2008

The development of a framework for enterprise security architecture and its application in organizations

Yi-Ting Shen

THE DEVELOPMENT OF A FRAMEWORK FOR ENTERPRISE SECURITY ARCHITECTURE AND ITS APPLICATION IN ORGANIZATIONS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of

Business Administration:

Information Assurance and Security Management

---

by

Yi-Ting Shen

June 2008

THE DEVELOPMENT OF A FRAMEWORK FOR ENTERPRISE SECURITY ARCHITECTURE AND ITS APPLICATION IN ORGANIZATIONS

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Yi-Ting Shen

June 2008

Approved by:

[redacted]

Frank Lin, Ph.D, Committee Chair,
Information and Decision Science

6/3/08
Date

[redacted]

C.E. Tapie Rohm, Ph. D

[redacted]

Walt Stewart, Jr., Ph. D,
Department Chair

ABSTRACT

The enterprise architecture (EA) plan is a long-term view or blueprint for an organization. It is a very important blueprint for balancing business and IT technology and for adding value to an organization. Security is also an essential dimension for enterprises nowadays. It can prevent confidential information from leaking, being stolen and lost, or suffering from other serious disasters. There are many researches focusing on EA and specific aspects of security. However, there are very few researchers concentrating on enterprise security architecture that is based on the Zachman EA framework (Zachman, 2007). This paper will incorporate the security dimension with the Zachman EA framework, which intends to serve as an enterprise security framework assist an organization to successfully and effectively implement security.

ACKNOWLEDGEMENTS

I would like to express my sincere appreciation for many people who have assisted and supported me finish my study. I thank for Dr. Frank Lin who guides me through the process of this study, provides great direction of writing the paper, and assists me in resolving all kinds of issues relevant to the paper, improves the quality of the content of this paper, and asks Mr. Sean A. McFarland assist me in the flow of the content and grammar checks. Without his great help, this study will not be completed on time. I also thank for Dr. Javier Torner. He assists me a lot in security section. We almost met once a week to discuss security topics and analysis related to this study. Dr. C.E. Tapie Rohm and Dr. Walt Stewart assist in my learning and attending security conference for information gathering. They also assist me in meeting the deadline. Finally, I thank for my family for their support throughout my study. Without their support, I would not have come this far. In conclusion, I am really appreciative for each of them for their unconditional efforts in many ways throughout my study because each one of them plays an important role in the whole process of my study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

An enterprise architecture plan (EAP), provides a long-term view or blueprints for organizations. An EAP generally includes five essential categories: governance, business architecture, applications architecture, data architecture, and technology architecture (Carbone, 2004; Ross, 2003; Spewak, 1993; Zachman, 1987). The enterprise architecture starts with the forming of governance groups, such as an EA management team and an architecture team (Boh & Yellin, 2006). These two teams are in charge of developing the EAP, including setting the scope and goals. The architecture team starts by analyzing the business framework, such as where the organization is today, what the target will be, and what the critical success factors (CSF) are that would help to achieve set the goals and targets. After analysis, the business architecture is first built and then followed by the development of the data architecture, the application architecture and the technology architecture. Three essential principles of applying EA can benefit organizations the most. The first foundation EA principle is to align business and technology.

Tallon (2007) demonstrates the strong positive relationship between strategic alignment and firm performance, especially from process-level perspectives. He also demonstrates that proper alignment can enhance business value as well. The second principle is to link business needs to the IT infrastructure. This principle can ensure that IT infrastructure provides all services that a business needs. The third principle is to adopt top-down governance, which ensures the alignment of IT infrastructure with business goals and objectives.

Security architecture is a concept that aims to design the infrastructure of information systems to ensure that they provide enough security to organizations and businesses (Sherwood, 2005). Traditionally, organizations address two categories of threats against the security of organizations and their businesses: distributed attacks and insider threats (Fumy & Sauerbrey, 2006). Networking technology connects all computers together no matter where computers are located in the world. This technology creates convenience when conducting research, when connecting with people across the globe, when the need arises to gather needed information efficiently, and so forth. Nevertheless, it also provides great opportunities for attackers to

remotely access computers within enterprises locally. These types of threat are called a distributed attack. The second type of threat comes from insiders, such as employees. These insiders are authorized to access organizations' information systems. However, due to the lack of unawareness of the correct usage of information technology or other reasons, sometimes they involve the exploitation of non-technical vulnerabilities.

Today, most businesses rely on information technology much more heavily than in the past. Carelessly designed security architecture would have a serious impact on a business, such as the high risk of being unable to do daily business operations. This heavy reliance on information systems highlights the importance of developing efficient and effective security architecture within the entire enterprise.

Unfortunately, emphasizing security technology alone is not enough to produce effective and efficient security for the entire organization (Sherwood, 2005). Security technology itself is designed to resolve security issues without considering other factors, such as cost and business operating models. Businesses differ in terms of organizational scopes, sizes, capital capacities, business

operating models, and top management support (Boh & Yellin, 2006). These factors affect the security needs and the security trust level (Sherwood, 2005). Based on the Zachman framework to develop enterprise security architecture, developers can clearly understand the security needs of business and the priority of implementing security projects in a specific time period and in a specific manner. With a plan based on this framework, developers have a very clear view of the entire procedure and are able to fully control the situation, such as the status of implementing these security needs, and the impact, and the ability to effectively respond to unexpected events and so on. Furthermore, the enterprise security architecture based on the Zachman framework can allow developers to plan and examine new advanced information technology and systems with appropriate security solutions at once. This not only can provide new business opportunities by increasing the convenience and speed of business processes (Fumy & Sauerbrey, 2006), but also can guarantee the confidentiality, integrity, and availability of business information (Fumy & Sauerbrey, 2006). From the organizational perspective, it saves money. All of these advantages depict that the enterprise security architecture

based on the Zachman framework can produce effective and efficient security for an entire organization.

This research develops a framework that incorporates the security dimension within the Zachman EA framework, assist in successful implementation of the necessary security for organizations. In addition, it's also been applied to an organization for its efficacy. The result of this research provides a guideline for an organization to create an enterprise architecture plan efficiently, and to easily using this plan for transferring business security needs into IT and security infrastructure (implementation).

There are seven chapters in the paper. Chapter one is intended to provide the introduction of the paper. Chapter two is designed to discuss the literature review for the Zachman EA and security architecture. Chapter three is to describe the purpose of writing this paper. Chapter four consists of a framework development, which starts from providing an effective governance approach. An effective governance approach has three fundamental components: independent EA teams with top managers involved, formal monitoring process, and top-down governance approach. The second section is designed to define the scope and goals, which affect the time and cost of development and

implementing. The section business framework provides guidelines of gathering information efficiently and also presents alternative approaches for analyzing the current state and the target state, performing gap analysis, and identifying critical success factors. Aligning business security needs and security technology, and how to establish business architecture by using appropriate tools, such as ProVision and Rational Rose, are also presented in the third section. The fourth section 'framework for securing data, application, and technology' is addressed by providing security services, guidelines, strategies, principles, or architecture for three fundamental categories of IT infrastructure. The next section 'security framework' is intended to develop the entire lifecycle of security policy, which will also be used in the last section of this chapter for illustrating the role of security framework in the Zachman EA framework. In Chapter six, an organization is used as an example to illustrate the efficacy of the developed enterprise security framework. The analysis, results and implication of the organization will be written in Chapter five and six. The final chapter represents conclusions derived from this project.

CHAPTER TWO

LITERATURE REVIEW

There are very few research projects with a focus on enterprise security that is based on the Zachman architecture. Much of the academic research has been focused either on pure Zachman architecture or on security algorithms, database technology, application, and networking to improve efficiency and effectiveness (Cavusoglu, 2005; Danielyan, 2001; McGee, et al., 2004). Even though there are some books focusing on an entire company's security, most of these primarily focus on various up-to-date technologies for securing organizations (Buecker et al., 2004). Unfortunately, implementing security projects alone without considering business needs, aligning business and security technology, and applying appropriate, effective, and efficient governance mechanism can result in spending too much time and money for inefficient implementation of security technology that may not be very suitable for organizations.

This paper will develop a procedural-level framework that incorporates the security dimension with the Zachman EA framework. This approach can avoid delay in delivery

benefit of implementing projects and spending too much money on projects. Due to different business models, sizes, and financial conditions, organizations need to choose appropriate technology at appropriate security level for implementation, based on business needs and status. While alignment between business and security technology can allow managers to develop a comprehensive enterprise plans, and translate alignment into enhanced IT security, there are residual effects on business performance for producing IT security business value (Kearns & Sabherwal, 2006; Tallon, 2007). The appropriate governance approach can ensure alignment is translated into IT security effects in a cost-effective and time-efficient manner.

CHAPTER THREE

PURPOSE OF STUDY

The main purpose of this study is to develop an enterprise security framework that is based on a comprehensive following of the Zachman EA architecture. A top-down approach is used to arrange this paper, starting with an analysis of the security needs of the business framework for an organization. Then, the security architectures for data, application, and technology dimensions will be developed. Following the framework to develop an enterprise plan can eventually increase employees' security awareness. The reason is that at the implementation phase, the general written materials of the enterprise plan will be distributed to relative employees, and employees can learn security from well developed documentation. Furthermore, following the framework to develop an enterprise plan can identify and manage security concerns easily within an entire enterprise, facilitate the process of resolving security issues within an organization, adapt change, modify partial security architecture with ease, and to easily increase quality of the entire organizational security. The reason being is that at the

development phase, business security needs are considered within an enterprise plan. Consideration for these business security needs is also consistent within the entire enterprise.

CHAPTER FOUR

FRAMEWORK DEVELOPMENT

Based on the Zachman EA framework, strategic alignment and governance is an integral part of security in developing the enterprise security framework, and all security needs for data, application, and technology dimensions need to derive from business (Fumy & Sauerbrey, 2006; Sherwood, 2005; Zachman, 1987).

Proper alignment business security needs and security technology supports organizations to gain competitive advantages, and assists organizations to generate a higher return from its technical investment as compared to those which have a misalignment of business and technology (Ross, 2003). Developing enterprise plans with well planned strategic alignment can guarantee a certain degree of quality, and can consequently reduce implementation error or unexpected events from happening, as well as increase the likelihood of successfully implementing projects without delay to gain benefit from project investments (Kearns & Sabherwal, 2006).

From governance perspectives, the top-down and centralization of decisions is the most effective

governance approach to manage architectures for value (Kearns & Sabherwal, 2006; Ross, 2003). Efficient and effective governance can ensure that organizations are compliant with comprehensive enterprise plans, and eventually perceive IT security business value. Consequently, this research adopts a top-down approach, starting from presenting an effective governance approach, followed by identifying scope and goals, analyzing security needs for business framework, and developing the security architectures for data, application, and technology dimensions.

The term "developing teams" is used throughout this paper. Depending on where to mention the term in paper, the term "developing teams" can mean differently. It can be the architecture team, data architecture sub-team, application architecture sub-team, technology architecture sub-team, security policy teams, incident response team, risk management and analysis teams, or implementing teams for different phases.

Framework of Governance

The practice of governance can help organizations apply IT technology and security efficiently and effectively (IT Governance Institute and the Office of Government Commerce, 2005). Governance is like the top roof of the building, which guides, controls and monitors all dimensions mentioned above in this paper. Governance addresses essential parts of IT and security activities: strategic alignment, value delivery, risk management, resource management, and performance measurement. Hence, an effective governance framework and practice of governance can align business and technology, making sure that organizations spend money and time on advancing technology which is what businesses need. An effective framework and great practice of governance also can optimize cost and guarantee to provide the value of IT to organizations. Resource management that governance focuses on, can make sure IT and security projects apply optimizing infrastructure of IT and security. Another benefit that the effective framework and practice of governance can provide to organizations is to control and trace the status of project delivery, to measure performance, and to monitor IT activities and services.

An Effective Governance Approach

An effective governance approach should consider structure of governance, monitoring process of governance, and the direction of governance.

Structure of Governance. Forming integrating managerial and architectural teams and clearly defining their roles, authority and responsibility is the most effective governance approach (Boh & Yellin, 2006). This approach can facilitate EA development and implementation by dividing the whole EA project into different sub-projects and sub-tasks, which are assigned to different team members. This approach formally gives team members accountability for coordinating across units, because the main goal of these teams is to govern the setting and use of EA. Major responsibilities of each role are elaborated below.

Roles and Responsibilities. There are different roles within teams. Different roles have different levels of authority and responsibility. With clearly defined roles, authority and responsibility are properly defined in terms of who handles which tasks. This process can help to easily pinpoint which EA sub-projects and sub-tasks have accomplished and by whom. Boh and Yellin (2006) define four

main roles: EA management team, chief architect, architecture team, and key EA stakeholders.

EA Management Team. An effective governance approach is to get the board and top managers from business units and IT departments involved in the EA management team (National Computing Centre, 2006). The main responsibilities of the integrating managerial team are to set direction, to guide management by aligning business needs and technology, and to make sure IT issues are uncovered.

Architecture Team and Chief Architect. An architecture team is formed not only for developing EA but also for governing EA. An architecture team can be divided into different sub-teams, based on functions needed. Generally, the entire architecture team has at least 3 sub-teams: a data architecture sub-team, an application architecture sub-team, and a technology architecture sub-team. The chief architect is the leader of all sub-team, and is responsible for guiding the entire architecture team to govern EA.

EA Stakeholders. According to the definition from Boh and Yellin (2006), EA stakeholders can be IT personnel who implement projects. They also can be the end users who

are working within the business units. Both IT personnel and end users know their daily operating procedures and the needed data to operate efficiently.

Monitoring Process of Governance. In addition to the structure of governance, the monitoring processes of governance should also be formalized. The monitoring processes of governance are defined as the processes of monitoring whether organizations' operations conform to the settings of EA. Appropriate monitoring processes of governance also can facilitate architecture teams in the implementation EA within the organization. Boh and Yellin (2006) mention that two aspects can be considered for monitoring processes: developing EA based on industrial standards, and conforming to EA.

Developing EA Based on Industrial Standards. Some of the most well-known industrial standards of security are ISO, CoBit, and ITIL (*IT Governance and the Political Dimension, 2007)*. Developing EA, based on these industrial standards, can have a many advantages. Adopting industrial standards into EA can assure that organizations can find compatible technology easily, and that skilled technical employees can be found without any problems. Another advantage is that organizations can gain benefit directly

from these well-known industrial standards without taking much risk in terms of failing projects. The reason is that these industrial standards have been developed deliberately, and have been examined by many companies in various industries.

Conforming to an EA Plan. Conforming to an EA plan can ensure that organizations obtain maximum benefit from adopting EA. A well developed EA plan consists of balancing business security needs and security technical investment, and appropriately transferring business security needs to data architecture, application architecture, and technology architecture in a cost-effective manner. In other words, conforming to a well developed EA plan can ensure that all business needs have been considered for implementation into data architecture, application architecture, and technical architecture. Furthermore, conforming to a well developed EA plan can also create a better quality of implementation with fewer errors (Kearns & Sabherwal, 2006). Without conforming to an EA plan, the EA plan is just a documentation of a blueprint, and organizations not only waste time and money to develop the EA plan, but also a delay in the gain of benefits from implementing any projects at all.

The Direction of Governance. Top-down governance is the most effective direction for governance (Boh & Yellin, 2006; IT Governance Institute and the Office of Government Commerce, 2005). There are two reasons that this is the most effective direction with the first being that the top-down approach makes communication easy between the architecture team and IT employees. Technical employees can just simply follow the blueprint to develop and implement specific projects. They also can provide their thoughts and concerns to the architecture team. Secondly, a top-down governance approach can make controls standardized (Kearns & Sabherwal, 2006), which can easily manage, control, and monitor the status of technical diversity in organizations. In other words, the top-down governance approach can effectively reengineer infrastructures, implement new technology, control schedules of implementations and integrations, and monitor all types of project activities (IT Governance Institute and the Office of Government Commerce, 2005).

Scope and Goals

Clearly defining scope is very important. Clear scope can give team members ideas about the size of projects,

overall estimated time for development and implementation, and which areas the projects will affect.

Knowledge of organizational goals is one fundamental step to integrate business security needs and opportunities in future technical projects (Fumy & Sauerbrey, 2006). Based on organization's goals, developing teams can help to develop comprehensive enterprise plans by identifying a target state, analyzing the businesses current environment, identifying potential risks and opportunities, aligning business and IT security, and eventually translating into IT security infrastructure. This approach can help to ensure that security projects be implemented meet business needs.

Business Framework

When establishing an appropriate and clear enterprise security architecture plan that can be easily implemented, incorporating Zachman's enterprise architecture with enterprise security architecture is believed to be a good practice. The main reason is that the Zachman framework starts from business needs, and then transforms business needs to technical projects, including IT and security projects (Zachman, 1987). Applying the Zachman framework

can help to ensure that all technical projects are actually needed by the business and are implemented in a cost effective manner.

The fundamental step of the Zachman framework is to analyze organizations and their businesses (See Figure 1), which in turn can develop business attribute profiles. Continuously analyzing these collected business attribute profiles helps to identify what organizations' goals are, what an organizations' operating models are, and what the critical success factors are.

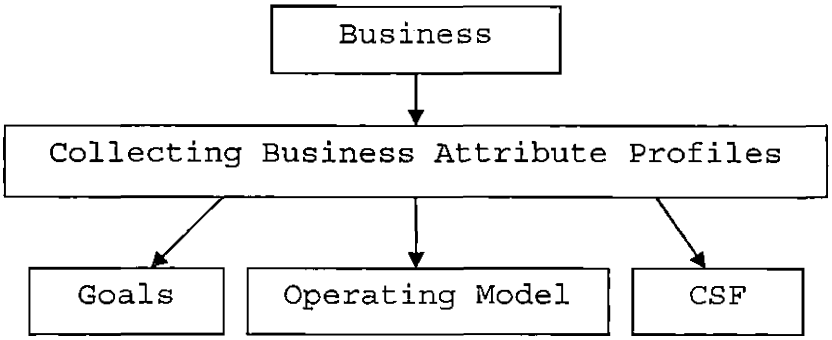


Figure 1. Business and Contextual Security Architecture Derived from (Carbone, 2004; Sherwood, 2005)

Building a business framework can help developing teams efficiently identify all needed information for establishing an appropriate and clear enterprise security architecture plan (Carbone, 2004), which can be effectively implemented. The business framework is composed of the

current state, the target state, and the gap between the two (See Figure 2). Developing teams can analyze gap and know what the CSF are for effectively achieving the target state, which are the organizations' opportunities. Knowing all of the above information helps to ensure that business security needs have been considered for further IT and security projects.

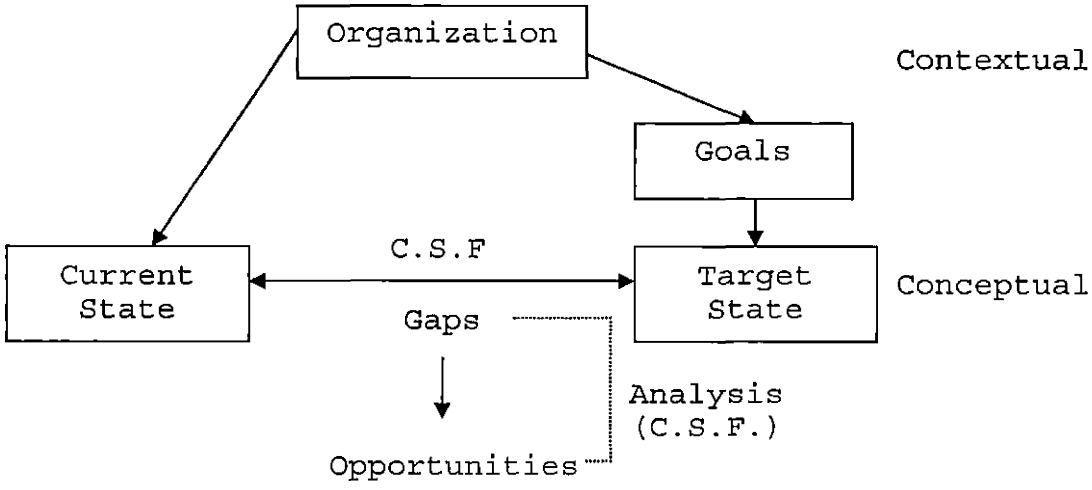


Figure 2. Business Framework
Derived from (Carbone, 2004; Sherwood, 2005)

Gathering Sufficient Information and Documentation

To analyze the current state and construct the target state, developing teams need to collect sufficient information about organizations. Developing teams can start to collect key facts about organizations. See Appendix B

for getting of some essential information that needs to be collected, and some essential collection resources and approaches, which can help developing teams more efficient in capturing the current state and bottom-line security concerns of organizations (Carbone, 2004).

