IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITP4562

# Assurance Through Control Objectives, A Governance Basis for Managing Corporate Information Assets

Dan Shoemaker and Antonio Drommi
College of Business Administration, University of Detroit Mercy
Detroit, Michigan 48219
(313) 993-3337 voice (313) 993-1052 fax
Shoemadp@udmercy.edu and drommia@udmercy.edu

## INTRODUCTION

Information security systems have to meet two logical criteria to be effective. First the protection must be *complete*, in the sense that the response should address the entire problem (e.g., everything that requires assurance is secured). And second the safeguards have to be *uniform*. That is, there should be an organization-wide commitment to security. The first principle is established through a systematic implementation strategy. The second requires the organization to define substantive policies, roles and responsibilities, educate employees and describe and enforce accountability. The problem is that this effort takes time and precious resources.

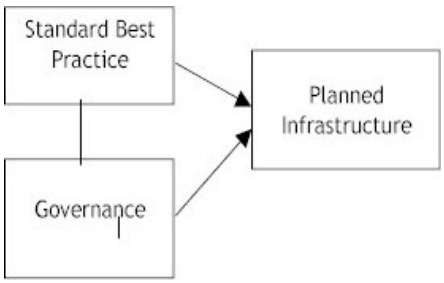
Nevertheless there are very real and substantive consequences if the security protection scheme is inconsistent. For example, a secure network without policies to control the people who operate it can be breached no matter how sophisticated the technology employed. One recent illustration of how that exact scenario played out is the national database, which was raided by four inside employees for the credit information of 30,000 individuals. That information was sold to an identity theft ring, which subsequently used it to commit massive credit card fraud.

As a matter of fact there are actually very few breaches of corporate information security that directly involve the technology. Specifically, seventy two percent of the serious losses recorded by the FBI in 2001 originated from the actions of inside people rather than hackers (CSI 2002). Which underscores the principle that, no matter how robust the encryption scheme, there are no practical safeguards unless everybody involved understands what constitutes a violation and what the consequences are for committing one. So, the correct response in nearly three-quarters of the cases last year should have been a systematic set of organizational control procedures, not a more sophisticated firewall.

## THE THREE BUILDING BLOCKS OF A SYSTEMATIC SOLUTION

Which conveniently leads us to the theme of this paper. Control objective based security frameworks are constructed around three high-level principles. Figure One itemizes these and illustrates their relationship to each other.

*Figure One: Fundamental Components of Information Assurance*




The first principle is standard best practice. This term just denotes the fact that the collective body of knowledge of the profession can be tapped for expert advice about the best way to respond to a practical concern. When best practices are formally recorded and conveyed as a set of recommendations this is called a "standard". Standards are disseminated by acknowledged and authoritative entities.

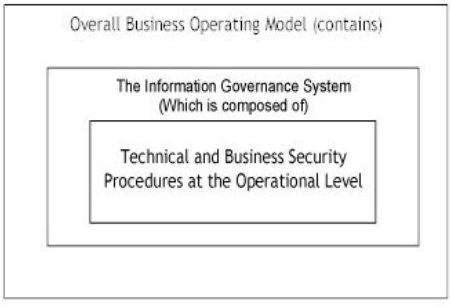
The second principle is governance. This is the generic organizing and control function that underwrites any form of proper management. Where that governance applies directly to the supervision of the organization's information assets it is specifically termed "information governance". The information governance function seamlessly integrates every aspect of information and technical assurance into a single coherent and continuously evolving response. In that respect substantive information governance is attained through a tangible, organization-wide system of rational policies, and their attendant control objectives. Figure Two outlines that.

The process focuses specifically on establishing an integrated and documented set of policies, which are aimed at ensuring that the complete set of information assets is fully secured. These must be sufficiently detailed to allow employees in the entire organization to understand how to establish tangible control over their applicable operational activities.

Since that implies a comprehensive set of components that have to be related, there is an implicit requirement for some sort of infrastructure. Which brings us to the final principle, organizational infrastructure. The role of infrastructure is to make two intangible concepts real. Figure Three portrays that.

