107

Common Models for Architecting an Enterprise Security Capability

Matthew J. Decker

107.1 Introduction

Enterprise security architecture (ESA) comprises all aspects of a security program, including corporate leadership, strategy, organizational structure, policies, procedures, standards, and technical components. The purpose of this chapter is to present a road map for achieving an effective ESA, via implementation of common security models, standards, and practices.

107.2 System Security Models

The three system security models briefed in this section are well known, and have formed the basis for the development of secure systems, pursuant to the needs of the entities that employed them. Each offers

AU7495—Chapter107—27/1/2007—12:27—VELU—14767—XML MODEL CRC12a – pp. 1413–1430.

a different definition for a secure system. This drives home the point, at a most fundamental level, that an organization must clearly define security in terms of what makes sense for them. The models are presented in the order that they were published, from earliest to most recent.

107.2.1 Bell and LaPadula Model

The Bell and LaPadula (BLP) Model is most commonly associated with the classification policy used by the military, which is more concerned with the confidentiality of data at higher levels of sensitivity than the ability of users to modify that data, intentionally or not. The BLP is a finite-state machine model that employs the following logic: if a machine starts in a secure state and all possible transitions between states within the machine result in secure states, then the machine is secure.

There are four components to the BLP Model, as follows:

1. *Subjects* are the users and system executable processes.
2. *Objects* are the data elements.
3. *Modes of access* include read, write, execute, and combinations thereof.
4. *Security levels* are essentially security classification levels.

These four components are used to establish three security principles to formulate the basis for the BLP Model. The three principles are as follows:

1. *Simple security property*, which states that the level of the subject must be at least the level of the object if the mode of access allows the level to be read.
2. *Confinement property* (a.k.a. "*star*" *property, or* **-property*), which states that the level of the object must be at least the level of the subject if the mode of access allows the subject to write.
3. *Tranquility principle*, which states that the operation may not change the classification level of the object.

Confidentiality of data is protected, but the fact that users with lower privileges are permitted to write data to objects with a higher sensitivity level does not sit well in many environments. Biba developed a model to address this integrity issue.

107.2.2 Biba Model

The Biba Integrity Model was published at Mitre after Biba noticed that the BLP Model did not address data integrity. The problem was that lower-level security users could overwrite classified documents that they did not have the authority to read. Although the Biba Model has not been widely implemented, it is well known. The Biba Model is based on a hierarchy of integrity levels. Integrity levels (a hierarchy of security classifications) are assigned to subjects (e.g., users and programs) and objects (data elements), and are based on axioms (rules) that define the integrity policy to follow.

The Biba Model supports five different integrity policies, including:

1. *Low Water Mark Policy* permits the integrity level of a subject to change. The new integrity level is set to the lower of the integrity levels for the object, or for the subject that last performed an operation on the object.
2. *Low Water Mark Policy for Objects* adds permission to permit the integrity level of an object to change.
3. *Low Water Mark Integrity Audit Policy* adds axioms to measure the possible corruption of data.
4. *Ring Policy* enforces a static integrity level for the life of both subjects and objects. Subjects cannot write to objects with higher integrity levels, or read objects with lower integrity levels. Further, subjects cannot invoke other subjects with higher integrity levels or write to objects with a higher integrity level, but can read objects at a higher integrity level.
5. *Strict Integrity Policy* adds to the Ring Policy the axiom that a subject cannot read objects with a higher integrity level.

The BLP Model works well for military environments, although it is not well suited to commercial entities because it does not address data integrity. The Biba Model addresses this integrity issue but is still not sufficient in commercial environments to prevent a single individual with a high level of authority from manipulating critical data, unchecked. The Clark–Wilson Model, discussed next, addresses both of these issues.

107.2.3 Clark–Wilson Model

The Clark–Wilson Model is most commonly used in a commercial environment because it protects the integrity of financial and accounting data, and reduces the likelihood of fraud. This model defines three goals of integrity, as follows:

1. Unauthorized subjects cannot make any changes.
2. Authorized subjects cannot make any unauthorized changes.
3. Internal and external consistency is maintained.

In a commercial environment, these goals are well suited to ensuring the integrity of corporate financial and accounting data. Not only are unauthorized individuals prohibited access to protected data, but even individuals authorized to access this data are prohibited from making changes that might result in the loss or corruption of financial data and records.

Clark–Wilson introduced an integrity model employing two mechanisms to realize the stated integrity goals, as follows:

1. *Well-formed transactions*, which introduces the concept of duality for each transaction. Each transaction is recorded in at least two places such that a duplicate record exists for each transaction. This is not necessarily a copy of the transaction, but a separate record that is used to validate the accuracy and validity of the original transaction.
2. *Separation of duty*, which prohibits one person from having access to both sides of a well-formed transaction, and also prohibits one individual from having access to all steps of a complete transaction process. This reduces the likelihood of fraud by forcing collusion between multiple users if the fraud is to go undetected.

This integrity model does not apply classification levels to data, or users. Instead, it places strict controls on what programs have permission to manipulate certain data, and what users have access to these various programs.

107.3 Common Standards and Practices

Common security standards and practices are tools used in conjunction with modeling techniques and should be adopted by organizations as a matter of policy. In fact, although they are called "standards," they are actually guidelines until they are adopted by an organization as its standard. Publications addressed in this section include ISO 17799, COBIT, Common Criteria (ISO 15408), and NIST's Generally Accepted Principles and Practices for Securing Information Technology Systems. The first three are internationally accepted standards, whereas the fourth one is exactly what it states to be, which is a statement of generally accepted principles and practices. Each of these shares a number of common characteristics, including:

- They are all reasonable and practical.
- Where they overlap, they are generally consistent with one another.
- They are applicable for use in any organization, or any industry.
- Tuning to the organization and culture by adopting only those focus areas relevant to the business or mission is expected for an effective implementation.
- They can be employed in parallel; thus, selection of one does not preclude use of the others.