Current Security State

Knowing the current security state can help developing teams establish appropriate enterprise architecture and plan further security projects in cost effective manner. Each organization has different security states. Generally speaking, security states of organizations can be classified into two categories: green-field type and experienced type (Fumy & Sauerbrey, 2006). Green-field type indicates that organizations have very limited security, or may have a less than acceptable level of security for their business and organizations (Fumy & Sauerbrey, 2006). Experienced type indicates that organizations have a well developed security infrastructure in organizations for years to come. These organizations have concrete ideas about information security management, such as security policy, risk management, and business continuity management (Fumy & Sauerbrey, 2006). Usually, it takes a few years of development to go from the green-field type to the

experienced type (Fumy & Sauerbrey, 2006). In other words, different types and states of security will result in developing different enterprise security architectures. Therefore, knowing what types and states of security that organizations currently have is a fundamental and significant step in building appropriate enterprise security architecture, and also helps developing teams to further plan suitable security projects. Collecting information and documentation about organizations and business can help developing teams identify which types and states of security that organizations currently have, which can also be called the current security state in business framework.

Analyzing the Current Security State

Developing teams can use an assessment indicators approach to analyze the current state. This approach can enable developing teams to efficiently summarize the essential current status about organizations. Some basic assessment indicators include stress points, risks, strengths and weaknesses, challenges, environmental factors, and growth/cost containment opportunities (Carbone, 2004). Developing teams can simply list all answers for these assessment indicators first, and then document it.

Constructing the Target Security State

The target state is the state that organizations try to achieve. It embodies the achievement of a mission and goals. Developing teams can start to construct the target state simply by reversing results of each indicator this is defective in the current state. At the target state, all issues mentioned at the current state should be resolved. Developing teams can discuss all answers of each indicator first, and then document it. This process of conversion is a very important step. This step can allow developing teams to obtain a much more clear idea of what the target should be for organizations. Defining targets for further security plans can narrow down the scope of finding sufficient information for establishing a clear plan and easily identifying critical risks (Fumy & Sauerbrey, 2006).

Identifying Gaps, Opportunities (Critical Success Factors), and Potential Projects

Knowing the CSF is extremely important because it transfers business security needs to IT and security projects. Developing teams can start with comparing each statement of the current state with each statement of the target state, and extracting a set of target business opportunities that can direct and drive the IT and security

architecture effort (Carbone, 2004). Developing teams need to identify actions of these opportunities, which will become potential or candidate projects later (See Figure3), and document them.

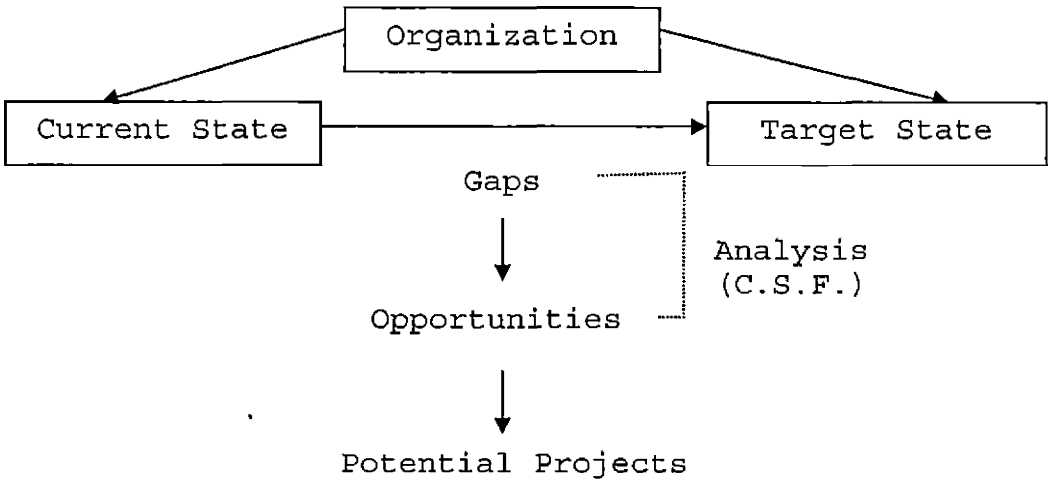


Figure 3. Flow Chart of Identifying Potential Projects Derived from (Carbone, 2004)

At this identification phase, the last thing that developing teams should do is jump to conclusions and state that, "xxx project is what we are going to do". There are two reasons for this. First, if a developing team skips the analysis of identifying gaps and opportunities, not all developing team members will really understand what an organization really needs or the impact of the changed direction. When developing team members are not clear about what can make organizations more competitive, it is not

easy to develop the suitable business architecture (See Figure 4 step 1). An incomplete or inappropriate business model would result in badly designed data architecture, application architecture and technology architecture for organizations (See Figure 4 step 2). Eventually, it would result in failure of implementation (See Figure 4 step 3). Second, analyzing the target state sometimes can bring about different solutions than what was expected at the beginning. Everybody has "blind spots", which causes developing teams to miss some essential points at the beginning. By efficiently analyzing both the current state and target state with appropriate tools, critical issues or potential issues can be easily pinpointed.

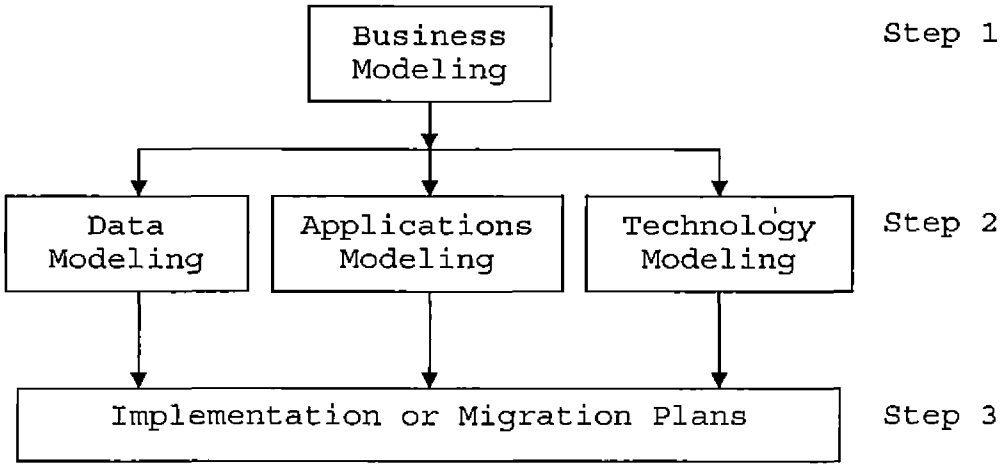


Figure 4. Steps of Modeling and Implementation
Adopted from (Spewak, 1993)

Critical Success Factors - Security. The effective use of policy and security technology is critical to the success of organizations. Critical success factors are factors that enable organizations to obtain a competitive advantage, increase productivity and profile, and ensure a great reputation that comes from providing secure service to customers. Critical potential risks that hurt businesses or cause severe damage for organizations are also CSF. For example, no backup plan for the core database that businesses use every second of the day is a critical risk. Organizations could lose a lot of money when something goes wrong with the core database. Hence, securing the core database is one of the CSF for organizations. The identification of CSF will gain as much benefit as possible from IT and security investment.

Risk assessment and analysis can become a tool to analyze gap, which is between the current security state and target security state, and to identify CSF for organizations at this phase. One main purpose of risk assessment and analysis is to identify risks and to prioritize them. These critical risks are critical success factors because reducing or removing these critical risks can protect business drivers from keeping or gaining

competitive advantages in organizations. Therefore, risk assessment and analysis can play an essential role in analyzing gaps and in identifying CSF.

Risk Management and Analysis. Risk management is also an essential pre-requisite to make organizations secure. Security policies and risk management play different roles to keep organizations secure. Security policies are "the bottom line-the boundaries of security acceptability" (The Information Security Policies & Standards Group, 2007) while risk management plays the role as a supplement to security policies. From a security perspective, some areas may be more sensitive than others within organizations. Applying risk management in organizations can supplement security policies for these sensitive areas that need more stringent security measures.

The Importance of Risk Management and Analysis. Organizations would suffer serious loss if they do not pay enough attention to potential risks resulting from external factors (e.g. attacks), or from failed or inadequate internal processes, people, and systems. Risk assessment can reduce the probability of loss and damage, caused from threats. Risk concept has five basic elements: assets, threats, impact, vulnerabilities, and likelihood (Sherwood,

2005). Assessing risk involves identifying assets that organizations have to protect for running daily businesses, identifying threats that may cause damages, evaluating and knowing impact of threats, identifying vulnerabilities that become weakness parts for potential attacks, and determining likelihood of vulnerabilities. Therefore, the result of risk assessment is one of the essential drivers for enterprise security. Developing teams also can base decisions on the result of assessing risk and business needs to establish appropriate enterprise security sub-architectures for information, applications, and technology.

Life Cycle of Risk Management and Analysis. The life cycle of risk management and analysis is illustrated in Figure 5. The first phase is to form risk management and analysis teams. The second phase is to perform risk assessment and analysis. There are many methods and various steps for assessing and analyzing risks. This paper covers only some of the common main steps. After the second phase, teams should regularly track risk for preventing disasters from happening suddenly.

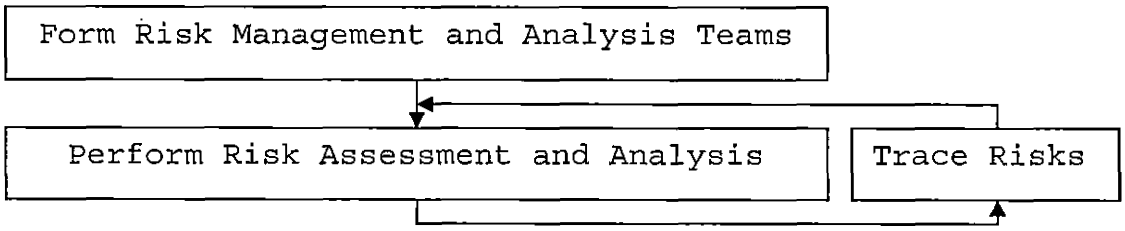


Figure 5. The Life Cycle of Risk Management and Analysis

Risk Management and Analysis Teams Formation. The main purpose of risk management is to continually identify, assess and analyze risk, prioritize risk, reduce risk levels to acceptable levels, and implement appropriate protection strategies or mechanisms for keeping organizations secure (Carnegie Mellon Software Engineering Institute, 2007). The main goal of risk management team is to protect organizations in the most cost-effective manner (Harris, 2005).

A risk management team is composed of current full-time senior employees, not new employees. Full-time employees have been working for organizations for a while so they understand the organizations status, including weaknesses, threats, strengths, and so forth. It would be a better practice to have managers in teams because strong management support is a key factor for successfully implementing projects. These ideal candidates include

senior managers, chief information officer, system information owners, department managers, IT security program managers, IT security officers, administrators, security specialists, computer specialists, or security awareness trainers (Stoneburner, Goguen1, & Feringa, 2002). Leaders of a risk management team can be either IT security program managers or IT security officers.

Risk analysis is like a tool for risk management (Harris, 2005). Risk analysis is used to identify risk and loss that those risks may cause, and then to determine which risks should be handled first and then to take appropriate actions for protecting organizations against them.

Having senior professionals or employees from different departments in teams can help to easily point out vulnerabilities in their professional areas. In other words, it would be a great practice to have various backgrounds in teams for ensuring that all threats can be pinpointed and handled. These desired candidates can be security specialists, IT administrators, systems administrators, data administrators, IT employees who work directly with applications, or representatives at different levels of all management (Threat and Risk Assessment Working Guide, 2007).

Interviews can be conducted if some of them are not able to be included in teams.

For efficiently assessing and analyzing risk, all team members should have a clear idea about why the team is formed, and what they are expected to contribute.

Risk Assessment and Analysis. For performing risk assessment and analysis, there are many methods with various steps. These methods fall into two categories: quantitative and qualitative approaches. For conducting quantitative risk assessment and analysis, teams need to use actual numbers and industrial formulas to calculate monetary loss of each threat for assessing, analyzing, and prioritizing risks. For conducting qualitative risk assessment and analysis, teams do not need to know neither actual numbers nor industrial formulas. Teams simply need to know scenarios of threats, and use simple scales to determine the degree of business impact, vulnerabilities, and likelihood for assessing, analyzing, and prioritizing risks (Harris, 2005).

This paper covers only some of the common main steps for performing risk assessment and analysis (Harris, 2005; Sherwood, 2005; Shoniregun, 2005; Stonebumer, 2002), as illustrated in Figure 6. The first step is to set the scope

for assessing and analyzing risks. The second step is that teams need to identify information and assets, and then assign a value to each asset. The third step is to identify threats, followed by analyzing business impact, assessing vulnerabilities and likelihood. After gathering all needed information, teams can start to assess, analyze, and prioritize risks, which is step six. Step seven is to select the most appropriate countermeasures and protection mechanisms for organizations, based on the result of assessing, analyzing, and prioritizing risks. These countermeasures and protection mechanisms can fall into four categories: rejecting, reducing, transferring, or accepting risk. The last step is to plan and take action to handle risk.

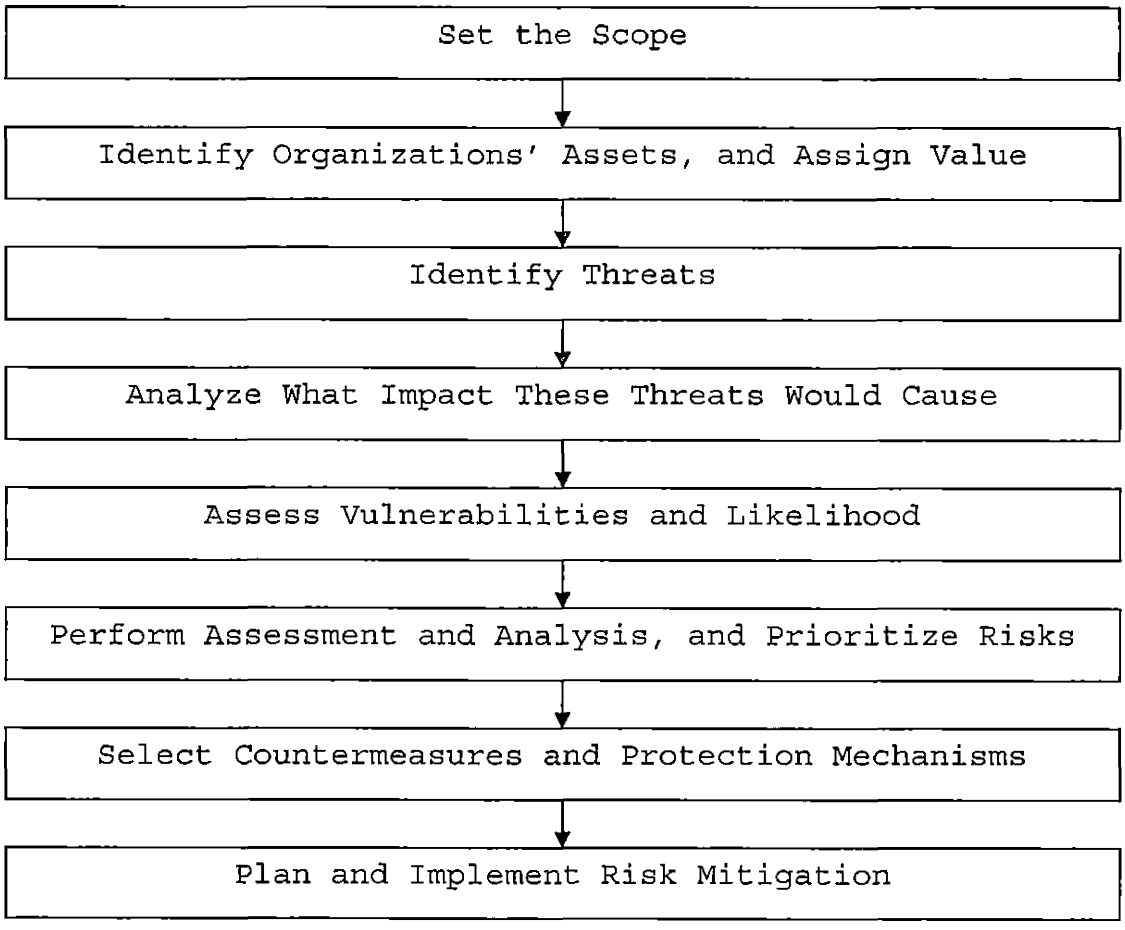


Figure 6. Steps of Performing Quantitative Risk Assessment and Analysis
Derived from (Harris, 2005; Sherwood, 2005; Shoniregun, 2005; Stonebumer, 2002)

Step 1: Set the Scope. It is always a good practice to set the scope for each project. Performing risk assessment and analysis should enable a team to set the scope. Setting the scope can allow all team members to have an overall picture about what they should focus on and where they will go.

Step 2: Identify Organizational Assets, and Assign value. It is important for teams to know what should be protected and how much it would cost if appropriate protections are not applied. Team members can base on the scope of the project, organizational attributes, policies, or external drivers, such as standard compliance and regulations (Threat and Risk Assessment Working Guide, 2007), to identify all assets. In the quantitative assessment and analysis approach, for precisely assessing and analyzing risk, teams also can assign the total estimated value to assets. The total estimated value of assets not only includes the value of tangible assets, but also includes the value of intangible assets, personnel, and services (Beauchemin & Dansereau, 2007). Identifying organizational assets and knowing their value can also give a team a much clear idea about what the most important assets are and which levels of protection are worthy and should take place.

Step 3: Identify Threats. Based on different types of threat agents, threats can be classified into eight categories: virus, hacker, user, fire, employee, contractor, attacker, and intruder (Harris, 2005). Teams can focus on those identified assets to make a list of all

threats, which are relative to the identified assets. In addition, teams can try to identify threats by looking at process, design, test results, potential shortfalls, dependencies, and so forth (Department of Defense, 2006). No matter which method a team uses for listing threats, they should begin to identify threats as early as possible and should regularly review them. The difference between the quantitative approach and qualitative approach is that scenarios of threats should be discussed and documented in the qualitative approach.

Step 4: Analyze What Impact These Threats Would Cause. Teams need to assess these threats by analyzing what impact these threats would cause for organizations and their businesses. There are two different approaches, quantitative and qualitative approaches, to analyze what impact these threats would cause.

Quantitative Approach for Impact Analysis. One of the popular approaches to calculate impact is the single loss expectancy (SLE) (Mealy, 2005). SLE is equal to the value of a certain asset times percentage of impact that a threat would cause on this certain asset (SLE = asset value * percentage of impact). Percentage

measurement of impact can also be called exposure factor (EF) (Mealy, 2005).

Qualitative Approach for Impact Analysis. Teams can use a simple scale to prioritize these threats, which allow readers easily understand which threats should be taken care of right away and which threats will not be very harmful to the organizations. There are two types of scales used in general. The first is a scale with high impact, medium impact and low impact. The second is a scale with 1 to 9 scores (Carbone, 2004). The number '1' indicates less impact while the number '9' represents severe impact to organizations. In order to use the simple scale method, teams should also describe a scenario of threats and potential consequences for a clear understanding and documentation (Hansche, Berti, & Hare, 2004).

Step 5: Assess Vulnerabilities and Likelihood. Assessing vulnerabilities and the likelihood of occurrence can help teams identify what vulnerabilities organizations have and their likelihood of occurrence. This step can help teams clearly understand an organizations weaknesses and strengths for building solid security infrastructures in the future. There are two different

approaches, quantitative and qualitative approaches, to assess vulnerabilities and their likelihood.

Quantitative Approach for Assessing Vulnerabilities and Likelihood. Assigning estimated percentages as likelihood can help teams calculate the annualized loss expectancy (ALE) (Meritt, 1998), prioritize risks, and calculate total risk and residual risk (Harris, 2005) in the following steps. Estimated percentage is called "the annualized rate of occurrence (ARO)" (Harris, 2005). It is based on a one-year timeframe to calculate the estimated percentage of a certain threat occurring. The estimated number '0' means that it will not take place. The estimated number '1' means that it will take place once per year. The estimated number that is larger than the number '1' means that it will take place several times per year. For example, using airplanes to attack an organization main building may occur once in 2000 years, the value of ARO will be 0.2% (1 / 2000 = 0.002 = 0.2%).

Qualitative Approach for Assessing Vulnerabilities and Likelihood. Teams can use the same simple scale method (Hansche, Berti, & Hare, 2004) as the previous step used for clearly documenting likelihood. If teams use the scale with high impact, medium impact and low

impact for prioritizing these threats by their impact at the previous step, teams should use the same scale to indicate likelihood at this step. If teams use the scale with 1 to 9 scores at step 3, then teams should use the same scale method at this step. Using the same scale method for step 3 and step 4 can facilitate teams to perform assessment and analysis, and to prioritize risks at the next step.