An infrastructure is nothing more than the particular embodiment of the concepts of best practice and information governance in a given organization. It is always documented in an explicit and traceable way. Tangibility is the key attribute. Accordingly, security infrastructures are implemented by the deliberate deployment of a set of rationally derived relationships and processes, embodied as a specific framework of control objectives. Operationally, a security infrastructure forges a specific link between the overall business strategy and information security requirements. This is illustrated in Figure Four.

*Figure Two: Levels of Information Management*



A formal strategic planning and development process such as this represents the ideal means to transform intangible concepts into a working day-to-day security operation. However in order to do this, the generic best practices specified in the expert model have to be adapted to the specific environment. The practical approach to this is hierarchical. Or in essence an optimum solution is engineered top-down. In practice this is called "tailoring" (or sometimes "customization"). Tailoring creates a tangible, complete and rational document set, which embodies all necessary security activities down to the level of utilitarian tasks. The end product is a set of explicit procedures that convey the exact substance (e.g., assigned activities) of the assurance tasks to every employee sufficient to ensure effective coordination of the work.

*Figure Three: Relationship of the Concepts of Best Practice and Governance to Infrastructure*

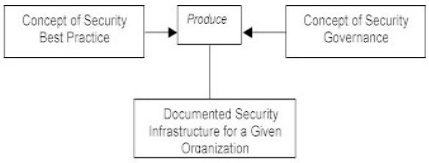
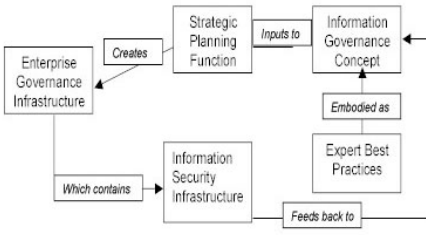



*Figure Four: The Relationship between Strategic Planning and Security Infrastructure*



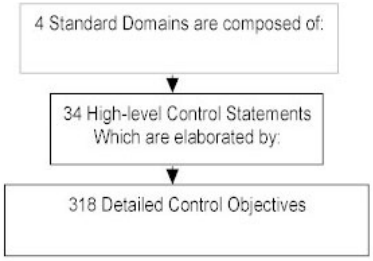

**The Three Standard Models**

There are three globally accepted frameworks that embody these three principles in a security infrastructure. These are COBIT (ISACA, 2002) ISO/IEC 15408: (ISO, 1997) and BS 7799 (BSI, 2000). Each has a slightly different orientation but they all convey a complete conceptual model, with the necessary actions spelled out through a distinctive set of control objectives. These control objectives are nothing more than the explicit definition of the desired result or purpose to be achieved by the security element they are attached to. Accordingly, the aggregate set of control objectives provides a concrete and detailed picture of the security solution that each of these standards represents.

**COBIT**

COBIT supports the development of clear policies and procedures that enforce operational control over IT. It was developed out of 41 primary sources, which is important since legitimacy is an essential requirement of any best practice standard. COBIT assumes that effective security control is based on four domains labeled: *1) planning and organization, 2) acquisition and implementation 3) delivery and suppor*t and *4) monitoring*. Each of these domains is further defined by a set of 34 high-level control objectives, which embody 318 itemized control objectives. Figure Five outlines that structure:

*Figure Five: The COBIT Hierarchy of Control Statements*




We are going to employ the first of these domains (planning and organization) to illustrate this model. The planning and organization domain (PO) contains eleven of the 34 high-level control objectives, which essentially represent the topics that must be specifically addressed as part of the security assurance for that domain. These eleven are:

| | |
|---|---|
| PO1 | Define a strategic IT plan |
| PO2 | Define the information architecture |
| PO3 | Determine the technological direction |
| PO4 | Define the IT organization and relationships |
| PO5 | Manage the IT investment |
| PO6 | Communicate management aims and direction |
| PO7 | Manage human resources |
| PO8 | Ensure compliance with external requirements |
| PO9 | Assess risks |
| PO10 | Manage projects |
| PO11 | Manage quality |