Of course, for these statements to be true, it is clear that all aspects of these common standards and practices are not utilized by every organization. Every organization, especially from different lines of business, should select its own standard(s), and then the components of the standard(s) with which it intends to comply. Each of the standards presented in this section is well known, and has been thoroughly implemented in practice.

107.3.1 BS 7799 and ISO 17799

BS 7799 Parts 1 and 2, and ISO 17799 are addressed together in this chapter because they are so closely related. BS 7799 Part 1 has essentially been adopted as ISO 17799, and thus warrants no further discussion for our immediate purposes. We discuss ISO 17799 shortly; thus, providing highlights of BS 7799 Part 1 would prove redundant. So why mention BS 7799 in this chapter at all? There are two reasons for this. The first objective is to make clear the origins of the ISO standard. The second and more significant point is that BS 7799 Part 2 establishes the concept of an Information Security Management System (ISMS), which is not addressed in the ISO standard and is not likely to be adopted by ISO any time in the near future.

BS 7799 Part 2 (BS 7799-2:2002) was published on September 5, 2002. It provides the framework for an ISMS establishing monitoring and control of security systems, thereby providing a framework to minimize business risk. The concept of an ISMS may be of greater importance than the original Code of Practice (Part 1) because it enables a security program to continue to fulfill corporate, customer, and legal requirements.

BS 7799-2:2002 provides for the following:

- Guidance on creating an ISMS
- A Plan-Do-Check-Act (PDCA) Model for creating and maintaining an effective ISMS
- Critical success factors to successfully implement information security
- Ability to continually improve the security management process
- Ability to continually assess security procedures in the light of changing business requirements and technology threats

ISO 17799 (ISO/IEC 17799:2000) is essentially BS 7799 Part 1, with minor revisions. The purpose of the standard is to establish a Code of Practice for Information Security Management. This standard establishes a hierarchy of 127 controls, within 36 control objectives, within 10 security domains.

The ten security domains that form the framework of the standard are as follows:

1. Security Policy
2. Organizational Security
3. Asset Classification and Control
4. Personnel Security
5. Physical & Environmental Security
6. Communications and Operations Management
7. Access Control
8. Systems Development and Maintenance
9. Business Continuity Management
10. Compliance

Within these ten domains lies the set of 36 control objectives, which are further broken down to reveal 127 more detailed controls. An organization should select those controls that are important to achieving their security goals, and set aside the others. Organizations choosing to adopt this standard need not attempt to comply with every aspect of the standard. Like every other standard, it should be applied in accordance with the needs of the organization.

ISO 17799 maintains a focus on IT security. It is specific in terms of what constitutes sound security practices, yet does not recommend technology specific guidelines. Certification to the standard can be made an organizational goal but most organizations simply use the standard to benchmark their security capability against sound practices.

BS 7799-2:2002 and ISO/IEC 17799:2000 are available online (http://www.iso-standards-international.com/bs-7799.htm) or via CD-ROM for a nominal fee.

107.3.2 COBIT®

COBIT (Control Objectives for Information and related Technology) was developed jointly by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) as a generally applicable standard for sound information technology (IT) security and control practices, and is now in its third edition (COBIT® 3rd edition©). This widely accepted standard provides a reference framework for management, users, auditors, and security practitioners.

COBIT is a mature standard that continues to be updated and improved. The COBIT IT processes, business requirements, and detailed control objectives define what needs to be done to implement an effective control structure. The IT control practices provide the more detailed how and why needed by management, service providers, end users, and control professionals to implement highly specific controls based on an analysis of operational and IT risks.

COBIT provides an IT governance and objectives framework, stated in business terms. Broader than just security, this is a six-volume work containing an IT governance guideline, and an entire volume of management guidelines that provide management tools to use for evaluating the status and effectiveness of the enterprise. This standard establishes a hierarchy of 318 detailed control objectives within 34 high-level control objectives (IT processes), and are organized within 4 domains.

The framework for these four domains, and the number of IT processes addressed within each, is as follows:

- Planning and Organization (PO) contains 11 high-level control objectives.
- Acquisition and Implementation (AI) contains six high-level control objectives.
- Delivery and Support (DS) contains 13 high-level control objectives.
- Monitoring (M) contains four high-level control objectives.

It is beyond the scope of this chapter to delve into the details of the detailed control objectives; however, it is worthwhile to tie in how this standard can be used to assist with establishing an overall ESA. A break-out of one of the 34 high-level control objectives is used to emphasize this point. The sample below is taken from the COBIT Framework document, Planning and Organization domain, Objective 8 (PO8), ensuring compliance with external requirements. COBIT structures this high-level control objective as follows:

Control over the IT process of

ensuring compliance with external requirements

that satisfies the business requirement

to meet legal, regulatory, and contractual obligations

is enabled by

identifying and analyzing external requirements for their IT impact, and taking appropriate measures to comply with them

and takes into consideration

- Laws, regulations and contracts
- Monitoring legal and regulatory developments
- Regular monitoring for compliance

- Safety and ergonomics
- Privacy
- Intellectual property

This sample illustrates several points related to establishing an overall ESA:

- *That IT controls are driven by external factors, not within the control of the organization*. Other high-level control objectives address internal factors as well.
- *That controls placed into operations are there to satisfy a specific business requirement*. All of the high-level control objectives identify the business requirement for the stated control.
- *A clear indication that a legal representative should play a key role in the overall security program and architecture*. Other high-level control objectives bring out the need for involvement of additional non-security, non-IT functions, each of which should have a say in the overall security scheme.

The majority of COBIT 3rd edition is available for complimentary download, as an open standard, from www.isaca.org/cobit.htm. The entire COBIT 3rd edition print and CD-ROM, six-volume set can be purchased for a nominal fee, and is discounted to ISACA members.