Step 6: Perform Assessment and Analysis, and Prioritize Risks. Each the previous steps are preliminary steps that lead to step 6 which assesses, analyzes and then prioritizes risks. After assessing, analyzing, and prioritizing risks, the developing teams are able to allocate limited resources for risk mitigation and management. Otherwise, it would not be easy to prevent organizations from severe damages, such as loss of revenue. There are two different approaches, quantitative and qualitative approaches, to perform assessment and analysis and to prioritize risks.

Quantitative Approach for Risk Assessment, Analysis, and Prioritize. After collecting sufficient information during the previous steps, teams can use the industry accepted formula for calculating the

annualized loss expectancy (ALE) (Meritt, 1998). The annualized loss expectancy (ALE) is an estimated monetary loss on assets per year, which is caused by a certain threat. The purpose of ALE is to provide teams with ideas about how much the organization should spend for providing protection. Teams can also calculate total risk and residual risk. Total risk is all of the various kinds of risks that organizations face if there is no protection at all. Teams can multiply asset value by threats and vulnerability for getting the value of total risk (total risk = asset value * threats * vulnerability). Residual risks are risks that have been left over to deal with. For the value of residual risk (residual risk = total risk * control gap), teams can multiply total risk by control gap (Harris, 2005), which is the gap between risks that are able to be controlled and risks that have been left to deal with. After teams know all values of the ALE, total risk, and residual risk, teams can start to prioritize risks. Usually, the highest value of ALE should be protected first while the low value of ALE should be protected last.

Qualitative Approach for Risk Assessment, Analysis, and Prioritize. Developing teams now can create the graph (See Figure 7 or Figure 8) for easily

assessing, analyzing, and prioritizing risks. The X axis represents business impact while the Y axis represents likelihood. The difference between figure 7 and figure 8 is the scale. In figure 7, the scale high, medium, and low are used. In figure 8, the number '9', '6', and '3' are used. The lower number means less likelihood of occurrence while the higher number means higher likelihood of occurrence. Developing teams can base decisions on information gathered in steps 3 and 4 to prioritize risks. Developing teams should focus more on higher business impact and likelihood than lower business impact and vulnerability. Developing teams can define different categories for prioritizing risks (Department of Defense, 2006; Sherwood, 2005). Developing teams also can define different colors for representing different categories. Figure 7 and figure 8 illustrate how to utilize four categories and their colors to prioritize risks. Category A, represented in red, means that risks are severe, and these types of risks have the most resources for risk mitigation. Category B, represented in yellow, indicates that risks are significant. Category C, represented in green, represents that risks are acceptable. Category D, represented in blue, means that risks are negligible.

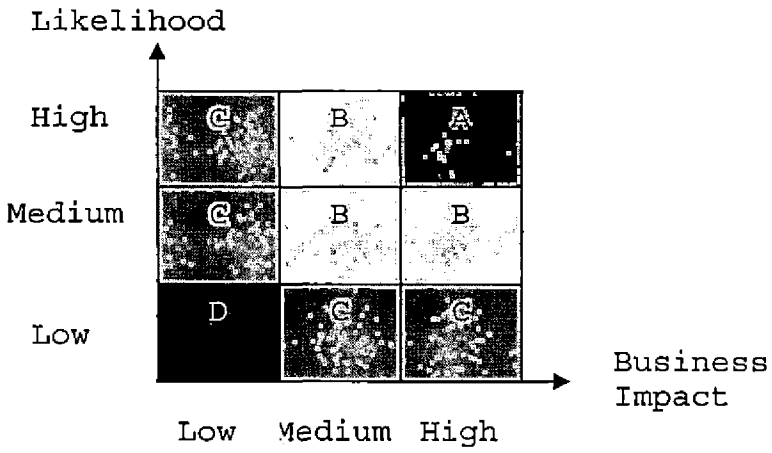


Figure 7. Risk Assessments and Analysis, and Prioritize Risks (1) Adopted from (Sherwood, 2005)

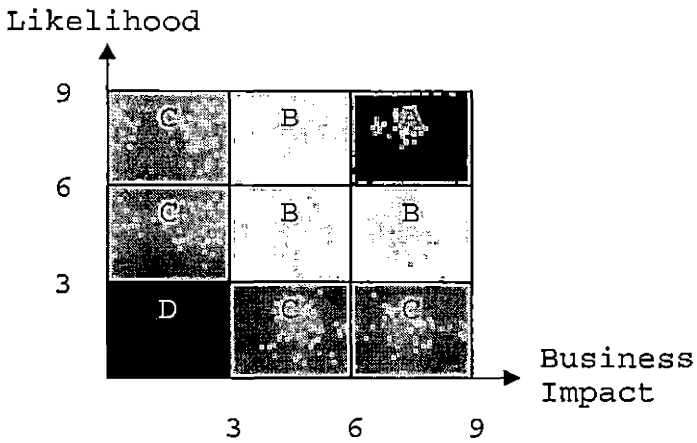


Figure 8. Risk Assessments and Analysis, and Prioritize Risks (2) Derived from (Sherwood, 2005)

Step 7: Select Countermeasures and Protection Mechanisms. Risk prioritization, which is done

during the previous step, gives developing teams some ideas about what the most critical risk is, how much it will cost organizations if appropriate protection mechanisms have not been implemented, and how much organizations should spend on protection mechanisms. At this step, developing teams start to take action to find the right countermeasures for protecting organizations. The main purpose of this step is to evaluate various kinds of countermeasure, and identify which countermeasure is the most appropriate solution for a certain critical risk. In comparing processes, developing teams not only need to look for the best features of countermeasures, but also need to investigate different cost scenarios by a cost/benefit analysis (Harris, 2005). Through the selection process, developing teams will know which countermeasures can provide the most benefit to organizations, and what the most advantage organizations will gain from the chosen countermeasure if the target countermeasures have been implemented successfully. In other words, the chosen countermeasure should be of the highest advantage to organizations among different countermeasures. Selecting the best and right countermeasures for organizations can reduce probability of

risk taking place and reduce cost of damage if disasters happen.

There are four methods (Department of Defense, 2007) to mitigate risk. The first method is to avoid risk. Developing teams can implement countermeasures to reduce or eliminate risks. The second method is to control risk. Some types of risk are controllable, such as employees' misbehaviors. Employees can be trained to develop increased awareness of security and to consciously change behaviors. The third method is to transfer risk. One example is to use honey-pot intrusion detection systems (IDS). The honey-pot IDS acts like a honey pot, and can simulate vulnerable systems, which can make intruders think that they have found the target. This type of system can transfer risks from the real system to simulating systems, which can reduce damage to organizations.

The last one is to assume the level of risk. This type of risk can be a very minor risk that will not hurt organizations much. In addition, the cost of implementing countermeasures and protection mechanisms is higher than the monetary cost of damages resulting from risks. Hence, assuming the level of risk may not be a bad idea in this case.

Step 8: Plan and Implement Risk Mitigation. At this phase, developing teams can base decisions on the chosen countermeasures or protection mechanisms to establish a risk mitigation plan and implement it for mitigating risk successfully (Department of Defense, 2007). A risk mitigation plan should include requirements of mitigating risks, risk mitigating approaches, detail procedures about how to mitigate risks, and an organizations previous history of mitigating risk. Support from top managers to allocate budget and time is the main factor for effectively implementing the plan.

The Role of Risk Management and Analysis in the Zachman EA Framework. Risk management and analysis is an important approach to analyze the current security state and the gap, and to identify CSF. The result of assessing risk becomes one driver for securing organizations and their businesses. The assessing result can also be used to drive through the detailed design of security controls at different architectural levels. Figure 9 illustrates the role of risk management and analysis in the business model of the Zachman EA framework. The second and third steps of risk management and analysis are to identify the current assets, value, and threats. The fourth and fifth steps are

to analyze the gap between the current security state and the target security state by analyzing what impact identified threats would cause, assessing vulnerabilities and likelihood, performing assessment and analysis, and prioritizing risk.

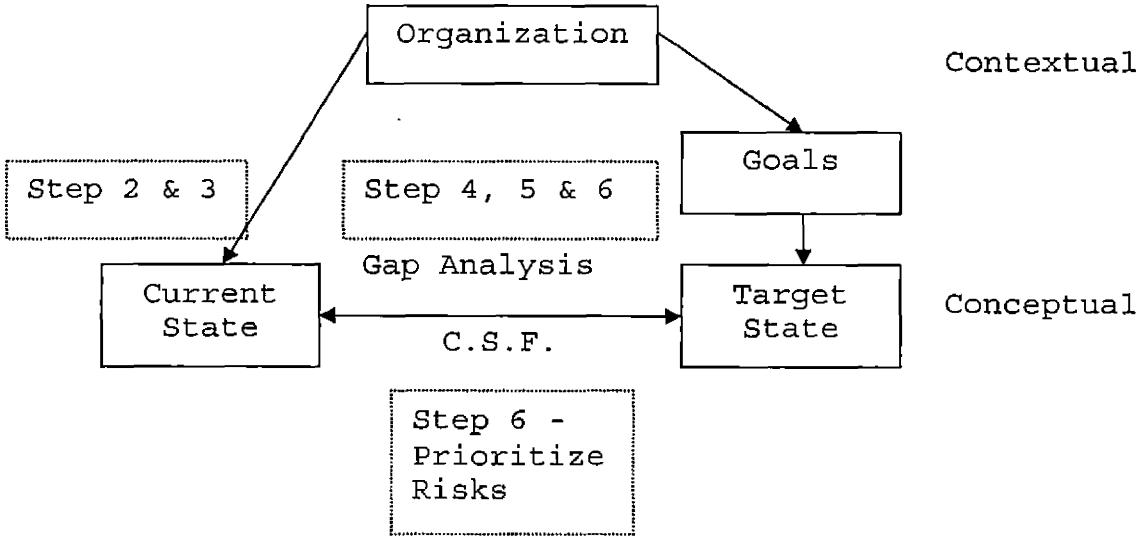


Figure 9. The Role of Risk Management and Analysis in the Business Model of the Zachman EA Framework Derived from (Carbone, 2004; Sherwood, 2005)

Alignment

Similar to alignment between businesses and IT technology, alignment between businesses and security technology plays an important role in an organizations success. Emphasizing business more than security technology or emphasizing security technology more than business will

not bring maximizing benefit to an organization. The former situation will create a lot of potential risk, while the latter situation will cause organizations to spend too much money on security controls than what optimal benefit organizations gain. From the investment perspective, there is an optimal cost/benefit point (See Figure 10 and Figure 11) (Anderson & Choobineh, 2008; Fumy & Sauerbrey, 2006) between cost of potential impact from risk happening and cost of security controls. This optimal point can make sure that an investment is occurring in a cost-effective and well-controlled manner. Therefore, alignment between business and security technology is the best decision for organizations, as illustrated.

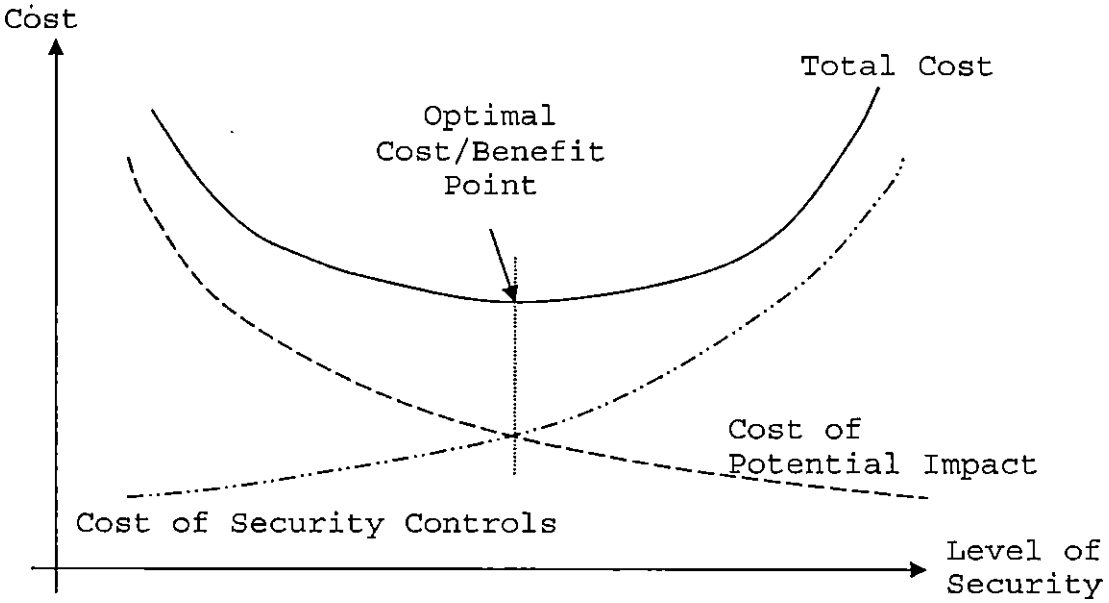


Figure 10. Optimal Investment Point
Adopted from (Fumy & Sauerbrey, 2006)

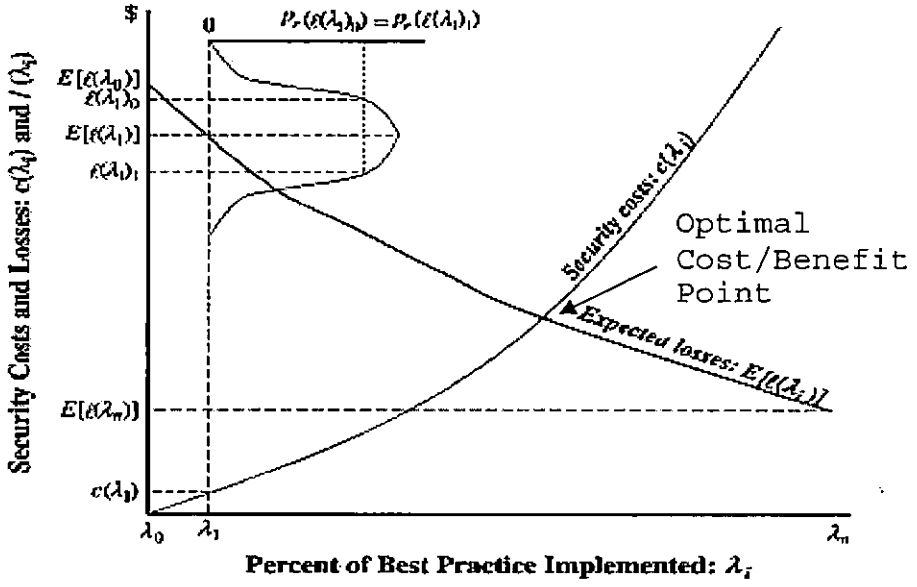


Figure 11. Alignment between Best Security Practice Implemented and Security Cost and Losses. Adopted from (Anderson & Choobineh, 2008)

Business Architecture

The foundation of the Zachman EA framework includes four essential architectures: business, data, application, and technology architectures. The business architecture is the graphical representation of the organization and the business (Spewak, 1993). The purpose is to provide an essential and complete knowledge for developing the data architecture, application architecture, and technology architecture, and for the implementation phase (See Figure 12). Any model that can identify the organization unit that is performing each business function should be included in the business architecture. An organizational chart, strategy model, goal model, and operating model are basic elements for the business architecture (Ross, Weill, and Robertson, 2006; Spewak, 1993). Developing teams can use the business framework to construct the business architecture. The current state is the current situation of organizations and business, and the target state is the state that organizations try to achieve, such as reducing risk, lowering cost, increasing profile, or being more competitive. Developing teams can simply base decisions on the result of the business framework for constructing level 0 current state and target state. In addition, developing

teams can also identify each business function with a brief description, which can help for constructing the other three architectures and implementation plan in the future.

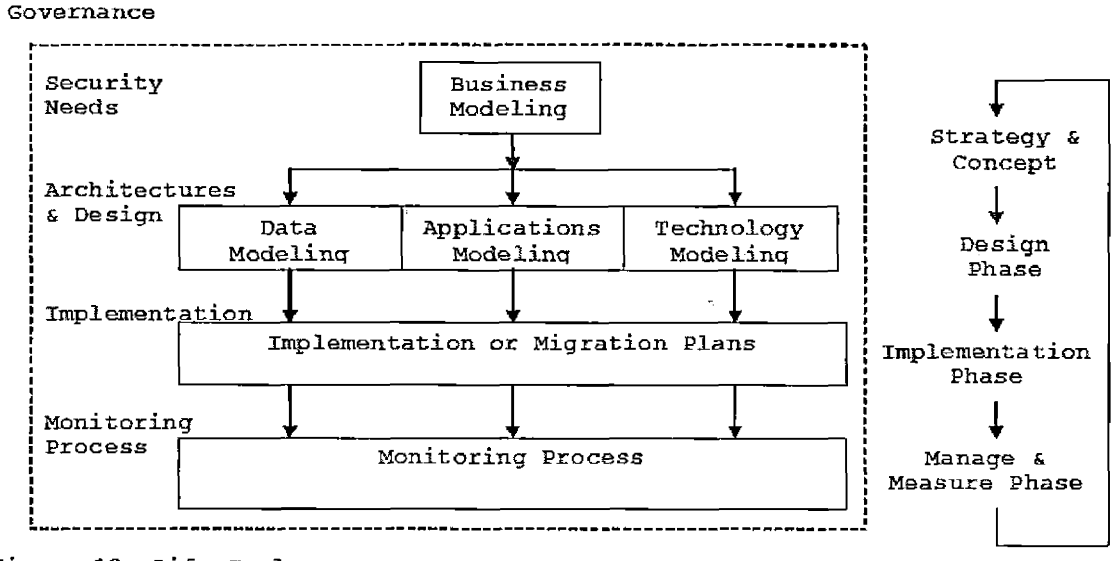


Figure 12. Life Cycle
Derived from (Sherwood, 2005; Spewak, 1993)

Framework for Securing Data, Application, and Technology

One essential principle of the Zachman EA framework is to develop a data model, an application model, and a technology model from the business model. Considerations need to be taken that there are differences among organizations as they differ in sizes, financial status, reputations, organization charts, states of technical environments, and so forth. That means that each organization has different business models and security

needs, which results in developing different data architecture, application architecture, and technology architecture for providing enterprise security.

Secure Information / Data

After defining business architecture, developers should define the data architecture first because data is the essential element of the information system function. The data architecture identifies and defines key data, which support the business functions. The data architecture is the foundation for the systems design, physical database design and database creation. In other words, it is a vehicle for analyzing the logical structure of an organization's information in the future. The data architecture consists of data entities, attributes, and relationships with other data entities. At the implementation phase, analysts and designers will have time to add more detail for creating the conceptual data architecture.

In most cases, physical databases have existed before creating the enterprise architecture. Hence, creation of the data architecture has to be based on the current data infrastructure, which is the current state of the data architecture. The target state of the data architecture

derives from the target state of the business architecture, which includes business functions and key information. Analyzing what the basic information blocks of the organization needed for achieving the goals can generate the list of sufficient data entities and the relationship among these identified key data entities.

Security Services for Data Management Function. When designing data architecture, developing teams should focus on four essential security services: access control, authorization, authentication of SQL requests and responses, and protection for data availability, integrity and confidentiality (Sherwood, 2005). Access control to different levels of data should be appropriately controlled with appropriate privileges granted. Privileges can be granted, based on subject roles or database function if conventional databases are used. Authorization should be granted, based on business needs. Authentication about executing SQL codes should really be paid attention, especially for accessing databases remotely. Protection for data availability, integrity and confidentiality can be achieved by various mechanisms. Applying various backup and restoration techniques can keep data available. Atomic transactions and commitment can maintain quality and

accuracy of stored data. Encrypting data can make sure that only authorized subjects are able to access stored data.

For easily managing security services in the data management systems, data classification and the designation of roles must be applied. Developing teams can base on sensitivity degree of data to classify data. Developing teams can base decisions on an employee's position, tasks, and business needs to design and assign them appropriate accessing roles for accessing different levels of data. The designation of roles can make authorizations and authentications easy to perform in data management systems.

Security Guideline. Sensitive data includes, but is not limited to, cost of products and employee data. Below are some security guidelines (Harris, 2005):

- Sensitive data needed to be protected includes an individual's education, social security number, medical history, financial history, criminal history, employment, and other similar types of information.
- Organizations cannot disclose this information without written permission from the individual.

- The reason for gathering data must be specified at the time of collection
- Data cannot be used for other purposes
- Unnecessary data should not be collected
- Data should only be kept for as long as it is needed to accomplish the stated task
- Always backup

Secure Application / Information System

The application architecture can provide an overview of major applications needed to manage the data and support the business functions of an organization. The application architecture is not a design for systems; rather it is a definition of what major applications should take place for managing data and providing functions for enterprise-wide employees. It can help organizations achieve a stated mission at an acceptable cost.

