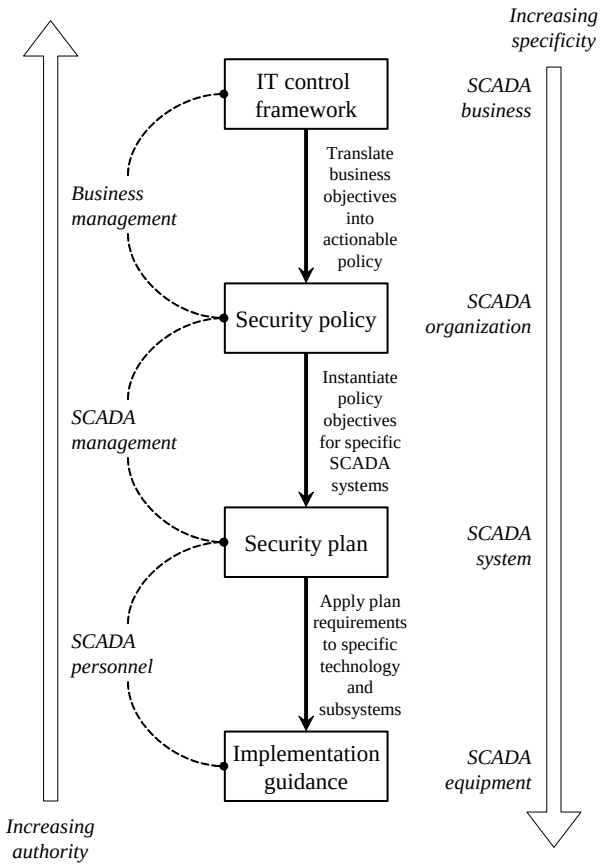

Figure 1. Relationship for SCADA security administration hierarchy.

A potential starting point for companies beginning to use the control framework concept is higher-level control objective DS5, "Manage System Security," and its associated 21 lower-level control objectives. Other control objectives can be integrated as the process matures.

An alternate starting point is the 2003 CobiT Quickstart guide. Quickstart is a subset of CobiT that can "serve as a starting point" for CobiT implementation. Only those control objectives that are considered the most critical are included, so that the implementation of fundamental CobiT principles can take place easily and relatively quickly. (CobiT) [9]

Sandia National Laboratories has not reviewed Quickstart but anticipates it being an effective path to take for CobiT implementation. For the latest information about Quickstart see the Information Systems Audit and Control Association (ISACA) website (www.isaca.org).

B. SCADA Security Policy

Unfortunately, the word policy has become the generic catchall for any semi-formal documentation within an organization describing its thoughts on any subject, from paternity leave to privacy. In an effort to distinguish policy for SCADA administration from the policy quoted by customer support representatives and the like, elaboration will be made forthwith.

Security policy for SCADA administration translates the desired security and reliability control objectives for the overall business into enforceable direction and behavior for the staff to ensure secure SCADA design, implementation, and operation. An organization should have one security policy with authority over all SCADA systems, connected elements, and personnel. The unique characteristics of SCADA necessitate a complete policy separate from the normal company information policy. The policy is formulated by the SCADA management staff, with input from the business leadership, which fosters a strong link between the control framework and the policy and mutual accord from what are typically diverse groups.

Elements of the security policy may be broken down into two major classifications [10]:

- Program level policy - applies to all activities relating to SCADA
- Issue-specific policy - delineates direction and security for individual subjects

This structure best allows for the situational condensation of the policy to apply to activities (and hence, applicability for groups of employees like network administrators, operators, et. al.). Simplification of policy that does not compromise its effectiveness is always preferable to the bludgeoning application of the entire document.

Each section of the security policy may include the following attributes:

- Purpose and goals
- Scope and applicability
- Statement of the organization's position
- Roles and responsibilities
- Compliance/enforcement
- References

Although this specification for the security policy is similar to the NIST description [10], the collection of general and issue specific policy is augmented by the addition of control objectives and its overall derivation from the control framework. The policy purpose, goals, positions, etc. relate specifically to higher- and lower-level control objectives, which links the policy more effectively with business objectives. Other verbiage for the policy statements can leverage existing work (NIST, ISO 17799 etc.). One possible framework for the SCADA security policy, which could be tailored to meet the security requirements of a specific SCADA operation, is shown in Figure 2.