107.3.3 Common Criteria (ISO 15408)

Version 2.1 of the Common Criteria for Information Technology Security Evaluation (Common Criteria) is a revision that aligns it with International Standard ISO/IEC 15408:1999. This standard largely supersedes the Trusted Computer System Evaluation Criteria (5200.28-STD—Orange Book, also known as TCSEC), dated December 26, 1985. TCSEC is one of the best-known documents comprising the rainbow series, which is a library of documents that addressed specific areas of computer security. Each of the documents is a different color, which is how they became to be referred to as the Rainbow Series. If the reader is interested in further information about the Rainbow Series, most of the documents can be found online at http://www.radium.ncsc.mil/tpep/library/rainbow/.

The objective of the Common Criteria is to provide a standard approach to addressing IT security during the processes of development, evaluation, and operation of targeted systems. Common Criteria can thus be adopted as a standard for use within an organization's system development life cycle (SDLC). It is sound practice to reduce the risk of project failure by adopting an SDLC to guide developers throughout development projects. Common SDLC methodologies generally fall into either "Heavy" or "Agile" camps, and there are literally dozens of widely known and accepted methodologies within each camp. Some common examples include Waterfall Methodology, Rapid Application Development (RAD), Spiral/Cyclic Methodology, Microsoft Solutions Framework (MSF), Scrum, and Extreme Programming (XP). One of the critical success factors met by the Common Criteria is the fact that it does not mandate any specific development methodology or life-cycle model; thus, it can be used by developers without forcing them into a methodology not suitable to their approach to system development.

Security specifications written using Common Criteria, and IT products or systems shown to be compliant with such specifications, are considered ISO/IEC 15408:1999 compliant, although certification of compliance can only be achieved through accredited evaluation facilities known as Common Criteria Testing Laboratories (CCTLs). It is important to note that Common Criteria is not applied as a whole to any particular system, or target of evaluation (TOE), as the standard is very large and complex. A security target (ST) is created using elements of the Common Criteria in an effort to provide the basis for evaluation and certification against the standard. Protection profiles (PPs) are developed and used to provide implementation-independent statements of security requirements that are shown to address threats that exist in specified environments.

PPs are needed when setting the standard for a particular product type, or to create specifications for systems or services as the basis for procurement. Numerous validated protection profiles have been

created and approved, and are available online at http://niap.nist.gov/cc-scheme/. This site also contains information regarding validated products, accredited CCTLs, and other useful information.

107.3.4 NIST SP 800-14

NIST (National Institute of Standards and Technology) is a U.S. Government organization whose mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. NIST has a Computer Security Division (CSD) that is dedicated to improving information systems security by:

- Raising awareness of IT risks, vulnerabilities, and protection requirements
- Researching, studying, and advising agencies of IT vulnerabilities
- Devising techniques for the cost-effective security and privacy of sensitive federal systems
- Developing standards, metrics, tests, and validation programs
- Developing guidance to increase secure IT planning, implementation, management, and operation

NIST Special Publication 800–14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, is an excellent resource for providing a baseline that organizations can use to establish and review their IT security programs. The document gives a foundation that organizations can reference when conducting multi-organizational business as well as internal business. The intended audience for the guideline includes management, internal auditors, users, system developers, and security practitioners. The following 14 common IT security practices are addressed in this publication:

1. Policy
2. Program management
3. Risk management
4. Life-cycle planning
5. Personnel/user issues
6. Preparing for contingencies and disasters
7. Computer security incident handling
8. Awareness and training
9. Security considerations in computer support and operations
10. Physical and environmental security
11. Identification and authentication
12. Logical access control
13. Audit trails
14. Cryptography

The entire 800 series of NIST documents provides a wealth of information to the security practitioner. Some of the documents are tuned to securing federal systems, but most are largely applicable to both the public and private sectors. These documents are freely available online at http://csrc.nist.gov/publications/nistpubs/.

107.4 Security Governance Model

The purpose of the Security Governance Model is to assist in marrying existing corporate organizational structures and cultures with new security program development activities, which are usually brought about by changing business needs. This is accomplished by identifying and classifying the existing organizational structure as a specific security governance type, and determining if the business needs of the organization can be met by achieving a security capability within this type. Dramatic changes to organizational structures can have a negative impact on a business, and most business leaders will find it

preferable to interject security into the existing corporate culture, rather than change the corporate culture to achieve a specific security capability.

The Security Governance Model addresses the way information security is mandated, implemented, and managed across the enterprise. Governance is generally categorized as being either centralized or decentralized, but these labels are oversimplified for practical modeling purposes. This is because many entities must apply both attributes to achieve their security goals in a cost-effective manner; thus, they are often both centralized and decentralized at the same time. We can model this by first recognizing that security governance has two primary components—control and administration—each of which can be centralized or decentralized. The following definitions for control, administration, centralized, and decentralized are used for this model:

- *Control* refers to the authority to mandate how security will be managed for an organization. Primary objectives are to develop policy and provision budget for security initiatives.
- *Administration* refers to the authority to apply, manage, and enforce security, as directed. Primary objectives include the plan, design, implementation, and operation of security in accordance with policy, and within the confines of budget.
- *Centralized* indicates a single authority, which can be a person, committee, or other unified body.
- *Decentralized* indicates multiple entities with a common level of authority.

Combining the above definitions provides the standard terminology used for this model. The terms "centralized" and "decentralized" no longer stand by themselves, but are coupled with the two primary components of security governance. This yields the following four terms, which form the basis for the Security Governance Model:

1. *Centralized control* (CC) is indicative of an organization where the authority for policy and budget decisions is granted to a representative person or assembly, and is applicable throughout the organization.
2. *Decentralized control* (DC) is indicative of an organization where no one person or body has been authorized to formulate security policy and develop budget for security initiatives.
3. *Centralized administration* (CA) grants authority to apply and manage security policy to security or system administrative personnel who share a common reporting chain.
4. *Decentralized administration* (DA) grants authority to apply and manage security policy to security or system administrative personnel who have multiple reporting chains.