The current state of application architecture consists of all applications that employees currently use for daily operations. The target state of application architecture will include all new application systems that can help an organization resolve current critical problems and issues at an acceptable cost. Examining opportunities and

analyzing the business architecture for conceiving opportunities and evaluating their contribution can provide a clear idea about what new applications should be. Team brainstorming also can generate good ideas about new application systems.

Security Services Needed. The main focus for application security is authorization. Developing teams should focus on whether users are granted privileges appropriately to perform the right tasks at the appropriate levels in the right applications. For achieving this mechanism, the application developers should include a few essential services within the application architecture: authorization, authentication, access control, audit, application-to-application communication security, and administration (Sherwood, 2005). The application architecture should have the process of granting privileges, and be able to verify whether users are authorized parties and to make access decisions based on a user's authorization status and authentication status. In addition, the application developers should include the process to audit trails, which can tell administrators about who did what at what time. Besides, developing teams should not ignore security among each application-to-application

communication. Confidentiality, integrity, authenticity, and non-repudiation are needed security services for application-to-application communication security. All these processes and services should be appropriately controlled by an administrator, which is referred to as security administration.

Security Guidelines. Applications provide a way to access data so access control for using applications becomes an extremely import factor for security. Below are some security guidelines (Harris, 2005):

- Only the necessary individuals who are required to accomplish the stated tasks can be allowed to use applications to access data
- The person responsible for maintaining applications and securely storing relative data should not allow unintentional "leaking" of data.

Integrated Application Architecture. From the entire application architecture perspective, the integrated applications architecture (Sherwood, 2005) is the best practical approach. The integrated application architecture (See Figure 13) means that there are common data repository, common interfaces, common services, and common external

interfaces among all business applications. Each application has accesses to common data repositories through common interfaces. Normally, there is separate layer between applications and common interfaces, and this layer has two categories: common services and common external interfaces. Examples of common services are printing services or security services. Examples of common external interfaces are web interface, banking interface, or B-2-B Electronic Data Interface (EDI) interface.

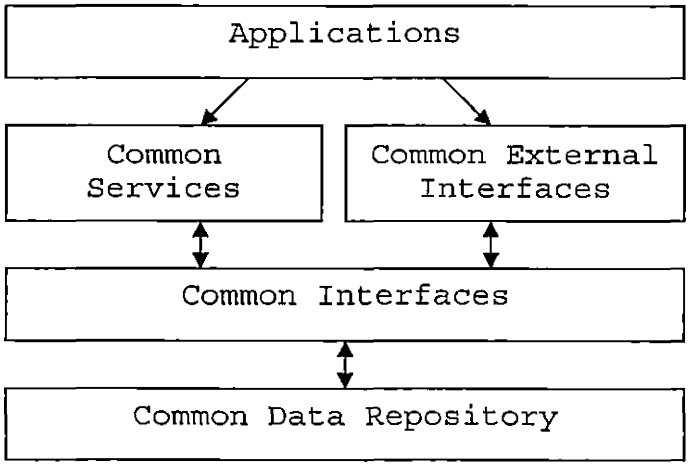


Figure 13. An Integrated Applications Architecture Adopted from (Sherwood, 2005)

There are a few advantages (Sherwood, 2005) for this wholly integrated application architecture. The first advantage is usage simplification for users. This type of application architecture not only asks users to simply sign

in once for using business applications, but also provides only one window (interface) for user administration. This can reduce cost on training, support, and administration, and it also can increase productivity. The other advantage is that there is only one database for storing information about authorization. This can simplify many processes for better control and maintenance.

Secure Technology

The main purpose of technology architecture is to provide appropriate environment for supporting business operations. The environment can make needed data and applications available to employees without concerning geographic difference and issues of physical facilities. Therefore, the first step of developing the technology architecture is to define the major technology that could provide all employees an environment for using applications and managing data. At the architectural phase, developing teams just need to 'define' major technology, such as the pipeline and physical facilities of utilities. Developing teams at this phase do not need to 'design' enterprise-wide computing networks for supporting the business operations with a shared data environment, as this will be done at the design phase.

Similarly with previous architectures, the current state of technology architecture consists of all platforms used for supporting current business. Developing teams construct the target state of the technology architecture, based on what business opportunities are, what business operating needs are, and what platforms are needed for using applications and managing data.

Strategies of Network Security. The network security does not exist solely for protecting application and data, it is also there for controlling and monitoring who and what have been transmited through the network and at what time. The goals of network security are to provide protection to the network management flows, and to prevent theft of bandwidth by unauthorized users. Appropriate network management can provide users with a high-quality, reliable and highly available connectivity (Sherwood, 2005).

A number of organizations have applied different forms of encryption technology for securing a network. However, applying these encryption technologies, such as VPN, SSL, TLS and IPSec, can provide only limited value for network security. For deploying the valid network security services, network security strategies should also be considered simultaneously (Sherwood, 2005), which lists below.

- Security policy for Network: need to define network domains, assign domain ownership, set domain security policy, need awareness on security policy, provide training on security policy, and implement network security policy successfully
- Segregation of network domains: need to have security gateways-firewalls at domain boundaries, and need to have relative security rules for firewalls to apply domain policy
- Redundancy and resilience of network components: need to have diverse routing, few access points, redundant equipments, and enough bandwidth for business needs
- Authentication of network entities: need to have authentication for mutual node-to-node or router-to-router within the entire network, for external entity at the network boundaries, and for managing network services
- Authorization of network entities: need to define roles that are associated with external network entities and define these roles' service profiles

- Boundary access control for network: need to have security gateways or firewalls to control boundary access for traffic from flowing into and out of network domains, and relative rules for restricting services
- Connectivity control: need to have authorization for connections, change control, and physical and logical security standards for all network nodes
- Management security for network: need to have operator entities that are authorized, access control, appropriate securing protocols for 'get' and 'set', remote authentication for operator entities, integration with system management architectures, and integration with management infrastructure
- Integrity protection of network resource: need to control software development lifecycle, control production, control delivery, control installation, control configuration, have operational lifecycle, have integrity for configuration data and routing table, and mange change

- Monitoring network and intrusion detection for network security: need to have instruction detection, have even logging and analysis at servers and majors network devices
- Incident handling for network security: need to include reporting, confirmation, escalation, response, recovery, analysis, and lessons learned
- Vulnerability research for network: need to collect, collate and analyze advisory notices, need to perform penetration intrusion test, and need to gather internet intelligence, including who is talking about us, what they are talking about, and why they are talking about it

Strategic Principles of Platforms Security. There are some strategic principles for designing security services on platforms and environments. These strategic principles include reducing vulnerabilities on platforms, segregating and isolating execution platforms and environments from development and tests platforms and environments. These principles also provide and maintain trusted platforms and environments for processing sensitive data and provide

secure storage for storing sensitive non-volatile data (Sherwood, 2005).

In addition to these strategic principles, developing teams could also focus on some major platform security services. Physical and environmental security for protecting platforms is the essential category of platform security services. The next category of major platform security services regards controlling local access and remote access. This includes user authentication, user access control, and audit trails. The next platform security service is to provide cryptographic services from local sub-systems. Local sub-systems can be hardware and software. The fourth category is to provide anti-virus services for protecting platforms, detecting intruders, reporting the status of platforms, restoring and recovery platforms back from virus and other malicious software attacks. The fifth category of platform security services provides control and management, such as change control, configuration control, security administration, operations management, and so on. The last category is to plan ahead for procedures on how to backup and to recover from disasters.

Technology Architecture. There are many ways to establish architectures for systems, platforms, and networking. Generally speaking, the more common secure architectures (See Figure 14) include outer hardened perimeter with a gateway, and few internal hardened perimeters with a gateway at different layers (Sherwood, 2005), as shown in Figure 14. Within different internal perimeters, the honeycomb model of security can be applied. The honeycomb model of security can make sure that privilege to access to one cell of the honeycomb cannot access to other cells of the honeycomb. The multi-layer hardened perimeter protection can make it hard for hackers to access the most sensitive data within the most internal perimeter. It can reduce the degree of damage when some disasters occur as well.

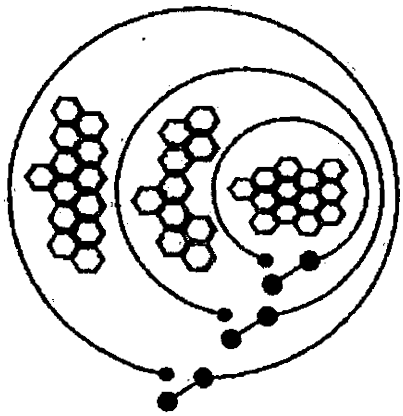


Figure 14. Common Secure Architectures
Adopted from (Sherwood, 2005)

Security Framework - The Life Cycle of Developing Security Policies

From security perspectives, security policy is a starting point for securing organizations. Security policy is designed to define how organizations protect and maintain the confidentiality, integrity, and availability of data resources, information systems, and network resources (Harris, 2005). In addition to ensuring the confidentiality, integrity, and availability of data resources, information systems, and network resources, developing security policies ensure compliance with external and internal requirements. External requirements are derived from laws and regulations for specific industries. Internal requirements not only can be derived

from the organization's business objectives, mission, and policies, but also can be derived from the needs for reducing risks, avoiding disasters, or compliant with standards, such as ISO 27000-series, CoBit, and ITIL. Another benefit of developing and maintaining security policies is to demonstrate the practice of 'due care' and 'due diligence' (Harris, 2005) within organizations.

Develop and Maintain Security Policies

Before developing and maintaining security policies, there is one essential preliminary phase. The preliminary phase is to build a solid foundation (Walker & Cavanaugh, 1998), which prepares all needs for developing security policies. The second phase is to develop security policies, followed by communicating with users and then implementing it. Developing teams also need to manage incident, which can prevent organizations from being hurt twice by the same incident. For ensuring a quick and effective response to security incidents, defining incident response is a must. The next step is auditing. This step monitors for compliance to security policies. The last phase is to regularly review security policies and update them. Figure 15 briefly depicts the entire cycle of developing and maintaining security policies (Walker & Cavanaugh, 1998).

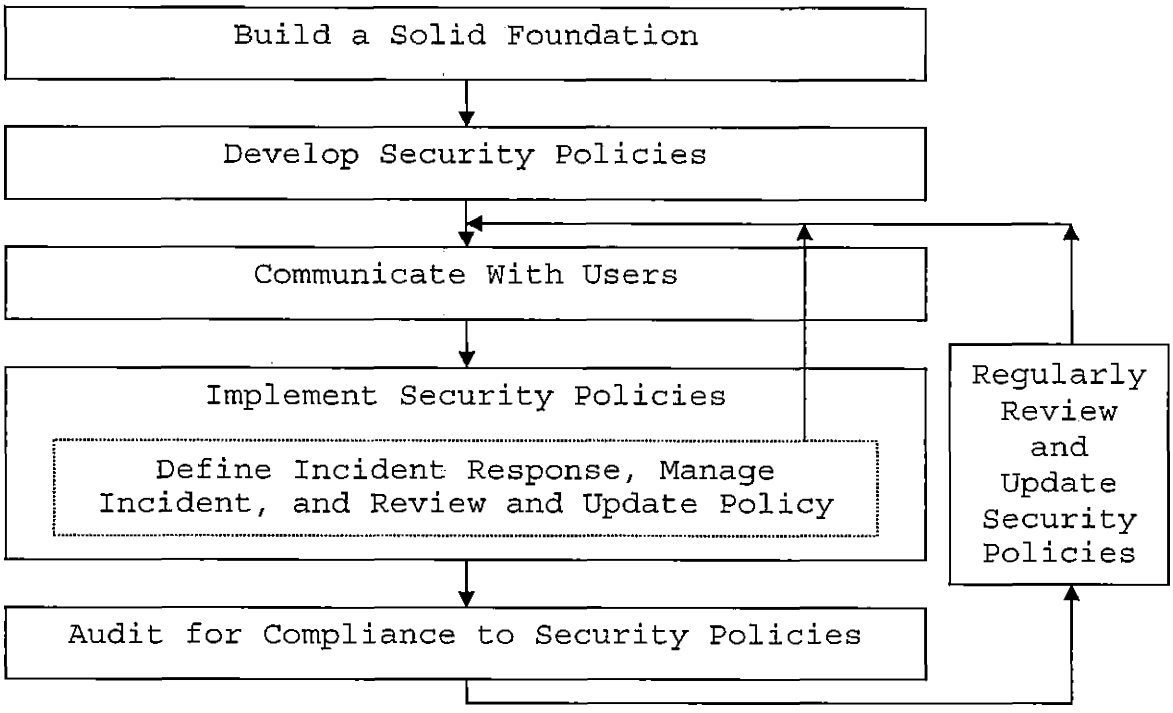


Figure 15. The Cycle of Developing and Maintaining Security Policies
Derived from (Walker & Cavanaugh, 1998)

Build a Foundation. The preliminary phase of developing and maintaining security policies includes many steps (See Figure 16). The first step is to establish a mission statement (Walker & Cavanaugh, 1998). A mission statement should not be too long. Short and clear mission statements can be easily understood in terms of overall goals or objectives of developing security policies and can help developing teams focus on security policies.

The second step is to identify the organization's assets. The process includes knowing all items that needed to be protected to ensure integrity, confidentiality, and availability. In addition, the process needs to record the items location and owners. Summarizing all this information in documentation can assist in further analysis for developing security policies (Walker & Cavanaugh, 1998).

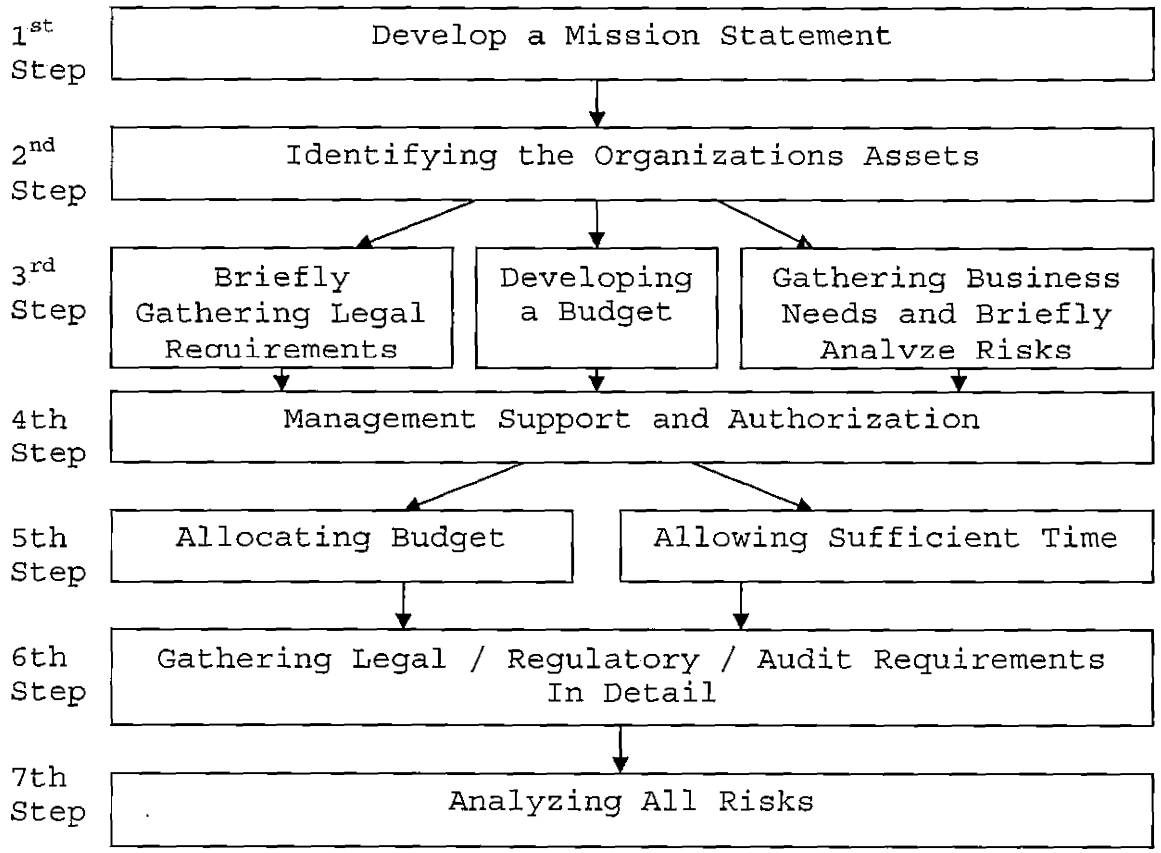


Figure 16. The Preliminary Phase of Developing and Maintaining Security Policies Derived from (Walker & Cavanaugh, 1998)

After identifying which assets need protection, the next step is to prepare needs for management support (Fedor et al., 2003). Management support plays an important role for implementing security policies effectively and efficiently (Walker & Cavanaugh, 1998). This step entails briefly gathering requirements from external and internal environments and to develop a draft budget. External environmental requirements refer to those from legal, regulative and auditory requirements. Internal environmental requirements derive from business needs, which includes organizational objectives, missions, and all areas or aspects that need to be protected for securing the entire enterprise and business units. In addition to gathering brief legal requirements and business needs, developing a draft budget is a must for applying financial support from management. Budgets should include cost for time, personnel who will be involved in developing security policies, supporting hardware and software equipments for developing security policies (Walker & Cavanaugh, 1998). Brief risk assessment (Refer to the session 'Risk management and Analysis') is a good tool to gather internal security needs. Information collected from the brief risk assessment also can be used for persuading managers into

supporting the project. After managers support the project and allocate budget and time, developing teams should start to gather external and internal requirements in detail for developmental, implemental, and maintaining purposes (Walker & Cavanaugh, 1998).

For successfully developing and implementing security policies, upper management needs to be involved in the project and strongly support the project (Lam, 2005). A proposal with a report of external and internal requirements and a draft assessing budget can easily persuade managers to support the project of developing and implementing security projects. Having management support and authorization can resolve money and time issues. These managers can allocate the required budgetary needs and allow sufficient time for development and implementation. In addition, top managers have power to affect processes by enforcing employees to do participate (Kearns & Sabherwal, 2006).

Before beginning to develop security policies for the entire organization, developing teams should be very clear about what security policies organizations should have, and what the organization is going to protect. All requirements derived from laws, regulations, and business needs should

be gathered and translated into security policies. Risk analysis (Refer to the session 'Risk management and Analysis') for the entire organization should be complete because risk analysis can help developing teams understand the security status of an organization and prevent disasters from happening. Nevertheless, good security policies should balance between protection and productivity for an organization (Walker & Cavanaugh, 1998).

The foundation for developing and maintaining security policies is an important approach to analyze the current security state, the target security state and the gap, and also to identify CSF. Critical success factors, which result from assessing and analyzing risks, become drivers for securing organizations and their businesses. Therefore, these CSF should be transferred to security polices, and then drive through the detailed design of security controls at different architecture levels. Figure 17 illustrates the role of this phase in the business model of the Zachman EA framework.

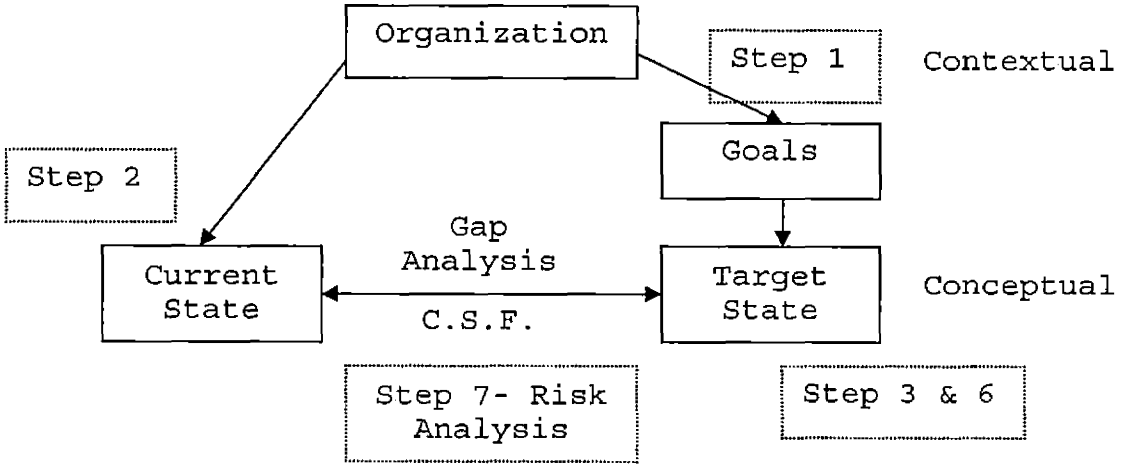


Figure 17. The Role of this Phase in the Business Model of Zachman EA Framework
Derived from (Carbone, 2004: Sherwood, 2005)

Develop Security Policies. Security policies are high-level statements that define an organizations high-level security philosophy. Security policies describe an organizations goals, missions, or objectives, and contain top manager's directives to create security programs, assign responsibilities, and to establish goals, measurement, and target (Hansche, Berti, & Hare, 2004). Security policies also can identify how organizations are compliant with legal systems, and how organizations are going to mitigate risks (Walker & Cavanaugh, 1998).