Since these are topics rather than explicit procedure specifications their precise implementation is essentially unclear at this level. Therefore each is further elaborated by 95 explicit control objectives. A number of these are aligned to every high level objective but there is never any less than one for each. Overall there are 318 control objectives in the COBIT model. These provide the real value since they specify in very precise terms what must be done to satisfy its general purposes. We are going to use the first control objective PO 1.1 (*IT as part of short and long range planning*) to demonstrate the level of specificity that this offers. That objective elaborates, the high-level control objective PO1 (*define a strategic IT plan*) which is part of the Planning and Organization (PO) Domain. This objective simply specifies that IT must be included as part of the long- and short-range business planning process. The steps that are required to satisfy this objective are itemized within the body of the description (from COBIT, 3rd Edition):

**PO 1.1 IT as part of long- and short-range planning**

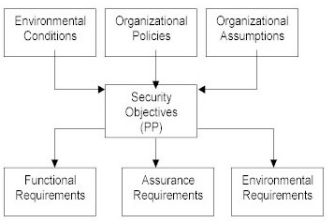
*Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organization's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organization's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organization.*

It cannot be stressed enough that the COBIT framework embodies 317 other statements of this type. As such, it should be clear that it offers very detailed guidance about the actions that must be taken to secure an IT function. The next model at is similar in its focus but it allows the organization to integrate security requirements into any information technology product or process.

**Example: Establishing Information Security through ISO/IEC 15408**

The goal of ISO/IEC 15408:1997 is to embed detailed information security requirements into the functional specifications of any IT product, system, or process. There are three parts to this standard. Each describes the implementation process for security controls that can be used to describe the behavior of a given Target of Evaluation (TOE). These control objectives are captured in a generic reusable Protection Profile (PP), which is then specifically tailored for a given product as a Security Target (ST). Figure Six illustrates this:

*Figure Six: Implementation of a 15408 Protection Profile*



Implementation revolves around the formulation of a reusable Protection Profile (PP), which in essence is the general set of selected security objectives for the organization. The PP allows an organization to create a global set of security requirements (Note: consumers can also employ a PP to specify IT security features to prospective suppliers). Operationally this profile is specified top-down, through the involvement of stakeholders. However, as the drawing illustrates the actual implementation of the security function is bottom-up because the explicit form of the security for any given instance is tailored to each security target.

These security objectives are then tailored into the specific functional, assurance and environmental requirements for any given security target. The security target (ST) expresses the particular security requirements of a given product as well as the security functions to be evaluated. Where the STs are represented as a definition of outcomes for assessment it is called a target of evaluation (TOE). Targets of Evaluation (TOEs) are composed of security objectives and assessment criteria specified in the standard.

The final model adds the policy dimension to the control objective concept. Because of that, it is the only one that builds a formal and permanent organization-wide information security management system (ISMS).

**Example: Establishing Information Assurance through ISO/IEC 17799**

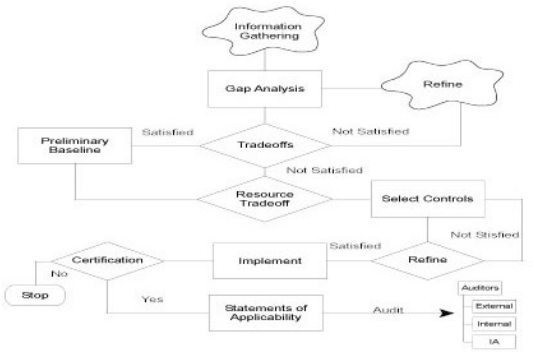
The International Organization for Standardization (ISO) created ISO/IEC 17799:2000 as the means to implement a comprehensive and persistent information security management system (ISMS). It touches on every aspect of IT security. It forces companies through a step-by-step assessment of their business needs and appropriate responsibilities with respect to security. It centers on developing a set of rational policies, which are designed to ensure that every aspect of the company's information resources will be secured.