Given an understanding of the terminology, the reader is now in a position to pair each of these control and administration components to formulate the four basic types of security governance:

1. *Centralized control/centralized administration (CC/CA)*: one central body is responsible for developing policies that apply across the entire organization, and all administration is performed by personnel within a single chain of command.
2. *Centralized control/decentralized administration (CC/DA)*: one central body is responsible for developing policies that apply across the entire organization, yet administration is performed by personnel within multiple chains of command.
3. *Decentralized control/centralized administration (DC/CA)*: several entities are responsible for developing policies that apply within their areas of responsibility, yet all administration is performed by personnel working within a single chain of command.
4. *Decentralized control/decentralized administration (DC/DA)*: several entities are responsible for developing policies that apply within their areas of responsibility, and administration is performed by personnel within multiple chains of command.

To utilize this model (Exhibit 107.1), an organization first defines the security needs of the business or mission, and classifies the type of security governance currently in place. A security strategy for the organization is then developed, taking into account the governance type and business needs. Once

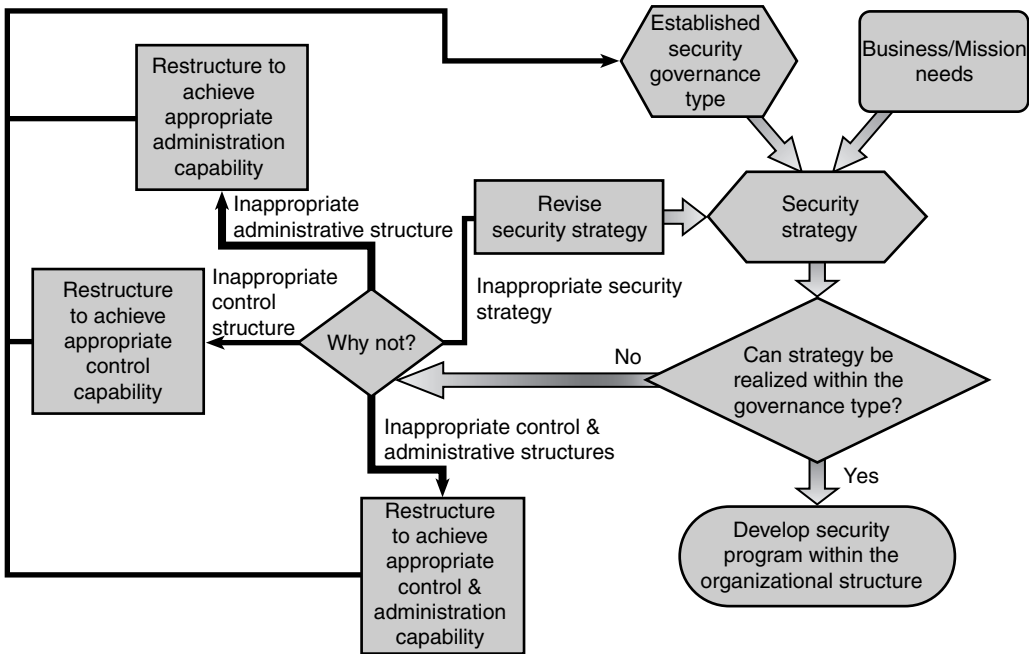

EXHIBIT 107.1 Security governance model.

a strategy is realized that can be effectively accomplished within the governance type, it is reasonable to proceed with further development of the ESA within the existing organizational structure. If the strategy cannot be realized within the governance type, then one is forced to change something. Assuming the main drivers have been properly identified as the business needs, there remain four areas of focus. The easiest approach is to revisit the security strategy. If the strategy can be revised such that an effective security capability can be achieved within the existing governance type, then the process is greatly simplified. If not, then the organizational structure must be modified to achieve the best cost/benefit security governance type for the organization.

This model does not mandate a specific organizational structure. Rather, the model associates aspects of the organizational structure to align business needs with the security capability desired by the organization by identifying the governance type that will best achieve the security strategy for the organization.

To assist with clarifying the four types of governance, organizational structure examples are provided for each type. The following should be noted when reviewing the samples provided:

- All of the examples with a CIO (Chief Information Officer) or CSO (Chief Security Officer) show them reporting to a COO (Chief Operating Officer). This is for example purposes only and is not intended as a recommended reporting structure. The CIO and CSO might report to any number of executives, including directly to the CEO (Chief Executive Officer).
- The CIO and CSO are intentionally identified as peers. If a CSO exists in the organization, then the CIO and CSO should report to the same executive officer, primarily to resolve their inherent conflicts of interest and to ensure unbiased appropriation of budgets.
- There are almost as many different organizational charts as there are organizations. The examples provided herein are intended to help clarify why an organizational structure fits a particular security governance type.

107.4.1 Centralized Control/Centralized Administration (CC/CA)

CC/CA identifies a truly centralized security capability (Exhibit 107.2). One central body is responsible for developing policies that apply across the entire organization, and personnel within a single chain of command perform all administration. Representatives for each department are assigned to a steering committee that ensures that each has appropriate influence over the policy-making process. This influence is depicted by the arrows in Exhibit 107.2, versus traditional organizational structure reporting.

In this case, the CEO has designated that the COO is responsible for a security program. The COO has delegated this responsibility by creating a CSO position. The steering committee exists to ensure that each department is given appropriate input to the policy-making process, because each department has security issues that must be addressed. Legal and regulatory issues such as the PATRIOT Act, Gramm–Leach–Bliley, Sarbanes–Oxley, HIPAA, and Safe Harbor, just to name a few, must also be addressed. The CSO typically chairs the security steering committee. Although the CSO must maintain proper control and administration over security, it is a function that impacts the entire organization.