Some components of the SCADA security policy include definitions of critical organizational elements and positions for the automation systems security administration, the need for data categorization and ownership, and an introductory description for important elements of the automation information architecture. The security policy must also create and enforce the risk management program for automation security, which is a critical consideration for evaluating vulnerabilities and their security controls (both technical and administrative), along with the relevant security investments and the residual risk (which must be evaluated and accepted). The risk management program policy also specifies its review cycle, which contributes to ongoing security through risk reevaluation. Other sections of the policy address data

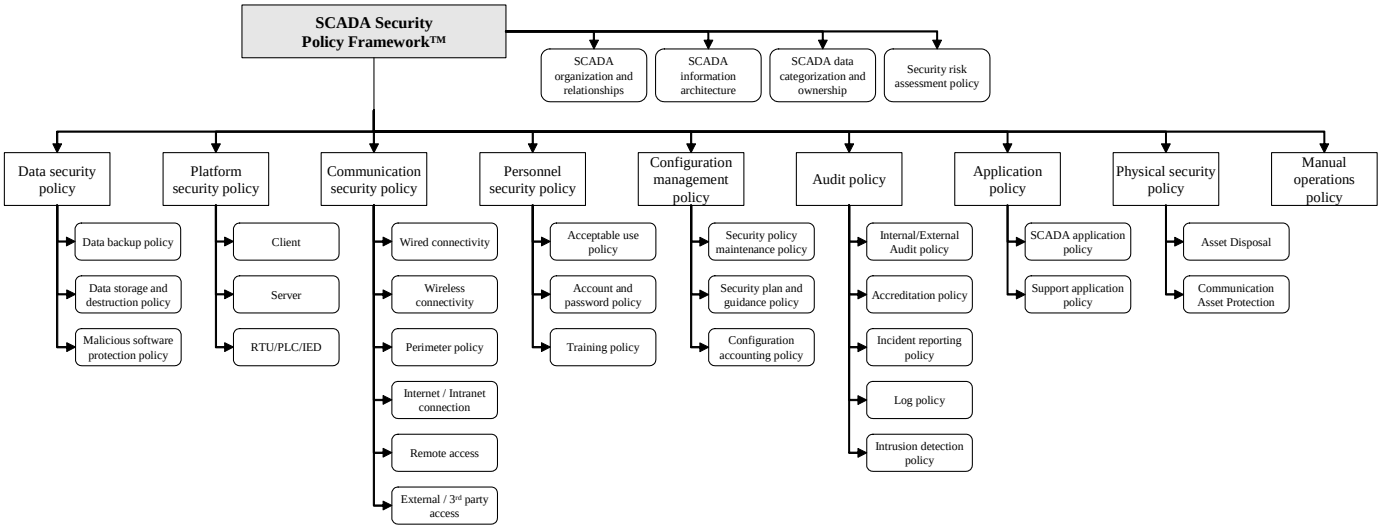

Figure 2. Framework for SCADA security policy.

security, platforms, communications, manual operation (including exercises), personnel, etc. Also, security training is essential for understanding policy and requirements, and staff compliance is predicated upon adequate awareness; together, these emphasize the importance of the training section of the SCADA security policy.

Furthermore, the security policy must mandate effective enforcement (analogous to controls). An essential element of the security policy is the necessary creation of security plans for specific systems or subsystems, as well as implementation guidance for specific technologies. Other components such as configuration management and auditing/assessment provide additional control. Since these important enforcement controls reach across administrative categories, they are addressed separately in later sections.

C. Security Plan

The SCADA security plan enumerates specific security guidelines for systems or groups of systems based on fundamental concepts from the security policy. Effectively, the plan instantiates concepts from the policy. For the SCADA system, the plan is the core security document for implementation, operation, and maintenance. This style of security plan is very similar in concept to the NIST definition [11]. (It is also comparable to the Information Assurance Plan described in military infosec policy.) The security plan details the collection of controls and control practices necessary to meet the control objectives of the security policy and control framework, and will be considerably more technical. Elements of the security plan can be garnered from statements of industry practice or best practice.

D. Implementation Guidance

Implementation guidance enforces the security plan and policy for the implementation of specific technologies. Typically, implementation guidance will enumerate a compilation of directives for the configuration, installation, and maintenance of equipment or software. Implementation guidance will be almost entirely technical. For example, there may be an implementation guide for the application of password checking software on some particular computing platform. (Taking the example further, the need for the software and its configuration are necessary to meet the requirements of the security plan, which in turn satisfy the demands of the SCADA security policy, derived from the control framework based on the business objectives of the company.) Other implementation guides will address subjects like network cabling, Ethernet switches, SCADA applications, operating systems, computing platforms, etc. Adherence to the relevant implementation guidance and to the security plan is tabulated in the system's configuration management.

E. Important Components of Security Enforcement

Although each successively detailed element for security administration necessarily enforces its antecedent, enforcement must at some point bridge administration to implementations. Two critical elements of enforcement that impose principles from security administration on the system implementation and users of the system are discussed.

1) Configuration Management

Configuration management is the process of managing the implementation details for the system and its components over the entire lifecycle, including design, installation, and maintenance. It is also adequately defined by IEEE Std-729-1983:

> *"The process of identifying and defining the items in the system, controlling the change of these items throughout their lifecycle, recording and reporting the status of items and change requests, and verifying the completeness and correctness of items."* (IEEE) [12]

The need for configuration management will be apparent from the set of control objectives, and the configuration management program is an essential enforcement control in the security policy. It is a necessary tool required to impose

security precepts from security plans and relevant implementation guidance. Without configuration management, enforcement of security becomes less formalized, offering greater opportunity for inadvertent vulnerabilities. In the case of a recently discovered software weakness, patching may be incomplete if the extent of the application of the affected software in the SCADA system is uncertain. More importantly, configuration management along with system logs and other sensor information are critical for productive system auditing.