Types of Policies. Security policies can fall into three categories: regulatory, advisory, and informative (Harris, 2005). Regulatory types of security

policies derive from laws or regulation. Organizations 'must' comply with these requirements. Advisory types of security policies strongly suggest to employees what 'should' or 'should not' be done within an organization. It would be advisable to mention possible ramifications if employees do not comply with advisory types of security polices. Informative types of security policies, the final category, provide information to employees about certain topics. Informative types of security policies do not force employees to do something or not to do something. In other words, employees 'may/might' or 'may/might not' comply with informative security policies.

Policies, Standards, Guidelines, and Procedures. Developing security policy does not entail only developing policies. It also entails development of security standards, guidelines and procedures for supporting policies. Security policies are like strategic goals while standards, guidelines, and procedures are like tactical tools. Effective security policies frequently refer to standards and guidelines. Clearly distinguishing these terms and understanding what roles these terms play in developing security policies can help developing team members

communicate effectively, and make development and implementation successful.

Policies are brief statements, high-level security philosophy, and technology- and solution-independent (The SANS Institute, 2008). Standards are a collection of external, internal, system-specific, or procedural-specific requirements, and provide measurable information in each policy. Standards are mandatory so all employees must comply with these standards. Guidelines provide system specific or procedural specific recommendations. All employees are not required to comply with guidelines, but are strongly advised to comply with these guidelines for best practice. Procedures, the lowest level in the hierarchical structure of security policies, describe step-by-step tasks that should be performed to achieve goals. Procedures are closest to computers and users, comparing with policies, standards, and guidelines. For instance, procedures can contain detailed steps of configuration and installation. Figure 18 illustrates the hierarchical structure among policies, standards, guidelines, and procedures.

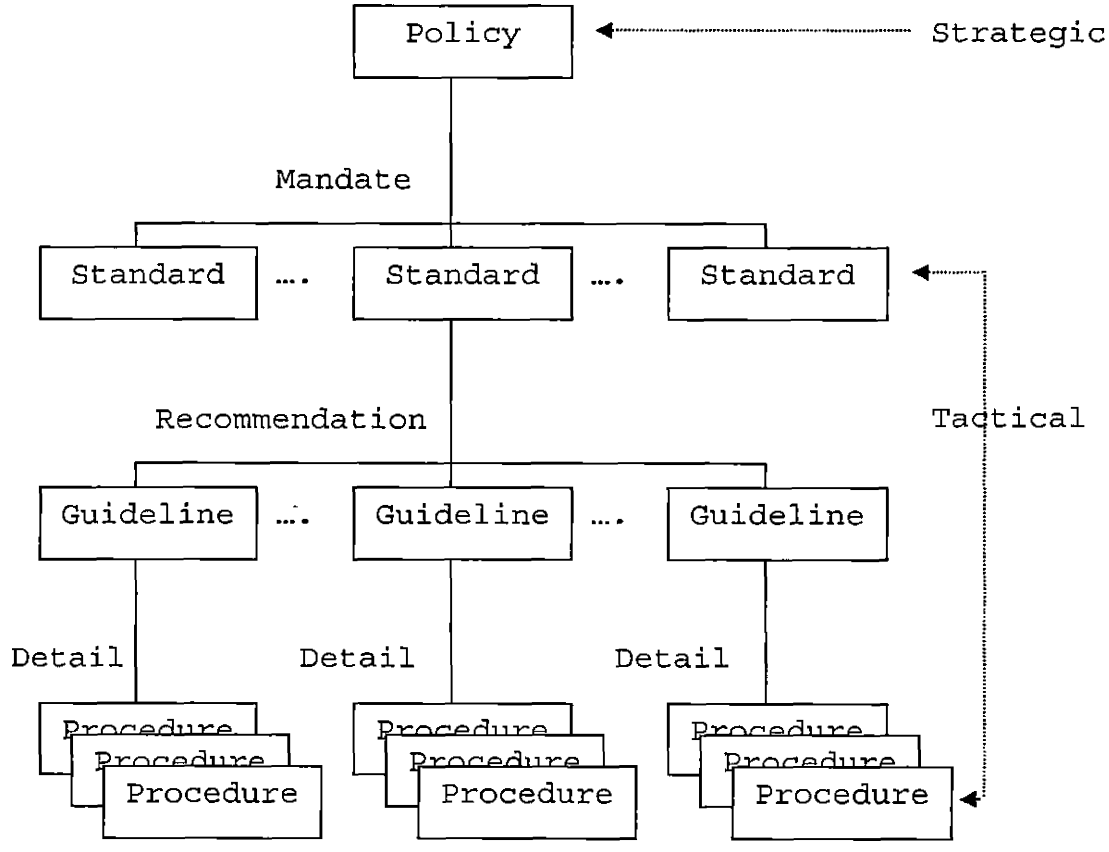


Figure 18. The Hierarchical Structure Derived from (Harris, 2005: Walker & Cavanaugh, 1998)

Steps of Developing Security Policies. Five essential steps of developing security policies are synthesized from research (Harris, 2005; Walker & Cavanaugh, 1998). These five steps are 'assign people who should be on the team', 'define security policy topics and assign responsibilities', 'define written components of security policies', 'develop policies, standards, guidelines, and

procedures', and 'review security policies for approval'. Figure 19 illustrates the flow of the development phase.

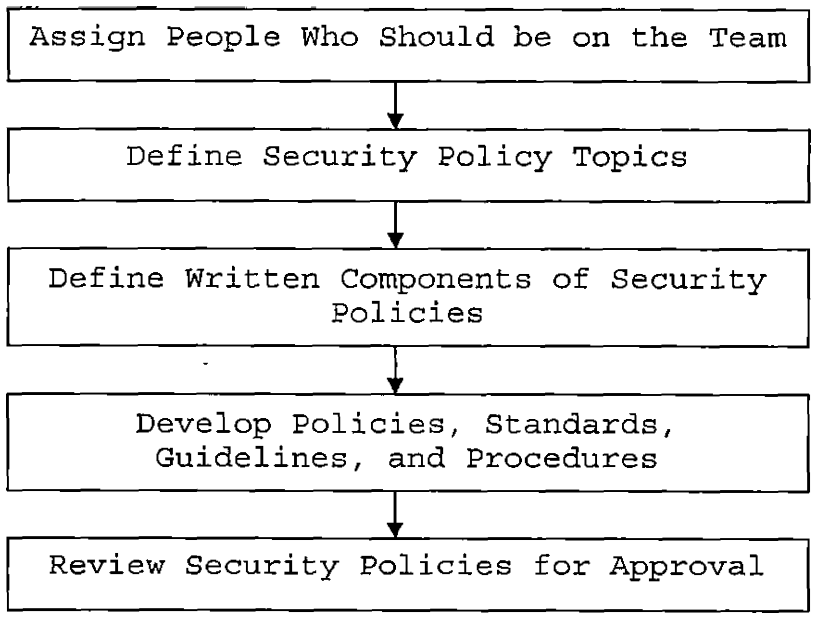


Figure 19. Develop Security Policies
Derived from (Harris, 2005; Walker & Cavanaugh, 1998)

Step 1: Assign People Who Should be on the Team for Developing Security Policies. After the preliminary phase, managers strongly support the project, and allocate budget and time. Organizational and business needs, legal requirements, and the result of risk analysis are gathered. The next step is to form a team to develop security policies. It is a good idea to have security professionals and technical personnel on the team. For best practice, having other specific professional people on the

team can avoid having blind spots. These specific professional people can come from a legal department, human resources department, audit and technical department, and so forth. Senior professional managers are the best candidates for developing security policies because security policies are high-level security philosophy, and contains managerial direction to create security programs, mitigate risks, assign responsibilities, and establish goals, measurement, and target (Hansche, Berti, & Hare, 2004). These specific senior professional managers involved in development can also make implementation efficiently and effectively. Reasons are that they know their professional fields well, they are very familiar with their departmental status and subordinates, and they have the power to influence subordinates to comply with security policies.

Step 2: Define Security Policy Topics and Assign Responsibilities. Developing teams can start to define the scope of the project and define security policy topics. After security policy topics are defined, based on their hard and soft skills, professional fields, and positions within the organization, all team members can be assigned roles and responsibilities for developing policies and implementation.

Step 3: Define Written Components of Security Policies. Defining written components of security policies can give all developing team members some ideas about how to write a security policy and what should be written for each security policy. There are six essential sections that are strongly advised to be written for each security policy: statement of purpose, scope, policy statement, enforcement, exceptions, and additional considerations (Walker & Cavanaugh, 1998). The statement of purpose simply describes the main purpose, such as the reason why the policy was developed and what is to be protected. The scope has to mention the policy's application, the technical platforms that the policy applies to, and an explanation of the types of information, definitions, and what is covered under the policy. The policy statement has to mention roles that are responsible for the policy, and their responsibility. This means that the policy statement should contain who is going to monitor for compliance to the security policy, and rules of implementation. Usually IS groups and internal audit groups are in charge of monitoring for compliance to the security policy. Enforcement sessions should describe who is responsible for enforcing the security policy. He/she

should be at a management level. An exceptions session is to include exception situations. The last session, additional considerations, can contain dates for developing policy or revising policy. It also can include names and departmental connection of those that develop policy.

Step 4: Develop Policies, Standards, Guidelines, and Procedures. For effectively and efficiently implementing and maintaining security policies, developing teams should follow the fundamental principles below for developing security policies.

Principle A - Simple Writing Format and Style. The security policy will be distributed within the entire organization. Readers could be technical personnel, or non-technical personnel who are in management positions (Walker & Cavanaugh, 1998). Therefore, easily understanding the security policy for all relevant people is the principle of producing the security policy.

Principle B - Policy Flexibility. Security policy should be flexible. Security policies usually remain applicable for some period of time until organizational business, operational objectives, or environments have a fundamental change (Hansche, Berti, &

Hare, 2004). Therefore, security policies should be hardware and software independent.

Principle C - Modulation - Efficiently Managing Security Policies. Developing teams can modularize the complete security policies by keeping standards, guidelines, and procedures separate and modular in nature (Harris, 2005). This method can make distribution and updating easier in the future. The section 'Standards' can be distributed to managers while the section 'guidelines' and the section 'procedures' can be distributed to IT administrators or operators.

Step 5: Review Security Policies for Approval. Once security policies have been developed, they need to be reviewed and used to collect feedback from technical employees, non-technical employees, and top managers (Walker & Cavanaugh, 1998). Communicating with users is an essential step to make sure that all parties are involved in developing security policies and have an opportunity to contribute their efforts. This process can ensure that the security policy is compliant with business needs, organizational policies, and legal requirements.

Communicate with Users. For effectively and efficiently implementing security policies, communicating

efficiently with users is an essential preliminary phase. Some security policies may affect internal cultures and employees daily operating behaviors, which is the hardest factor for teams to deal with. Efficient communication which requires employees to change cultures and existing daily operations in order to be compliant with security policies is necessary to achieve the desired end result. Effective communication plays an essential role in resolving these types of outcome issues. Effectively communicating with users can ensure that all understand security policies and accept to apply security policies. Teams also can record what those who were/are involved in developing security policies have read, understood, and agreed to obey in the security policies (Weise & Martin, 2001). Both effectively communicating with users and establishing a record can make implementation of security policies more efficient.

Implement Security Policies. Different organizations have different methods to implement security policies. Organizations vary in size, business type, needs, the policy itself, the technology used, finance, and so forth (Walker & Cavanaugh, 1998). These factors affect methods of implementing security policies. Below lists some of the

issues that implementing teams might face (Walker & Cavanaugh, 1998):

- Should security policies be implemented at once or by groups
- Should security policies be implemented as a whole or should they be based on priority to implement parts
- Should security policies be implemented by geographic area first or all at once if organizations are multi-national organizations

Implementation phase probably is the hardest phase in the life cycle of developing and maintaining security policies. Many organizations fail in this phase. For effectively and efficiently implementing security policies, teams need to resolve many issues. It could result from the lack of strong management support (Fedor et al., 2003; Lam, 2005), lack of budget (Kearns & Sabherwal, 2006; Martin, Pearson, & Furumo, 2007), lack of implementation time (Walker & Cavanaugh, 1998), lack of strong leadership (Fedor et al., 2003), lack of awareness of benefits of implementing security policies-"why for" (Hansche, Berti, & Hare, 2004), or ineffective communication with users

(Jackson, Chow, & Leitch, 1997; Walker & Cavanaugh, 1998). Resolving all of the above issues can help to successfully implement security policies.

Define Incident Response and Manage Incidents. Defining incident response and managing incidents can minimize the impact that incidents may cause. Good incident management can also make teams more aware of security weakness from these incidents occurring, and then establish solutions for preventing it from occurring next time. Therefore, it would be good practice for organizations. In this phase, there are three steps: define incident response, manage incidents, and review and update security policy (See Figure 20). Managing incidents includes three sub-steps: quickly response incidents, effectively handle incidents, and clearly document incidents (See Figure 20).

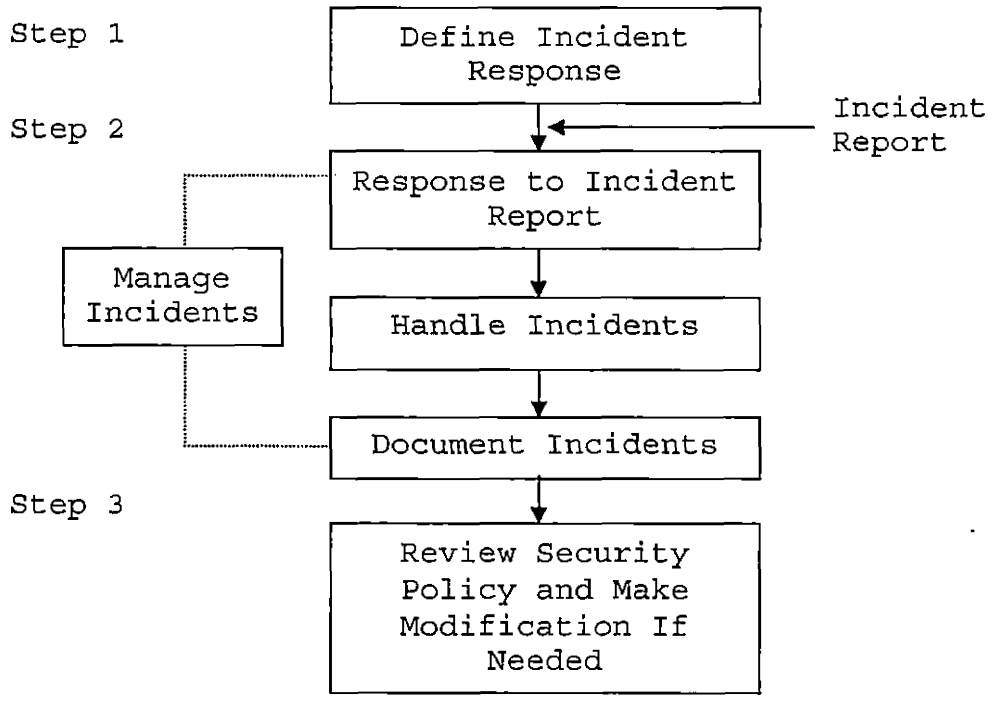


Figure 20. The Flow of Defining Incident Response and Managing Incident
Derived from (Harris, 2005; Walker & Cavanaugh, 1998)

Step 1: Define Incident Response. Planning incident response before actual incidents occur is necessary. One of the advantages of planning ahead is that key employees can have a clear picture about what kinds of incidents may occur, and how to react to different incidents appropriately (Harris, 2005). The other advantage is that these key employees can be trained with the necessary skills to appropriately react to different

categories of incidents before actual incidents occur (Walker & Cavanaugh, 1998).

Defining incident response should focus on developing reacting scenarios for each incident, based on the kind of violating security policy (Walker & Cavanaugh, 1998). These scenarios should be clearly defined in detail.

Most security incidents will fall into the five categories below (Hansche, Berti, & Hare, 2004):

- Attack type: terrorist attack, hacker attack, virus attack, malicious code attack, and insider attack
- Unethical type: competitive intelligence gathering
- Unauthorized type: employee unauthorized action
- Misbehavior type: employee error
- Hardware and software malfunction type

Step 2: Manage Incidents. There are three major tasks for incident management: response incidents to incident report, handle incidents, and document incidents. When incidents occur, employees should follow the defined procedures at the previous step for responding to incidents. Auditing trials may be needed for investigation. Teams can

use forensic techniques, which is like a tool to assist with computer security incident response, to collect, examine, analyze, and report incidents (Kent, Chevalier, Grance, & Dang, 2006). The purpose of investigation is to determine how and why the incident occurred, which can help teams apply appropriate correction approaches. After incidents have occurred and have been handled, teams should discuss and document these actual incidents, and then distribute these documentations to key employees. The focus of discussion and documentation should be on the description of incidents, causes (e.g. security weaknesses, missing steps, not follow processes, or procedural problems), how to discover incidents, procedures of how to fix these problems that caused incidents, monitor procedures, summarization of what was learned, and recommendation for updating the security policy (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003).

Step 3: Review Security Policy and Make Modification If Needed. Reviewing and updating security policy each time when organizations are hit by incident. Identifying the causing reason first can help teams to know which policies should be reviewed carefully and make modification. This step is like a prevention step, which

can prevent organizations from being hit again by the same incident.

Audit for Compliance to Security Policies. It is always a great practice to monitor for compliance to security policies (Walker & Cavanaugh, 1998). Auditing for compliance can allow for a certain degree of control to security. Usually, this action can be taken by information security officers, internal audit groups, external auditors, consultants, or the U.S. state auditors if organizations are in regulated industries.

Regularly Review and Update Security Policies. Security policies should be reviewed regularly and updated if needed (Weise & Martin, 2001). Regularly reviewing and updating process can translate essential changes within organizations into security policies, which can ensure that security policies will not become obsolete in the future. For effectively implementing updated security policies, regularly reviewing and updating processes, personnel involved, and those who must sign-off on the changes should be clearly indicated and understood.

Why Always Fail in "Why For" Developing Security Policies

Many security police developers know "how-to" develop security policies, but always fail in "why for" (Hansche, Berti, & Hare, 2004). There are few reasons for this situation. First of all, top managers do not offer strong support to develop and implement security policy. That means that top managers think that security policies are just statements and are not worthy of spending too much time and money for developing and implementing this security project. The result is that top managers or decision makers do not allocate enough budget and time towards developing and implementing teams. Second, the leader and team members of developing and implementing teams do not believe that this security project is worthy of completion. Hence, they are just doing the minimum work that is required to do, such as documenting security policies only. Third, the top team leader's leadership is not strong enough to successfully develop and implement security policies within the entire organizations (Fedor, et al., 2003).

Some actions can be taken to prevent this situation from happening. Emphasizing legal requirements, risks that

organizations have, and cost that organizations may be incur if risks have not been addressed is a useful action. Educating or training top managers or decision makers to strongly believe in the usefulness that security policies have in an organization is also a good idea, but may be harder to do. The leader and team members who are in charge of the security policies project should have a strong sense of security, and the leader should be carefully chosen. Chosen criteria should not only be based on hard-skills, but also base on soft-skills. Strong soft-skills can save a lot of effort for making a security policies project successful.

The Role of Security Framework In Zachman EA Framework

The Zachman EA framework is one of top-down approaches. Developing and maintaining security policy is also one of top-down approaches. Figure 21 illustrate the role of security framework in Zachman EA framework.