Security operations and IT operations have been completely separated. The CSO is responsible for all things security, while the CIO is responsible for IT operations. There is no overlapping of responsibility, although both groups will have responsibilities on the same devices. Firewalls provide a good example. IT operations must be able to reboot, or restore a firewall if a failure occurs, but need not be authorized to make changes to the rule set. Authority to make changes to the rule set falls to the security operations group, but this group must not be permitted to interrupt traffic or adversely affect operations except during scheduled maintenance periods. These groups work together to support organizational needs, but do not share operational tasks.

107.4.2 Centralized Control/Decentralized Administration (CC/DA)

CC/DA (Exhibit 107.3) is the most commonly implemented governance model type for mid- to large-sized organizations. One central body is responsible for developing policies that apply across the entire organization, yet personnel within multiple chains of command perform administration.

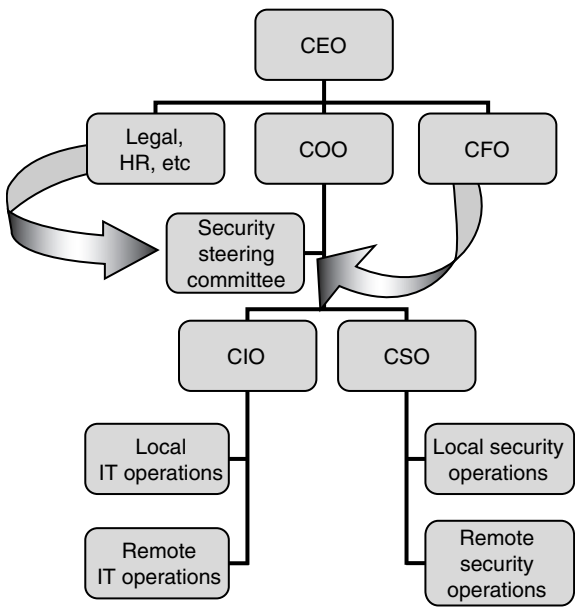

EXHIBIT 107.2 Centralized control/centralized administration (CC/CA).

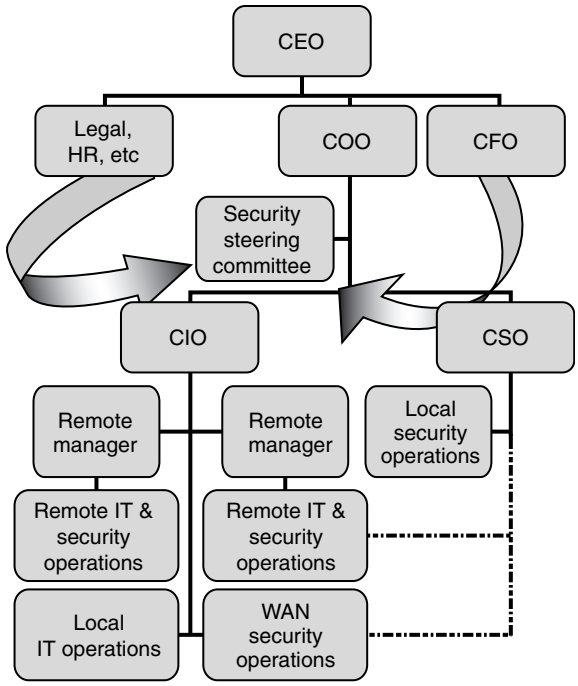

EXHIBIT 107.3 Centralized control/decentralized administration (CC/DA).

As in the prior example, the CEO has designated that the COO is responsible for a security program, the COO has delegated this responsibility by creating a CSO position, and the steering committee exists to ensure that each department is given appropriate input to the policy-making process. Again, the influence of each department over the security development process is depicted in Exhibit 107.3 by arrows. The aspects of centralized control have not changed.

The relationship between security operations and IT operations has changed dramatically. This organizational structure passes greater responsibility to IT managers located at remote facilities by permitting each to manage security and IT operations, inclusively. The CSO may have dotted-line control over security personnel at some remote facilities, as noted in the diagram, but there is not one central point of control for all security operations.

107.4.3 Decentralized Control/Centralized Administration (DC/CA)

DC/CA (Exhibit 107.4) is appropriate for some small organizations that do not have the resources to justify a steering committee. Several entities are responsible for developing policies that apply within their areas of responsibility, and these policies are pushed to operations managers for implementation and enforcement. This influence is depicted in the Exhibit 107.4 by arrows, versus traditional organizational structure reporting. Personnel within a single chain of command, in this case the COO, perform all administration.

Note that remote location IT managers might include co-location arrangements, where IT operations are outsourced to a third party, while ownership and some measure of control of the IT assets are maintained by the organization.

107.4.4 Decentralized Control/Decentralized Administration (DC/DA)

DC/DA (Exhibit 107.5) identifies a truly decentralized security capability. This structure is appropriate for some small organizations that neither have the resources to justify a steering committee nor keep their critical

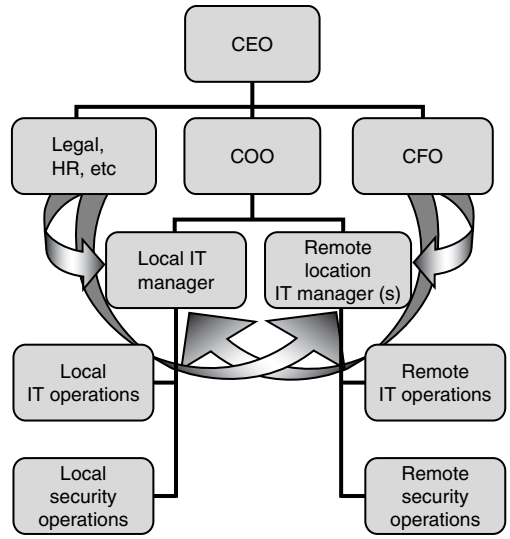

EXHIBIT 107.4 Decentralized control/centralized administration (DC/CA).