2) Auditing

Auditing is a critical step for the enforcement of the procedural and technical security measures (controls or control practices) in the system. The existence of an effective auditing program that contributes meaningfully to SCADA security meets requirements for security enforcement in the security policy and plans. Requirements for the necessary detail and repetition of the audits must be adequate to ensure compliance with the security controls but below the threshold of nuisance. Auditing may be performed internally or externally, with some mixture of both an optimal solution.

F. The Enforcement Cycle for SCADA Administration

As has been noted, each element in the administrative framework enforces other constituents. Annotated, the enforcement cycle for the proposed SCADA administration architecture is as follows:

- The IT control framework enforces the business direction of the company.
- The SCADA security policy enforces the IT control framework.
- Security plans and implementation guidance enforce the security policy.
- Configuration management enforces the security plan and implementation guidance.
- Auditing enforces configuration management, security plans, and implementation guidance.

Overall, assessment (internal and external) enforces the entire chain of security administration.

III. Conclusion

SCADA security depends on security administration, secure technology, and assessment, of which administration is the key for sustainable security. Control frameworks provide the best translation from business objectives and system lifecycle to control objectives for system security. Development of a security policy and security plans best provides effective and enforceable administration, which is the foundation for sustainable SCADA security.

In the case of any business using SCADA, the business leadership takes the lead in adapting the CobiT governance structure to their situation. Later, the combined business and SCADA administration translate the desired control objectives into the SCADA security policy. In turn, the policy is instantiated for a particular SCADA system through the efforts of the SCADA leadership and engineering personnel. Implementation guidance for specific technologies is developed to enforce the security plan, and configuration management/auditing provide additional important enforcement tools.

Acknowledgements

Funding for the composition of this article was provided by the DOE National Energy Technology Lab.

Acronyms

CobiT ..... Control Objectives for Information and related Technology
DS ..... Delivery & Support
IEEE..... Institute of Electrical and Electronics Engineers
IT..... Information technology
ITGI ..... IT Governance Institute
ISACA ..... Information Systems Audit and Control Association
ISO..... International Organization for Standardization
LAN ..... Local area network
NIST ..... National Institute of Standards and Technology
PCS ..... Process control system
PO ..... Planning & Organisation
RTU ..... Remote terminal unit
SCADA..... Supervisory control and data acquisition

References

[1] *Common Vulnerabilities in Critical Infrastructure Control Systems*, Jason Stamp, John Dillinger, William Young, and Jennifer DePoy, Sandia National Laboratories report SAND2003-1772C, Albuquerque, New Mexico (2003).

[2] *eTerrorism: Assessing the Infrastructure Risk*, Robert Lemos, ZDNet Australia, http://www.zdnet.com.au/newstech/security/story/ 0,2000048600,20267698, 00.htm (27 August 2002).

[3] *Frontline: Cyber War!* Public Broadcasting System, http://www.pbs.org /wgbh/pages/frontline/shows/cyberwar/view (24 April 2003).

[4] *A Security State of Mind*, Marianne Broadbent, CSO magazine (A CIO Publication), http://www.csoonline.com.au/index.php?id=468304772& fp=8&fpid=2 (25 July 2003).

[5] *CobiT Executive Summary (3rd edition)*, CobiT Steering Committee and the IT Governance Institute (July 2000).

[6] *An Introduction to Information Control Models*, Philip Campbell, Sandia National Laboratories report SAND2002-0131, Albuquerque, New Mexico (September 2003).

[7] *Board Briefing on IT Governance (2nd edition)*, IT Governance Institute, http://www.itgi.org/Template_ITGI.cfm?Section=About_IT_ Governance1&Template=/ContentManagement/ContentDisplay.cfm&C ontentID=6606 (2003).

[8] *CobiT Control Objectives (3rd edition)*, CobiT Steering Committee and the IT Governance Institute (July 2000).

[9] *CobiT Quickstart*, CobiT Steering Committee and the IT Governance Institute (2003).

[10] *NIST Special Publication 800-12: An Introduction to Computer Security – The NIST Handbook*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington, DC, http://csrc.nist.gov/publications/ nistpubs/800-12/handbook.pdf (February 1996).

[11] *NIST Special Publication 800-18: Guide for Developing Security Plans for Information Technology Systems*, Marianne Swanson, Federal Computer Security Program Managers' Forum Working Group, Washington, DC, http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.pdf (December 1998).

[12] *IEEE Standard Glossary of Software Engineering Terminology, IEEE Std 729-1983,* IEEE Computer Society, the Institute of Electronical and Electronics Engineers (1983).