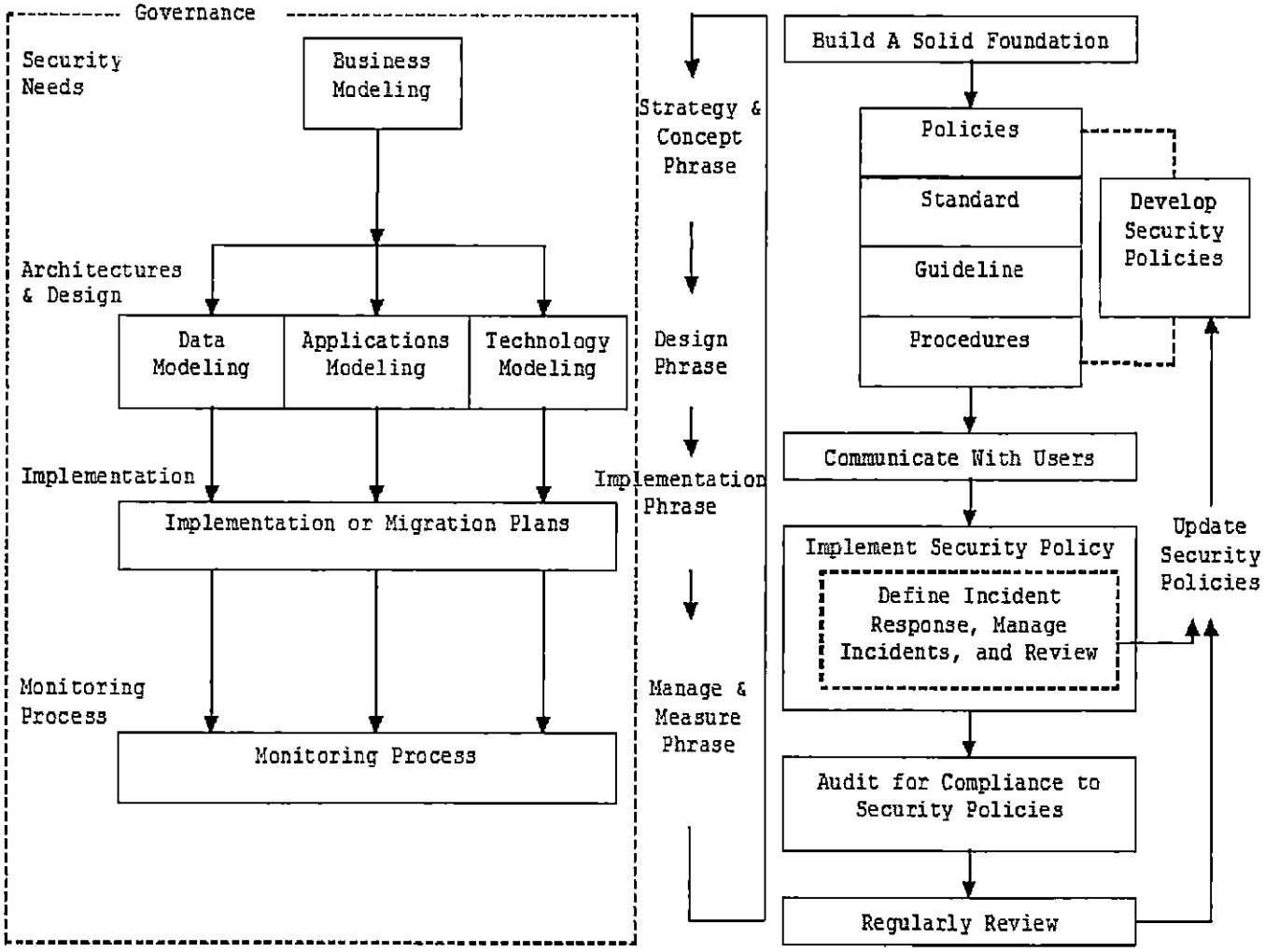


Figure 21. The Life Cycle of the Zachman EA Framework and Security Framework Derived from (Sherwood, 2005; Spewak, 1993; Walker & Cavanaugh, 1998)

CHAPTER FIVE

ANALYSIS

Chapter five and six discuss the gap analysis of the L system in access control, information security incident management, and business continuity management (BCM) for one chosen organization, and suggest a best practice model of developing security policy, access control and information security incident management modeled ProVison (Metastorm, 2008). Recently, the organization set a security goal for being compliant with security standard, ISO 17799 2005. To effectively achieve the main goal eventually, developers not only need to have a well developed plan that aligns IT security with business security needs, but also need to identify what critical tasks are and what should be worked on first. Applying the framework developed in the research, performing gap analysis can help developers easily identify CSF. This chapter summarizes the result of analyzing the gap.

The scope of the case is the L system, concentrating on analyzing access control, information security incident

management, and BCM. The target of this case is compliant these three aspects with ISO security standard.

The first step is the assessment of the current state. Conducting questionnaires of access control, information security incident management, and BCM, based on business model of the organization. Interviewing with IT personnel is necessary to gather needed data in this study. The topics of questionnaires are presented in Table 1, 2, and 3.

The gap analysis is performed based on the data collected.

The result of performing gap analysis will be presented by graphic charts only. In fact, these graphic charts also can illustrate how easily weakness, strength, and CSF can be identified for planning further potential / candidate projects.

In figure 22, 23, and 24, X axis represents control areas for access control, information security incident management, and business continuity management. The number represents different control areas. Table 1, 2, and 3 depict these control areas. Y axis represents what percentage of compliance with ISO 17799 2005. The number '0' represents nothing has been done at all while the number '100' represents full compliance with ISO security

standard. If percentage of compliance is lower than 50, that means those control areas should be paid attend immediately. All percentage of compliance is presented in table 1, 2, 3 as well.

CHAPTER SIX

RESULTS AND IMPLICATION

According to the figures (22, 23, and 24) shown below, access control has a lot of rooms for improvement while information security incident response and business continuity management have been controlled well. Figure 22 shows that many control areas have not been done well yet. Some control areas even have not been taken any action at all although few control areas have been full compliant with ISO 17799 2005. Low percentage of compliance with ISO security standard means that there is high likelihood that threats will occur. Based on the result, it is so easy to pinpoint out which areas will become apparently vulnerable and should be taken immediately action, such as control area #5 and #10 in figure 22, which have zero percentage of compliance. Good news for this organization by observing the result shown in Figure 22 is that three control areas (#7, #10, #20) have one hundred percentage of compliance with ISO standard.

Table 1. Access Control

Control Area	Access Control	Percentage of Compliance
1	Access Control Policy	33.33
2	User Registration	34.78
3	Privilege Management	16.67
4	User password management	66.67
5	Review of user access rights	0
6	Password Use	66.67
7	Unattended user equipment	100
8	Policy on use of network services	60
9	User Authentication for external connection	50
10	Equipment identification in networks	0
11	Remote diagnostic Port protection	66.67
12	Segregation in network	100
13	Network Routing Control	66.67
14	Secure log-on procedures	50
15	User identification and authentication	83.33
16	Use of systems utilities	68.75
17	Session time-out	83.33
18	Limitation of connection time	50
19	Information access restriction	83.33
20	Sensitive system isolation	100
21	Teleworking	76.32

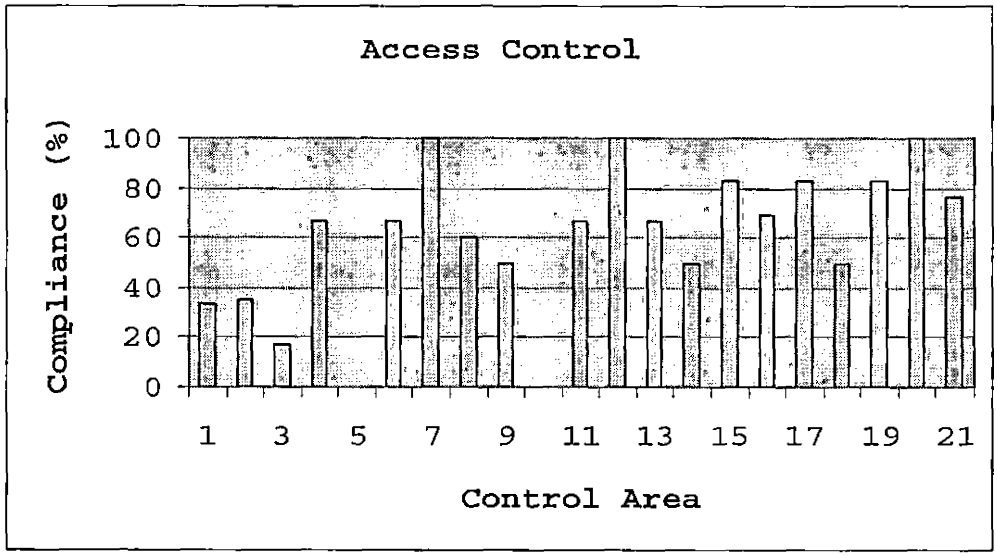


Figure 22. Access Control

Figure 23, information security incident management, has been controlled well. All five control areas have more than fifty percentage of compliance with ISO 17799 2005. Three out of five have one hundred percentage of compliance with the industry security standard. This shows that the organization can quickly response to some expected or unexpected events and effectively take right actions for these events.

Table 2. Information Security Incident Management

Control Area	Information Security Incident Management	Percentage of Compliance
1	Reporting information security events	66.67
2	Reporting security weaknesses	100
3	Responsibilities and procedures	68.75
4	Learning from information security incidents	100
5	Collection of evidence	100

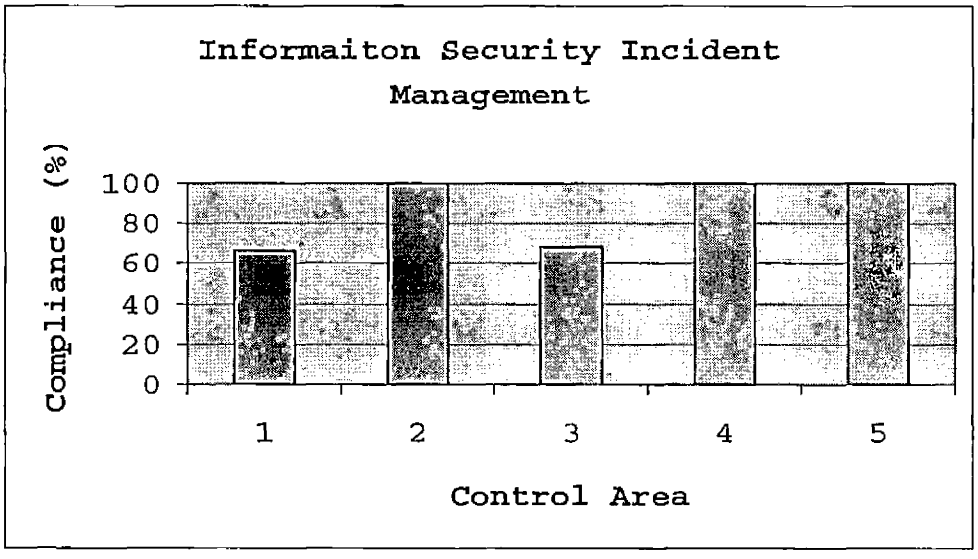


Figure 23. Information Security Incident Management

Figure 24, the last figure, also can demonstrate that BCM have been well controlled, except control area #5. Control area #5 is 'testing, maintaining and re-assessing business continuity', which only has 37.5% of compliance. That means that a well developed BCM plan does not have much opportunity to examine whether the BCM plan is

appropriate and applicable for quickly reaction to severe events and reduction impact of cost to less. Low percentage of compliance also means that the well developed BCM plan may not work as expected in the real world. Despite the control area #5, the organization has more than 85% of compliance in business continuity management, which indicates that the organization may be able to quickly get business back in normal after getting hit.

Table 3. Business Continuity Management

Control Area	Business Continuity Management	Percentage of Compliance
1	Including information security in the business continuity management process	100
2	Business continuity and risk assessment	100
3	Developing and implementing continuity plans including information security	88.89
4	Business Continuity planning framework	97.3
5	Testing, maintaining and re-assessing business continuity	37.5

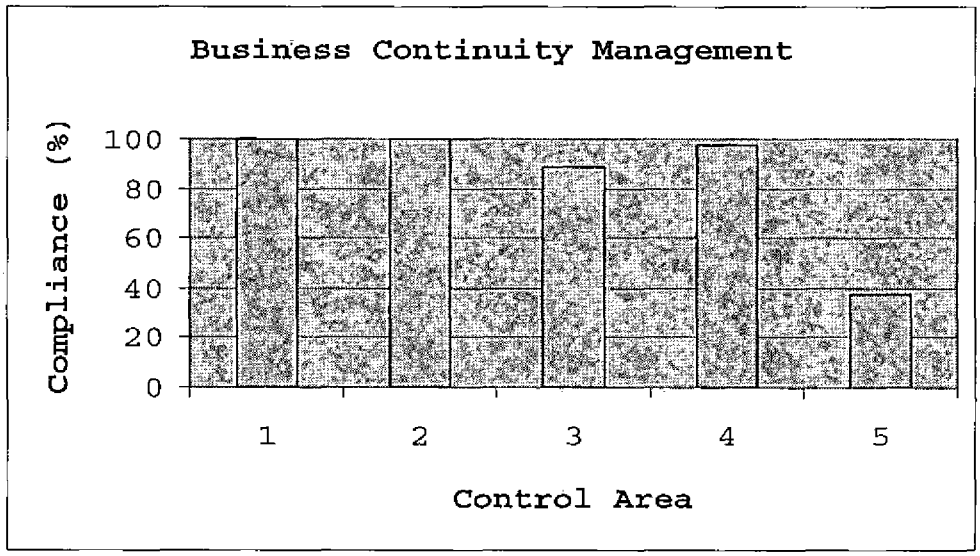


Figure 24. Business Continuity Management

The next step of this study is to develop a best practice framework, which is modeled using ProVision, for the organization. Before starting to demonstrate the best practice models, the overall business framework and L system is presented from Appendix A to J.

Due to data restriction, only information security incident management will be addressed at this point. From the table and bar chart (See Table 2 and Figure 23), 'reporting information security events' and 'responsibilities and procedures' only have about 66% to 69% of compliance with security ISO standard. The main reason of the low percentage of compliance for the former case is the lack of formal security incident response

policy, which describes how to report events. The organization only has security standard and process of security incident response. The recommendation here is to develop a formal and written security incident response policy. Appendix K, L, and M illustrate the best practice security framework first, followed by illustrating the best practice of developing security policy and the flow of effectively implementing one security policy. Following these strategies, the organization is able to develop useful security incident management policy.

For the latter one "responsibilities and procedures", the main reason of low percentage is lack of well documented guidelines for the complete cycle of responding and handling incidents. Well written guidelines can easily identify responsibilities of each role of responding and handling incidents, and provide clear guidelines of managing incidents. Appendix N, O, and P illustrate the best practice strategy for security incident response policy, followed by presenting the main scope of incident response policy in L system, and then the best practice workflow. The workflow demonstrates the complete cycle of managing security incident. One of essential steps for improvement is to follow written guidelines of responding

incidents for ensuring a quick, effective, and orderly response to information security incidents. In addition, determining and implementing countermeasures are recommended for preventing the same incident from happening again (Harris, 2005; Walker & Cavanaugh, 1998). After this step, all information relevant to incidents should be documented, including what the incident is about, what the impact the incident makes, how to handle it in what method, how to prevent it happened again, and so on. The last step should also review the security policy and make modification if needed. This complete cycle not only can well handle security incident correctly and efficiently, but also can ensure the same incident will not happen again in the future.

CHAPTER SEVEN

CONCLUSION

Security is important for all organizations, especially for large enterprises. Inappropriate security management can make critical events threaten organizations' bottom line, such as loss of reputation, customers' trust, fortune, confidential information, and so on. Incorporating security dimension into Zachman EA framework is a good practice for securing organizations efficiently and effectively. Zachman EA framework is a blueprint for the entire organizations. It allows developing teams, such as EA teams, to well align business and IT security, and transform business needs into IT security business value. Well developing plan can positively affect the quality of implementation and have less unexpected implementing errors. Strong top management support and applying top-down governance can make development and implementation successful to deliver value for organizations. Strong top management supports not only means "approval" for allocating enough time and budget, but also involve getting top managers to participate for successful development and

implementation. The reason is that these top managers have power to enforce different departments on cooperation, and eventually make the entire project successful. Applying top-down governance not only can efficiently develop settings and plans, but also can ensure organizations conform to well-developing plans. Top-down governance can efficiently control and monitor the state of enterprise security by looking all as one. All considerations will also be consistent within the entire enterprise. Top-down governance also can make communication easily because, general speaking, there are just two ways of communications: up-to-down or down-to-up communication.

The paper starts from presenting an effective governance approach, followed by presenting the framework from two perspectives. One is from EA perspective while the other is from security perspective. The first section is very useful for EA personnel to look at security dimension. The second section can help security personnel to see the whole picture of enterprise security easily, and how to fit into the Zachman EA framework.

In addition, this paper not only presents framework itself, but also illustrates developing processes of the

framework. This can provide developing teams as a standard or guideline for developing enterprise plan.

Applying the framework developed here can easily pinpoint security strengths and weaknesses of organizations, effectively develop the most appropriate security blueprint, and efficiently implement cost-effective security projects for enhancing security regularly. These benefits of applying the enterprise security framework is demonstrated in chapter five and six. In these two chapters, one organization has been applied using the framework developed in this research. Analyzing business framework and gap has been done by conducting questionnaires and interviews, and applying one step of risk assessment and analysis-assess vulnerabilities. Gap analysis can help developers easily identify CSF for achieving the target by prioritizing factors. At the last section of chapter six, a best practice model is suggested. These models are developed using ProVision.

APPENDIX A

THE BUSINESS FRAMEWORK INTERVIEW OUTLINES (Carbone, 2004)

KEY

Group 1 = Officers/Key Business Experts, CIO

Group 2 = Key Opinion Leaders (Business, IT)

Group 3 = Key IT Leaders

Group 1 Questions

As an officer of (organization):

1. What is (organization) vision/mission?
2. What is CIO vision/mission?
3. What are (organization)/CIO goals/objectives?
4. What are this year's key business initiatives/major programs?
5. Identify longer-term stress points or risks in the IT organization (major concerns).
6. Identify the strengths and weaknesses of the (organization) business (e.g., skill deficit, low turnover). These are characteristics for which the organization is known.
7. List the major current (short-term) challenges the organization faces.
8. List the major environmental changes (organization) IT faces, (e.g., new technology)

9. What are potential growth/expense reduction opportunities to which (organization) IT could contribute?
10. Describe significant "history" or changes in business direction (e.g., e-business, mergers and acquisitions, consolidations, deregulation, new ventures, new technology).
11. Describe the (organization) "culture" and identify the major themes or motivational forces that impact the behavior of the organization.
12. Identify key constraints (e.g., regulatory, legislative, shareholder considerations)

How would the business behave if:

- Stress points were relaxed/risks mitigated?
- Weaknesses were addressed and strengths fortified?
- Challenges were resolved?
- Environmental changes were accounted for?
- Growth/expense reduction opportunities were leveraged?
- The "world was perfect?"

Group 2 Questions

As a key opinion leader:

1. Identify longer-term stress points or risks in the IT organization (major concerns).
2. Identify the strengths and weaknesses of the (organization) IT business (e.g., skill deficit, low turnover). These are characteristics for which the organization is known.
3. List the major current (short-term) challenges (organization) IT faces. You can often tell a challenge by the fact that several different groups are working to address it.
4. List the major environmental changes (organization) IT faces (e.g., new technology).
5. What are potential growth/expense reduction opportunities to which (organization) IT could contribute? You can sometimes recognize a potential growth opportunity by the fact that a new idea or "buzzword" has cropped up and everyone wants to be associated with it.
6. Identify organization size in annual expenses and number of employees by organization (e.g., Marketing, IT).

7. List number and types of customers.
8. List users/customers of IT
9. List locations served and serving.
10. List key products and services.
11. List high-level organization structure and process flow.
12. Show organization structure for IT
13. Show processes/flow used for CIO
14. List sales channels (website, call centers, etc.)
15. List key partners/suppliers/vendors.
16. List key reports or indices.

How would the organization/IT behave if:

- Stress points were relaxed/risks mitigated?
- Weaknesses were addressed and strengths fortified?
- Challenges were resolved?
- Environmental changes were accounted for?
- Growth/expense reduction opportunities were leveraged?
- The "world was perfect?"

In the "ideal" future:

1. How will customers and suppliers interact with us (e.g., "suppliers will accept our orders electronically.")?
2. What will the future high-level business function flow look like?
3. What key business information will flow through the process?
4. What critical people plans and skills will be in place (e.g., "There is a single, cross-trained IT organization.")? What critical support processes and structures will be in place (e.g., "The new skills assessment process is used by all managers.")?
5. What key enabling capabilities will enable the desired state (e.g., "We have the capability for a customer with a service problem to reach a live agent from the web site.")