IT operations in-house. In this example, the CFO manages a contract for outsourcing company financials, HR manages the contract for outsourcing human resources, and IT operations has little or nothing to do with either. The outsourced companies are responsible for the policies and procedures that apply to the systems within their control, and the customer either accepts these policies, or takes its business elsewhere.

The administration portion of the above example, under the COO, is indicative of a CA structure, yet the organization is classified as DA because the COO has no control over security administration for the

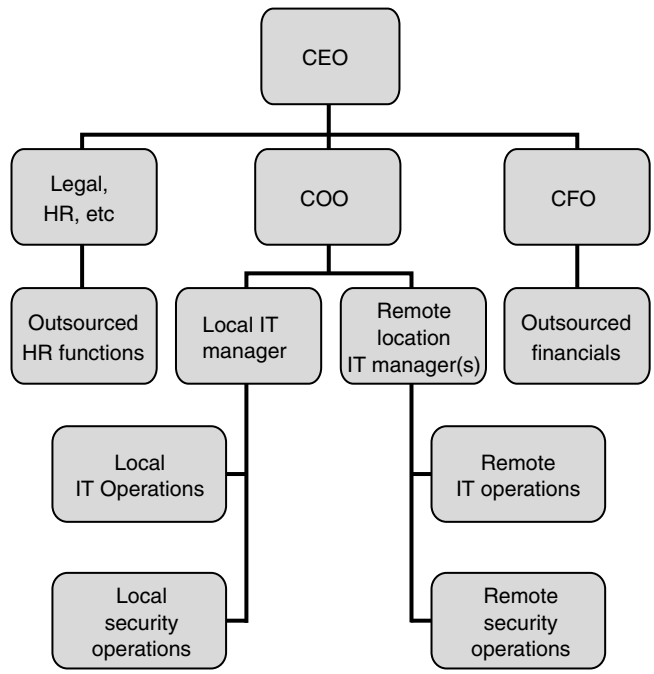

EXHIBIT 107.5 Decentralized control/decentralized administration (DC/DA).

outsourced IT capabilities. In this case, the responsibility for ensuring adequate controls over the security of company financial data is relegated to the outsourcing provider.

The advantages and disadvantages of each governance type will differ from organization to organization. One that is more expensive to implement in one organization may prove cheaper to implement in another. The fundamental objective is to achieve organizational security goals as effectively and painlessly as possible.

107.5 Enterprise Security Architecture Model

Enterprise security architecture (ESA) incorporates all aspects of security for an organization, including leadership, strategy, organizational structure, planning, design, implementation, and operations. It encompasses the people, processes, and technology aspects of security. Numerous models have been developed, and those that communicate sound security practices share a common approach to enterprise security. The ESA Model shown in Exhibit 107.6 is an open source model that this author has developed to communicate this approach.

107.5.1 Executive Sponsorship

Organizations should elicit executive sponsorship for developing a corporate security program; otherwise, the program leader will lack buy-in from other departments and will not have the ability to enforce compliance with the program. A brief policy statement, typically issued in the form of a formal corporate memo, should be presented from the highest corporate level in order to authorize the existence

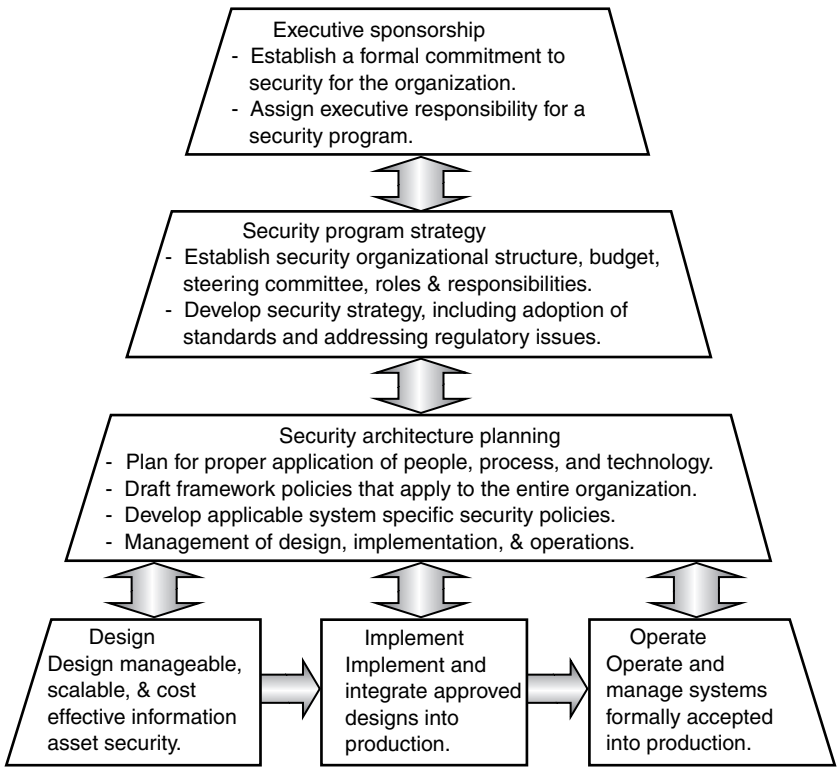

EXHIBIT 107.6 Enterprise security architecture (ESA).

of a corporatewide security program. This directive will justify development of the security program, thus establishing the requirement to develop a security program charter.

The security program charter authorizes development of a formal security program, and delegates an authority appropriate for the organization (e.g., the Chief Operating Officer [COO]). This executive would then typically delegate this responsibility by creating a CSO or equivalent position. Note that without executive sponsorship, the CSO will likely have difficulty applying and enforcing security directives that impact other departments.

107.5.2 Security Program Strategy

The CSO then formulates a formal policy statement in response to the corporate directive. This broad policy document will define the goals of the security program, as well as the organizational structure. These must generally be approved by the corporate Board of Directors. In this example, the CEO has designated that the COO is responsible for the security program, and the COO has delegated this responsibility to a CSO. Many organizations have appropriately created a CSO position that reports directly to the Board of Directors, which is preferable for organizations that face significant risks to their business from security breaches.