The information security management system is formulated based on ten security domains containing 127 high-level Control Objectives. The complete set of these control objectives is assumed to describe and embody all aspects of security for information and IT. By developing concrete responses to each of the high level objectives, the manager can ensure that a capable IT control system is in place for any type of organization at any level of security desired.

This originates from a risk assessment. Management uses this approach to map where the organization is in relation to the best-practice ideal defined by the Standard. Figure Seven describes that process.

ISO/IEC 17799 bases the security solution on comprehensive definition of policies, roles and responsibilities. This approach creates a complete and systematic enterprise governance response rather than a specifically IT oriented one. As we said earlier, the primary criterion for judging the effectiveness of a security solution is whether it is complete. This model provides assurance that the entire enterprise will be completely, correctly (with respect to best practice) and effectively secured, which might make it the most attractive of the three popular control objective based approaches discussed here.

*Figure Seven: Sample Process for Implementing 17799*




## SUMMARY AND A SHORT CONCLUSION

Information assets are more difficult to account for and control than conventional physical assets. That is, because IT work involves the production of virtual, highly dynamic products, which makes it hard to know WHAT to secure let alone how to do it properly. This has been such a universal and pervasive problem that the logical response was appropriately best practice models that can provide the comprehensive basis for information security assurance.

The International Standards Organization (ISO) has developed two formal reference models (ISO/IEC 15408 and ISO/IEC 17799) and the Information Systems Audit and Control Association/Foundation (ISACA/F) has provided another (COBIT). These frameworks serve both as a fundamental checklist for itemizing the elements involved in assuring a virtual asset as well as a foundation for building common understanding of the mechanisms required for security assurance.

This is highly advantageous because, notwithstanding the issue of whether technology can ever fully confront all of the issues associated with information security, a governance solution is more easily understood and accepted by the non-technical managers who oversee the bulk of the company's work. Furthermore security governance can be implemented without involving expensive technology, which means that it is less likely to involve capital investment. Finally it creates a comprehensive and consistent policy and procedure framework, which communicates and coordinates security assurance procedures corporation-wide. And since all of these are built through a definition process they can be altered in a rational and systematic fashion to meet changes in the original situation. Given the challenges of an uncertain age, a detailed governance based audit and control infrastructure built from expert advice and capable of serving as the basis for reliable and comprehensive information security protection, is an invaluable asset.

## REFERENCES AND ADDITIONAL READING:

*1. 7799 Standards Can Enhance Your Organization's Information Security Program* Business/Technology Editors, InfoWorld, 10, 2001

2. Ashton, Gerry, *Cleaning up your Security Act for Inspection*, Computer Weekly Jan 18, 2001

3. British Standards Institution, *BSI 7799:2, 1999*

*4. Internet Business News*, CSI survey, *FBI/Computer Security Institute, April 8, 2002*

5. Dorofee A.J., JA Walker, RC Williams, Risk Management in Practice, Crosstalk, Volume 10 #4, April 1997

6. European Accreditation (EA), EA 7/03, EA Guidelines for the Accreditation of Information Systems

7. Favell, Andrew, *Don't Leave it to Luck*, Computer Weekly, Oct 11, 2001

8. Goodwin, William UK's security code of practice becomes worldwide standard Computer Weekly, Jan 25, 2001

9. Information Systems Audit and Control Association (ISACA), *Framework*, COBIT (third edition)

10. Mcclure, Stuart, SECURITY WATCH: Mass manipulation isn't reserved just for presidential elections: IT world be warned, InfoWorld, Nov 20, 2000

1. Simons, Mike, *NHS takes unpopular BS 7799*, Computer Weekly, Jan 18, 2001

2. Swanson, Marianne, *Security Self Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology NIST 800-26, November 2001

3. United Kingdom Accreditation Service (UKAS), Assessment of Approved and Notified Bodies

4. United Kingdom Accreditation Service (UKAS), UKAS Directory of Accredited Inspection Bodies

5. United Kingdom Accreditation Service (UKAS), UKAS Application for Approval.