Group 3 Questions

As an IT leader/manager, please describe:

1. Number and types of customers
2. Users/customers of IT services
3. Locations served and serving
4. Data center/storage/distribution locations

5. Network and user locations

6. High-level organization structure and process flow

7. Organization structure for IT

8. Processes/flow used for IT

9. Key suppliers/vendors

10. Key reports or indices

11. Indices/measures for IT

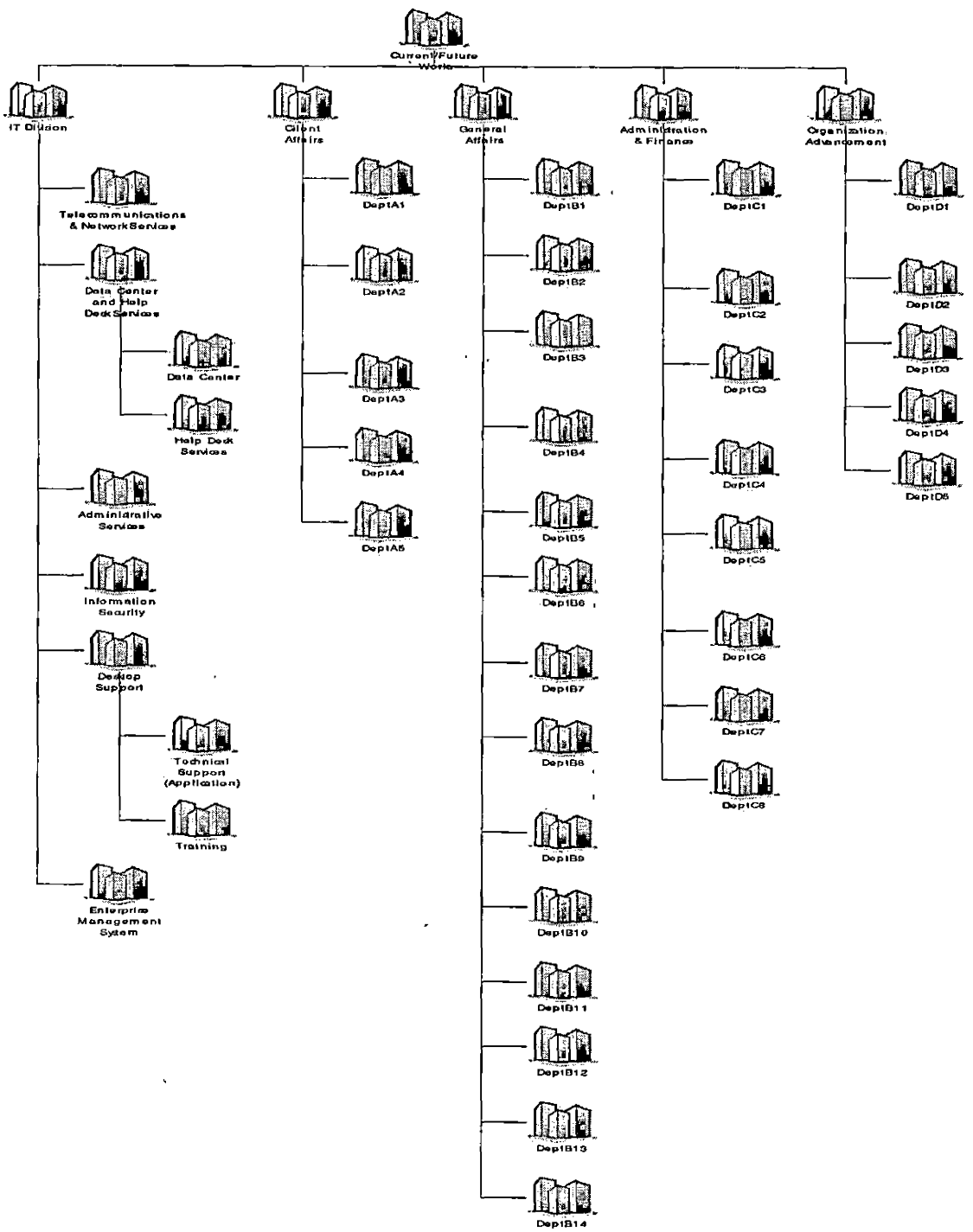
12 Current technologies:

- Network, severs, and operating systems
- Communications services - pair-wise interfaces, APIs, messaging, etc.
- Development/analysis tools
- External interfaces (e.g., external systems & databases)
- Data management software- extraction/cleansing/mapping, DW/DBMS, repository, modeling, etc.

13. Major applications (CRUD) and databases

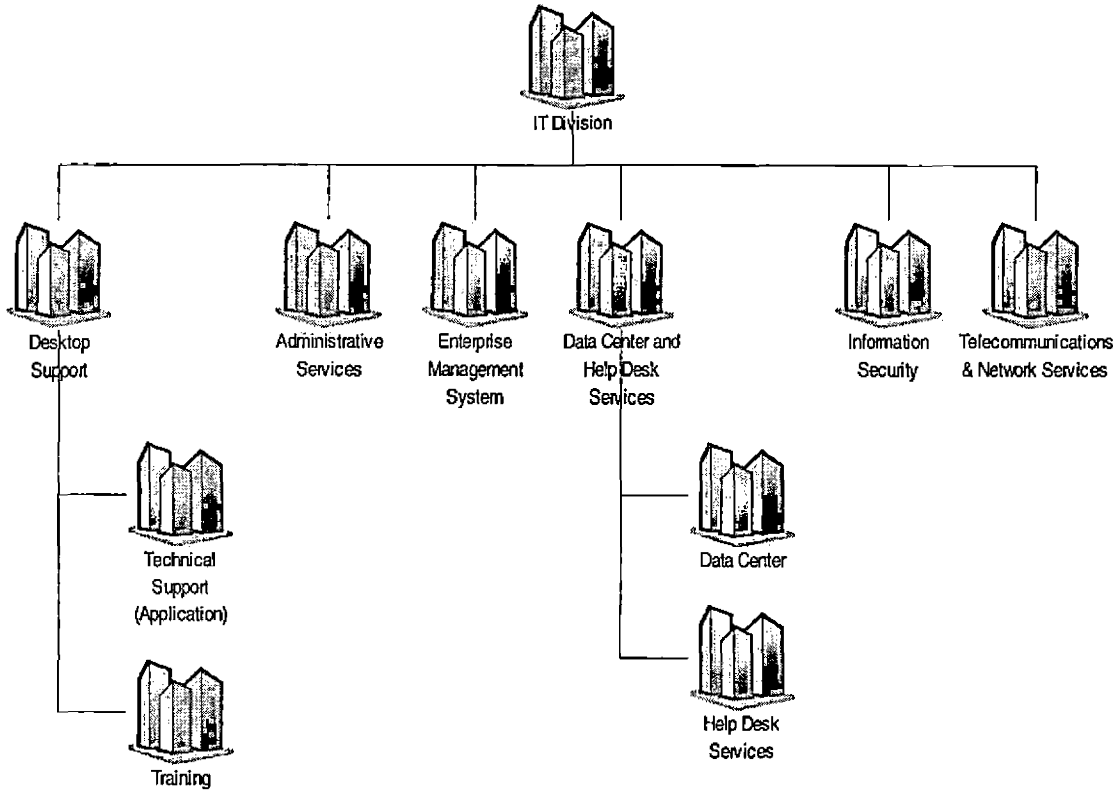
APPENDIX B

ORGANIZATION CHART


Current/Future World
IT Division
Client Affairs
General Affairs
Administration & Finance
Organization Advancement
Telecommunications & Network Services
Data Center and Help Desk Services
Data Center
Help Desk Services
Administrative Services
Information Security
Desktop Support
Technical Support (Application)
Training
Enterprise Management System
DeptA1
DeptA2
DeptA3
DeptA4
DeptA5
DeptB1
DeptB2
DeptB3
DeptB4
DeptB5
DeptB6
DeptB7
DeptB8
DeptB9
DeptB10
DeptB11
DeptB12
DeptB13
DeptB14
DeptC1
DeptC2
DeptC3
DeptC4
DeptC5
DeptC6
DeptC7
DeptC8
DeptD1
DeptD2
DeptD3
DeptD4
DeptD5

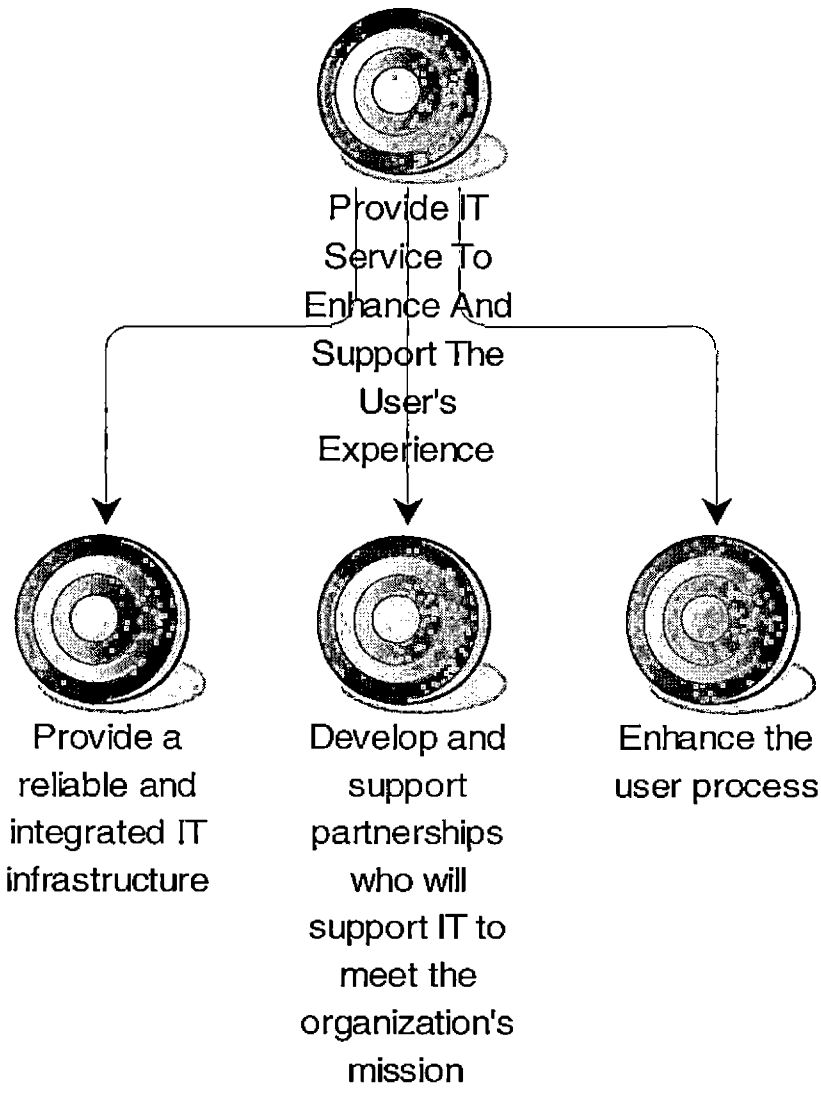
APPENDIX C

STRUCTURE OF INFORMATION TECHNOLOGY DEPARTMENTS


IT Division
Desktop Support
Administrative Services
Enterprise Management System
Data Center and Help Desk Services
Information Security
Telecommunications & Network Services
Technical Support (Application)
Training
Data Center
Help Desk Services

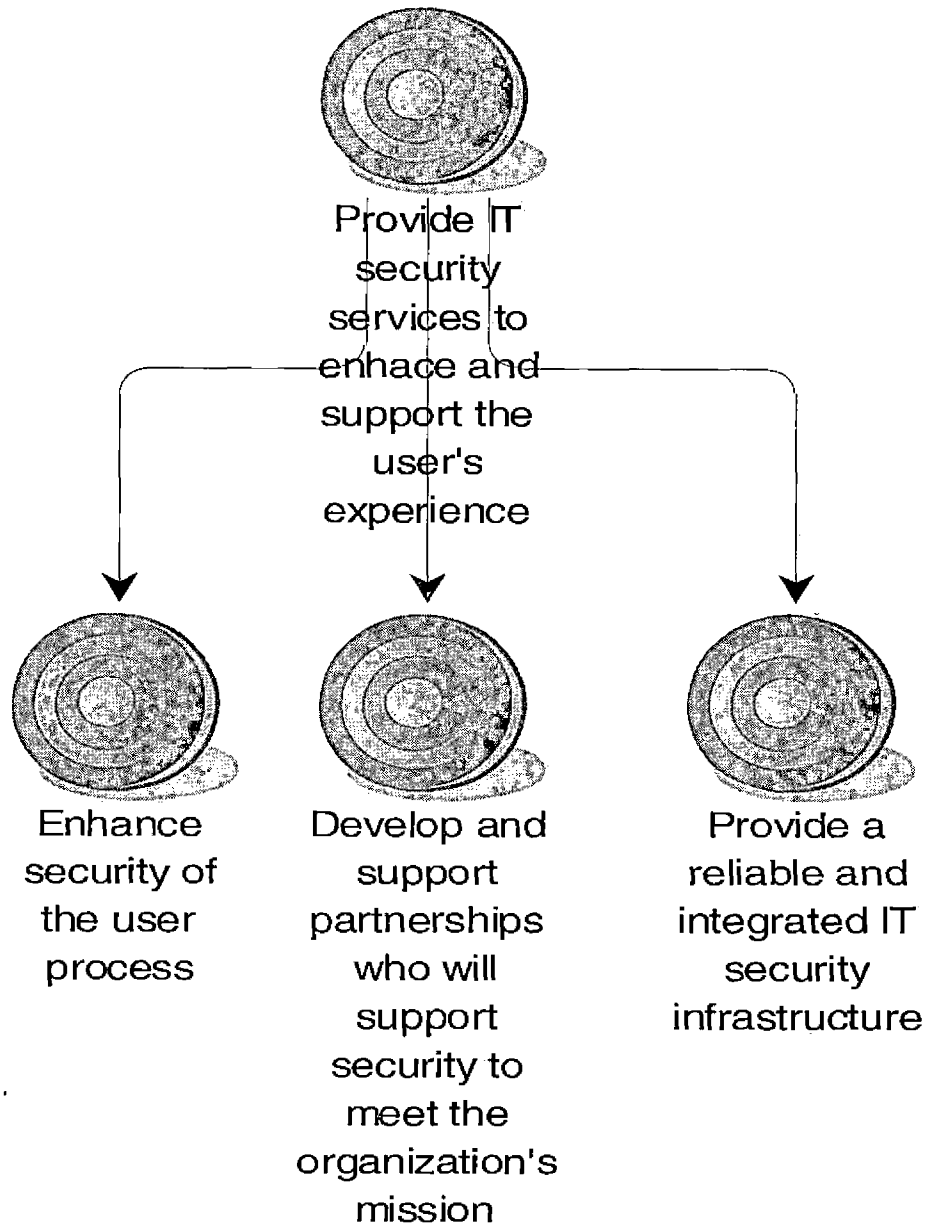
APPENDIX D

INFORMATION TECHNOLOGY STRATEGY


Provide IT Service To Enhance And Support The User's Experience
Provide a reliable and integrated IT infrastructure
Develop and support partnerships who will support IT to meet the organization's mission
Enhance the user process

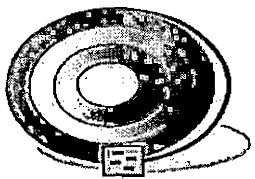
APPENDIX E

STRATEGY FOR INFORMATION TECHNOLOGY SECURITY

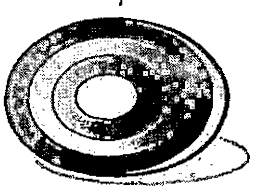

Provide IT security services to enhace and support the user's experience
Enhance security of the user process
Develop and support partnerships who will support security to meet the organization's mission
Provide a reliable and integrated IT security infrastructure

APPENDIX F

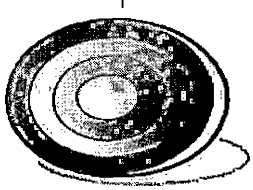
GOALS OF INFORMATION TECHNOLOGY



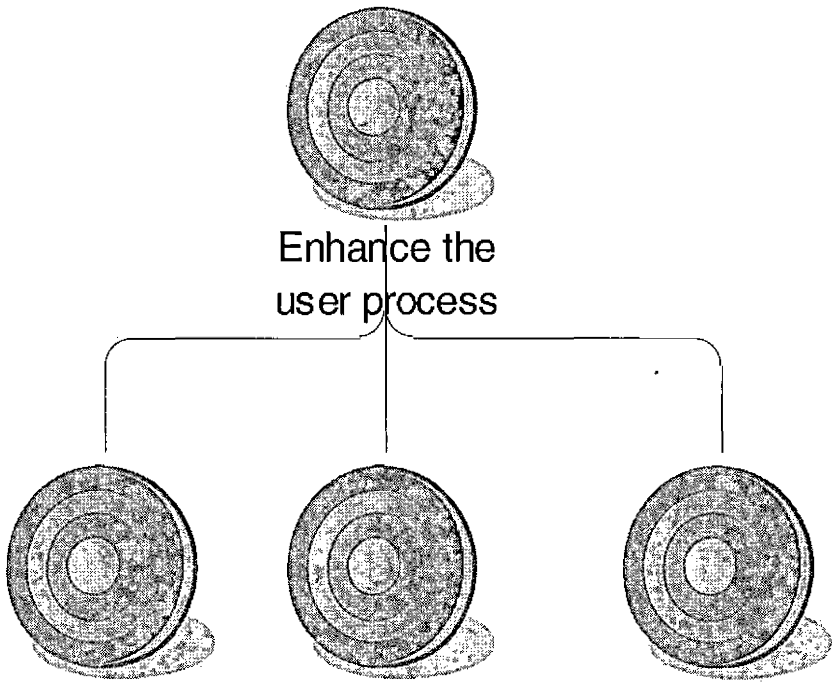
Develop and support partnerships who will support IT to meet the organization's mission

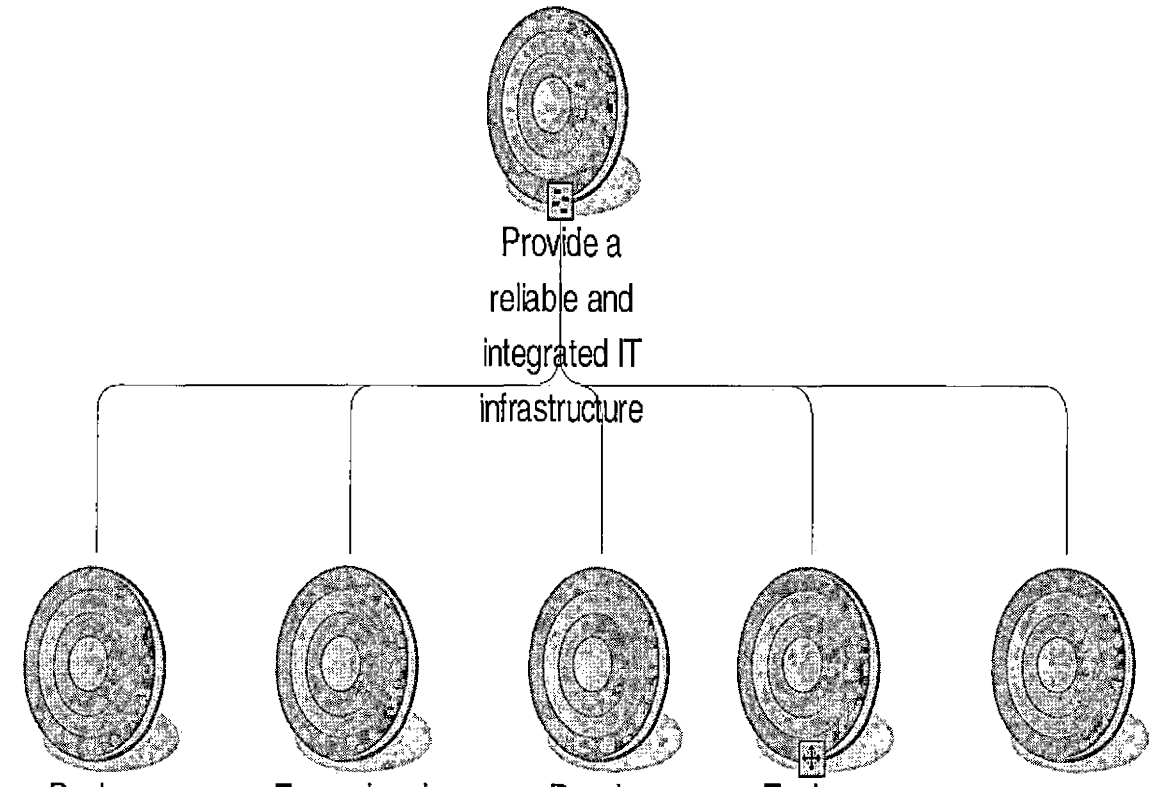


Maintain current partnerships, and develop new partnerships for meeting the goals and objectives of IT and the organizaiton