A security program strategy is drafted to meet the business or mission needs of the organization. The CSO drafts the overall security program strategy by aligning the organizational approach to security with sound industry practices, and by leveraging common standards and practices such as the ISO 17799, COBIT, Common Criteria (ISO 15408), and NIST publications mentioned previously in this chapter. Application of the Security Governance Model can be applied in this layer to assist in marrying an effective strategy with an appropriate organizational structure.

In many organizations, sound practices suggest that the CSO formulate a security steering group, or intra-organizational policy board, comprising representatives from each functional business area. Customer Operations, Engineering, Finance, Internal Communications, HR, IT, Legal, Marketing, and Sales are examples of departments that might be represented in this group. This steering group will oversee most security policy development for the company in order to establish the organization's overall approach to computer security.

107.5.3 Security Architecture Planning

Planning the architecture refers to planning that takes place within an established security organization. Planning to execute security initiatives is an exercise in futility if executive sponsorship and security program strategy have *not* been established. Planning encompasses the people, processes, and technology aspects of security, and thus addresses policy, procedure, and technical implementation. Having established executive sponsorship and security program strategy for the organization, one can continue to develop the ESA.

If COBIT has been determined to be the standard to be used by the organization, then guidance offered within the Planning and Organization domain falls primarily within this layer of the model, and the other three COBIT domains will each be spread across the design, implementation, and operations components of the lowest layer of this model. The model is scalable such that existing standards can and should be used, yet sufficiently flexible that no one standard must be used. Developing security policies is a critical component of this layer of the ESA Model. Again, selection of one standard does not preclude the use of other well-known and accepted publications. A sample approach to developing security policies in accordance with the guidance from NIST Special Publication 800-14 follows.

Program-framework policies can now be drafted to establish the organization's overall approach to computer security. This is a set of corporatewide policy statements that establish a framework for the security program. Board-level direction is recommended for establishing most program policy

statements because these policies provide organizationwide direction on broad areas of program implementation. This board-level direction is the fundamental function of the steering group, because representatives of the board are included in this committee. Policy statements at this level reflect high-level decisions about priorities given to the protection of corporate data. Board-level direction is recommended for acceptable use, remote access, information protection (a.k.a. data management), data retention, special access (root level), network connection, system acquisition and implementation, and other policies, as required. Program policy is usually broad enough that it does not require much modification over time. Additional policies will need to be developed, and are categorized as issue specific and system specific.

Board-level direction is also recommended for development of *issue-specific policies*, which address specific issues of concern to the organization. Whereas program-framework policy is intended to address the broad, organizationwide computer security program, issue-specific policies are developed to focus on areas of current relevance, concern, and possible controversy to an organization. Issue-specific policies are likely to require frequent revision as changes in technology and related factors take place. An example of an issue-specific policy is one that addresses peer-to-peer file sharing via programs such as Kazaa and Morpheus.

System owners, versus board-level representatives, are responsible for systems under their control, and as such should establish *system-specific policies* for these systems. System-specific policies focus on decisions taken by management to protect a particular system. Program policy and issue-specific policy both address policies from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or the direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. A system-specific policy fills this need. It is much more focused because it addresses only one system.

In general, for issue-specific and system-specific policies, the issuer is a senior official. The more global, controversial, or resource intensive the policy statement, the more senior the policy issuer should be.

Many security policy decisions will apply only at the system level and will vary from system to system within the same organization. While these decisions might appear to be too detailed to be policy, they can be extremely important, with significant impacts on system usage and security. A management official should make these types of decisions, as opposed to a technical system administrator. Technical system administrators, however, often analyze the impacts of these decisions.

Once a policy structure is in place, the overall planning and management of the security life cycle is maintained at this layer of the ESA Model.

107.5.4 Security Architecture Design, Implementation, and Operations

Security architecture planning establishes how an organization will realize its security strategy. Security architecture design, implementation, and operations are where the "rubber meets the road." Planned activities are realized and executed, usually in phases and with interim planning steps conducted throughout the cycle.

Support, prevention, and recovery occur in a continuous cycle at the foundation of this model. These activities can be effective when they occur as part of a well-structured security program. As an example, a qualitative risk assessment for the organization is among the activities to be executed. This includes identifying major functional areas of information, and then performing a risk assessment on those assets. The output of this process includes tables detailing the criticality of corporate systems and data in terms of confidentiality, integrity, and availability. Additional services or capabilities that are likely addressed include, but are certainly not limited to, the following:

- Firewall architecture
- Wireless architecture
- Router and switch security

- Network segmentation and compartmentalization
- Intrusion detection systems
- Business continuity
- Anti-spam and malicious code protection
- Incident response and digital forensics
- Vulnerability assessments and penetration testing
- Patch management

Additional models can be employed to address the technical security services associated with the design, implementation, and operations components comprising this foundational layer of the ESA Model. The model presented to address this issue is the Security Services Model.

107.6 Security Services Model

One model that should be considered in the design, implementation, and operations of technical security capabilities is detailed in NIST Special Publication 800–33, *Underlying Technical Models for Information Technology Security*.

This publication defines a specific security goal, which can be met through achievement of five security objectives. The stated goal for IT security is to:

> Enable an organization to meet all of its mission/business objectives by implementing systems with due care consideration of IT-related risks to the organization, its partners and customers.

The five security objectives are generally well understood by security professionals, and are as follows:

1. Availability (of systems and data for intended use only)
2. Integrity (of system and data)
3. Confidentiality (of data and system information)
4. Accountability (to the individual level)
5. Assurance (that the other four objectives have been adequately met)

This model next identifies and classifies 14 primary services that can be implemented to satisfy these security objectives. The 14 services are classified according to three primary purposes: support, prevent, and recover. Definitions of each of the primary purposes, as well as the 14 primary services classified within each, are as follows:

- *Support*. These services are generic and underlie most information technology security capabilities.
  - Identification (and naming)
  - Cryptographic key management
  - Security administration
  - System protections
- *Prevent*. These services focus on preventing a security breach from occurring.
  - Protected communications
  - Authentication
  - Authorization
  - Access control enforcement
  - Non-repudiation
  - Transaction privacy

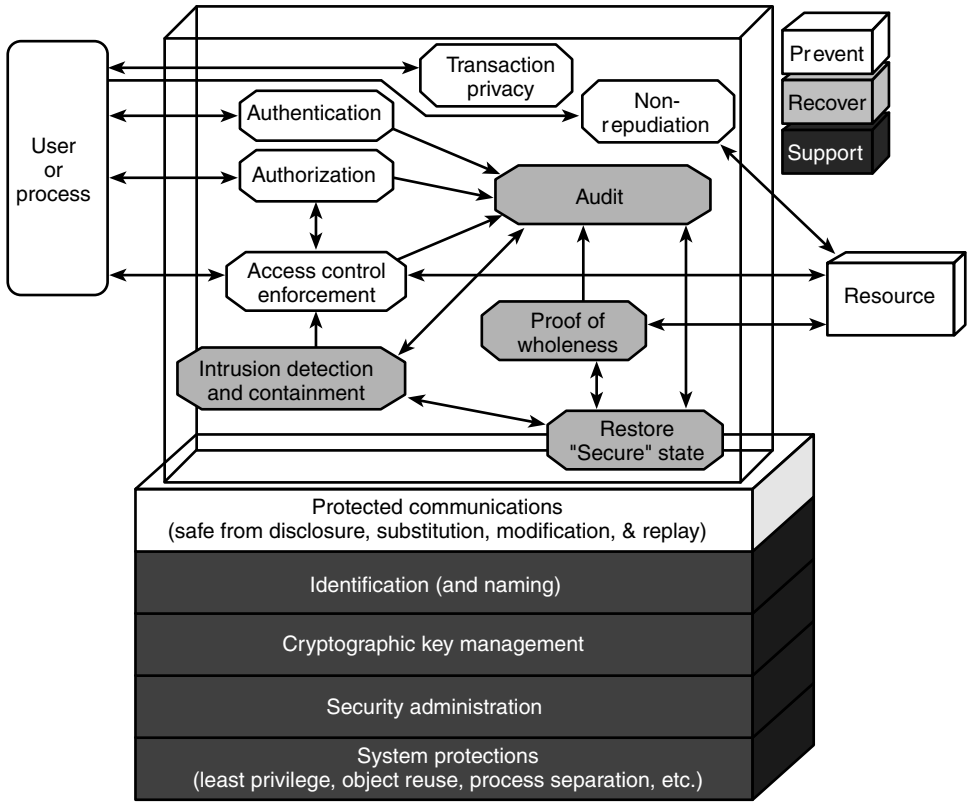

EXHIBIT 107.7 Security services model. (*Source*: Security Services Model, NIST Special Publication 800–33, *Underlying Technical Models for Information Technology Security*, p. 5.)

- *Recover*. The services in this category focus on the detection and recovery from a security breach.
  - Audit
  - Intrusion detection and containment
  - Proof of wholeness
  - Restore "secure" state

The underlying technical Security Services Model is depicted in Exhibit 107.7. This shows the primary services and supporting elements used in implementing an information technology security capability, along with their primary relationships.

Remember that we endeavor to meet a specific security goal by achieving five security objectives. It stands to reason that the above model must be broken out five different ways—one for each objective—in order to allow us to effectively implement a comprehensive technical security capability. The NIST publication does this, and it can be found at http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf if the reader is interested in delving into the further details of this model.

107.7 Conclusion

This chapter presented a number of security models that were brought together to form a road map to achieving an effective enterprise security architecture (ESA). The ESA Model provides this road map at a high level, and additional models have been introduced that can be applied within the layers of this model. System Security Models have been presented; these help to form the basis for the development of

secure systems. Common standards and practices were presented that assist in the development and realization of the security strategy. The Security Governance Model assists with categorizing and developing an organizational structure for the security program, and the Security Services Model details the primary services and supporting elements used in implementing an information technology security capability.

The models, standards, and practices presented in this chapter neither constitute a complete collection, nor is it the intent of this chapter to suggest that this is the only approach to an ESA. Numerous additional models and suggested standards exist, and can likely be substituted for those presented herein.

References

Bell, D. E. and LaPadula, L. J. March 1976. *Secure Computer System: Unified Exposition and Multics Interpretation*. Available as NTIS ADA 023 588. MTR-2997, MITRE Corp., Bedford, MA.

Biba, K. J. 1977. *Integrity Considerations for Secure Computer Systems*. USAF Electronic Systems Division.

Clark, D. D. and Wilson, D. R. 1987. A comparison of commercial and military computer security policies. In *IEEE Symposium on Security and Privacy*, pp. 184–194, Oakland, CA.

Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999.

COSO: Committee of Sponsoring Organisations of the Treadway Commission. 1994. *Internal Control—Integrated Framework*, 2 volumes, American Institute of Certified Accountants, New Jersey.

Fisch, E. and White, G. 2000. *Secure Computers and Networks: Analysis, Design, and Implementation*. CRC Press, Boca Raton, FL.

Information Systems Audit and Control Association. 2000. *COBIT 3rd edition*, Rolling Meadows, IL, ISACA.

ISO/IEC. ISO/IEC 17799. ISO/IEC, Geneva, 2000.

NIST Special Publication 800–14. September 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Marianne Swanson and Barbara Guttman.

NIST Special Publication 800–33. December 2001. *Underlying Technical Models for Information Technology Security*. Gary Stoneburner.

OECD Guidelines: Organisation for Economic Co-operation and Development. 1992. *Guidelines for the Security of Information*, Paris.