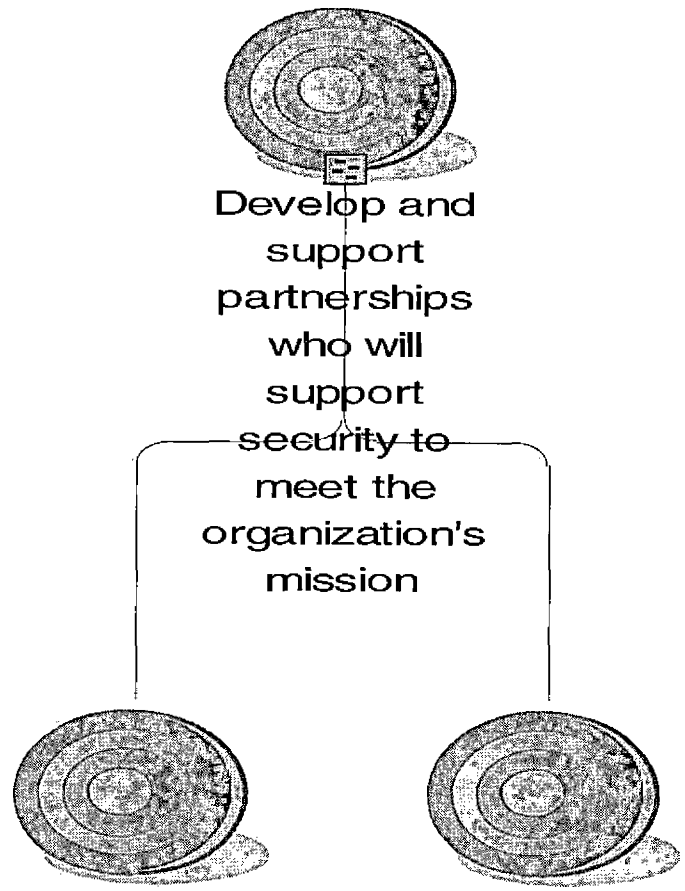
Market IT to the organizations

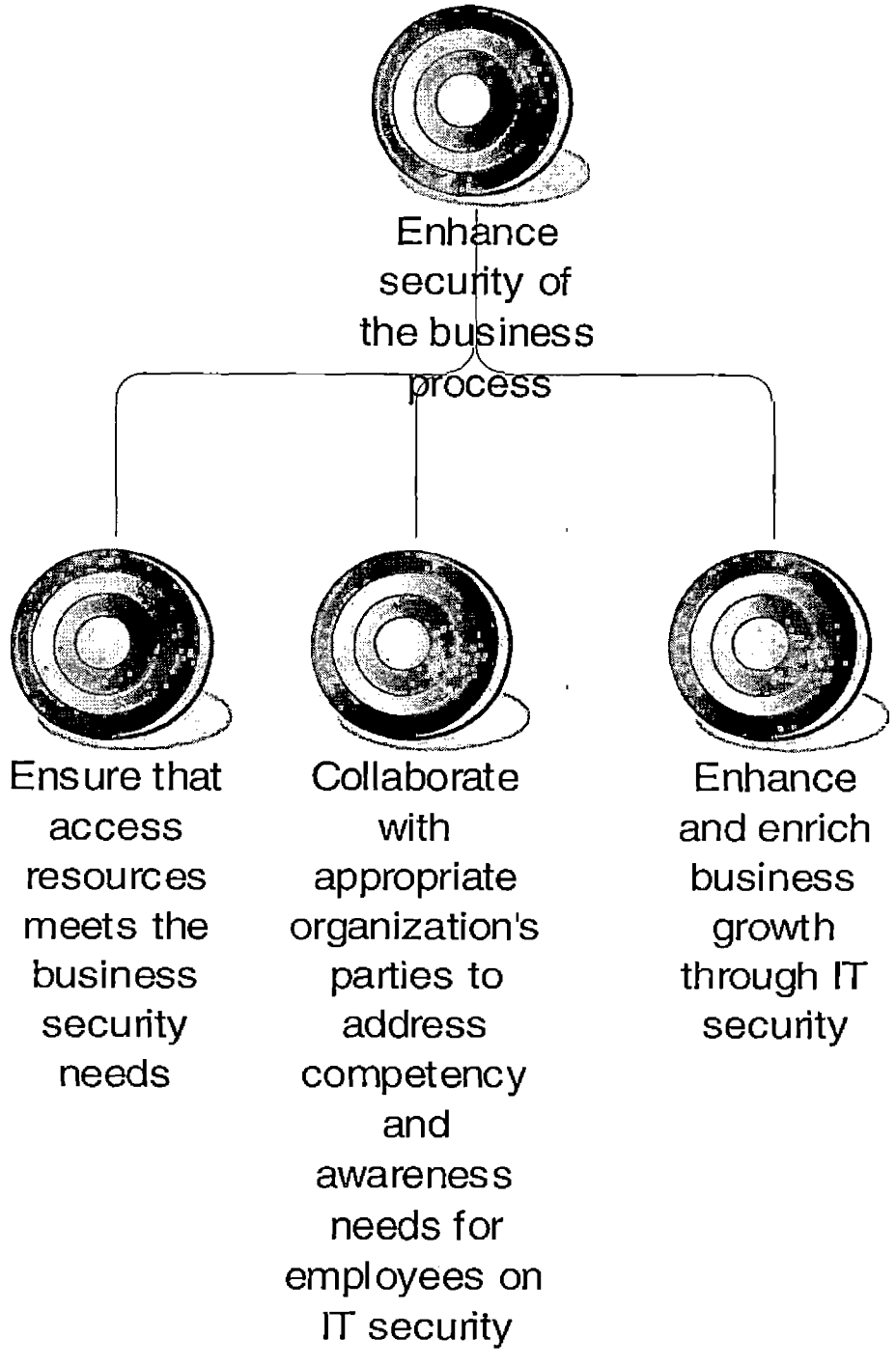

Enhance the user process
Ensure that access resources meets the business needs
Collaborate with appropriate organization's parties to address competency and awareness needs for employees on IT
Enhance and enrich business growth through IT

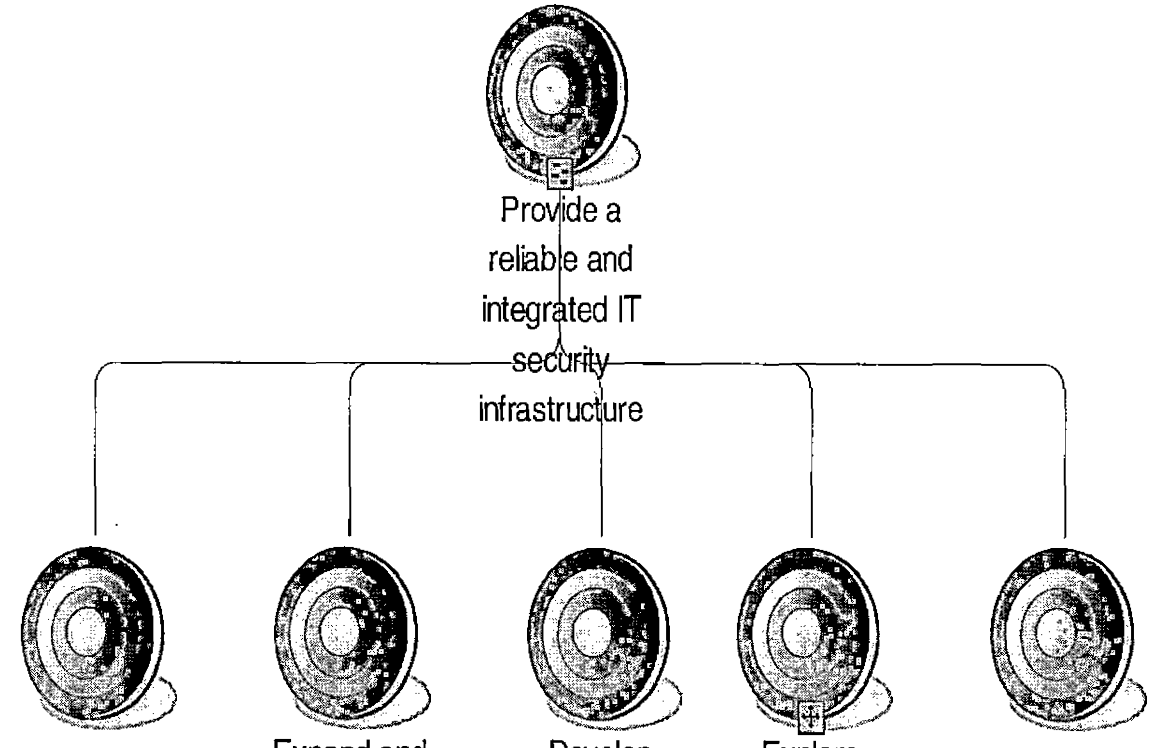

Provide a reliable and integrated IT infrastructure
Design, implement, and maintain a IT infrastructure to ensure reliable, 24*7 access to information
Expand and improve IT services to meet stated goals and objectives
Develop plans and policies that can effectively implement needed IT projects
Explore revenue enhancements and cost sharing alternatives to meet user demands
Develop a plan to safeguard assets and IT infrastructures

APPENDIX G

GOALS FOR INFORMATION TECHNOLOGY SECURITY

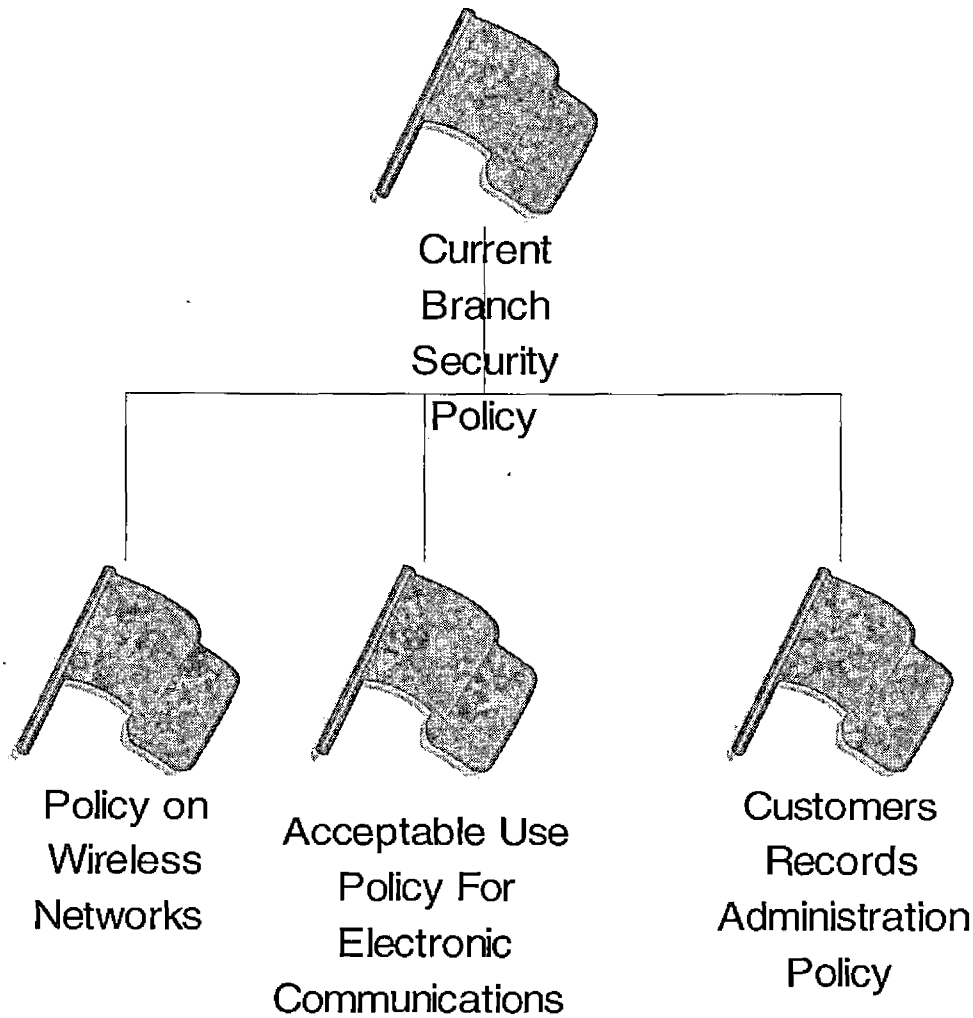

Develop and support partnerships who will support security to meet the organization's mission
Maintain current partnerships, and develop new partnerships for meeting the goals and objectives of IT security and the organizaiton
Market IT security to the organizations


Enhance security of the business process
Ensure that access resources meets the business security needs
Collaborate with appropriate organization's parties to address competency and awareness needs for employees on IT security
Enhance and enrich business growth through IT security


Provide a reliable and integrated IT security infrastructure
Design, implement, and maintain a IT security infrastructure to accomplish three fundamantal principles of security: availability, integrity and confidentiality
Expand and improve IT security services to meet stated goals and objectives
Develop plans and policies that can effectively implement needed IT security projects
Explore revenue enhancements and cost sharing alternatives to meet user demands
Develop a plan to safeguard the entire organization, including assets and IT infrastructures

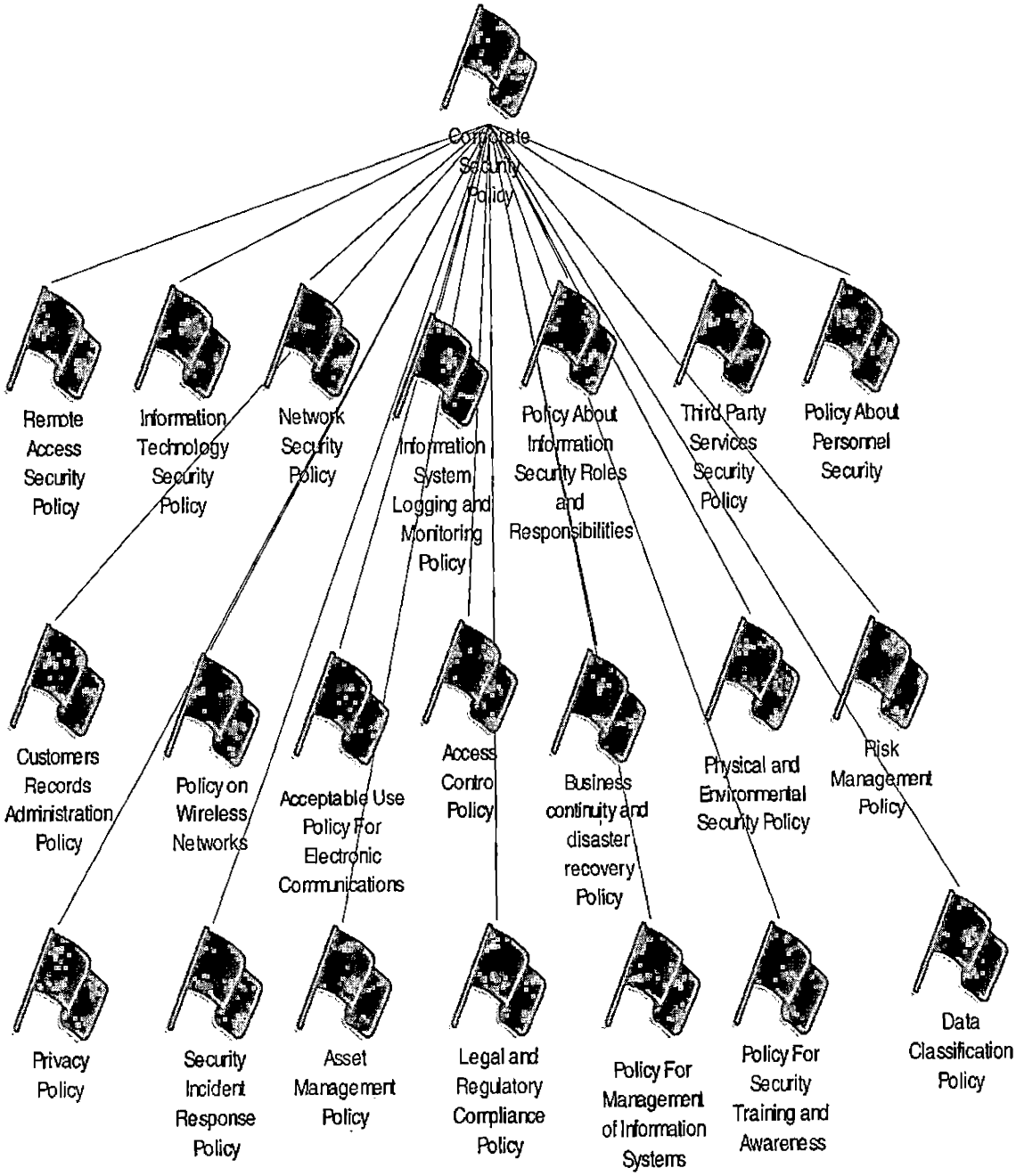
APPENDIX H

SUBSIDIARY EXISTING SECURITY POLICY


Current
Branch
Security
Policy
Policy on
Wireless
Networks
Acceptable Use
Policy For
Electronic
Communications
Customers
Records
Administration
Policy

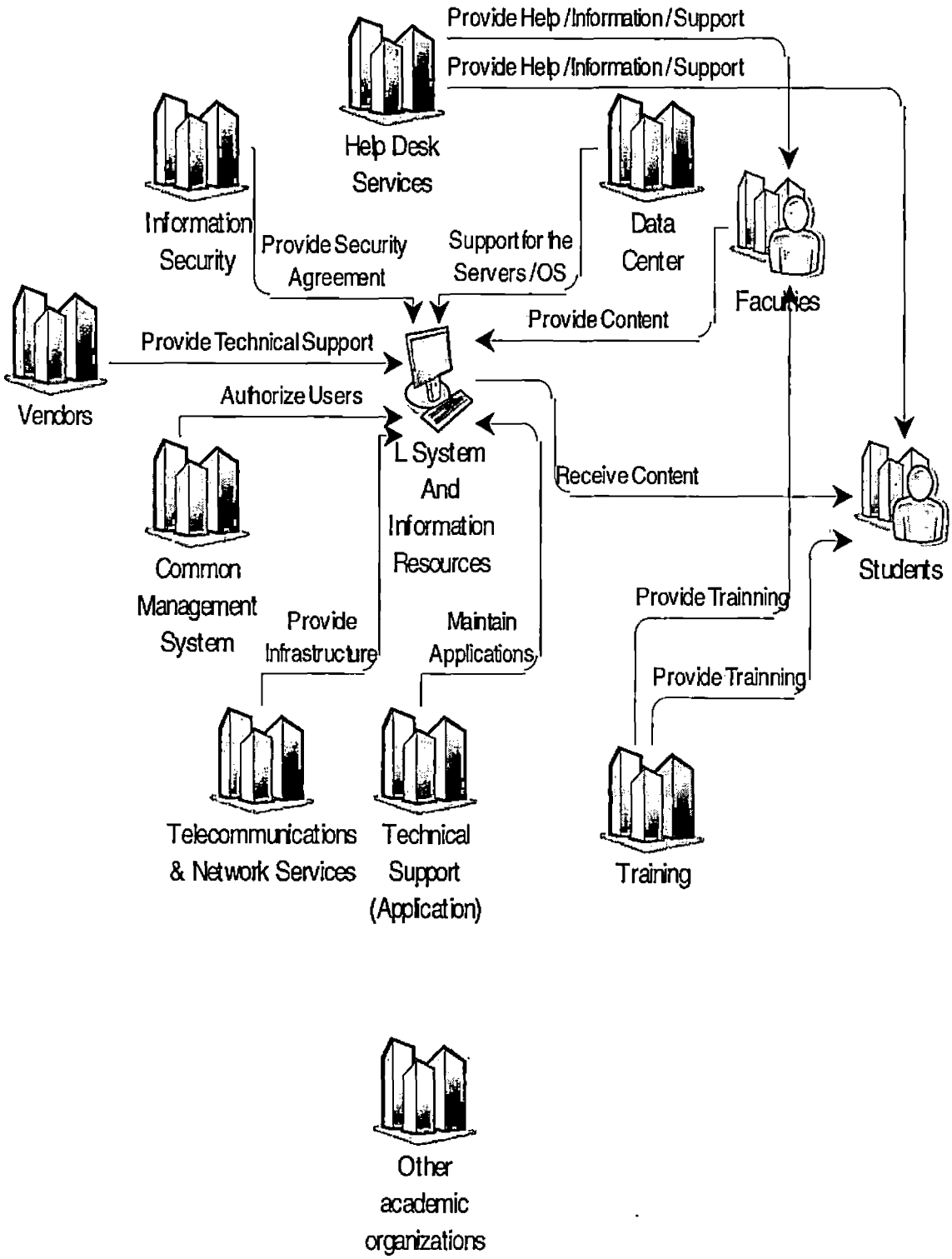
APPENDIX I

CORPORATE SECURITY POLICY


Corporate Security Policy
Remote Access Security Policy
Information Technology Security Policy
Network Security Policy
Information System Logging and Monitoring Policy
Policy About Information Security Roles and Responsibilities
Third Party Services Security Policy
Policy About Personnel Security
Customers Records Administration Policy
Policy on Wireless Networks
Acceptable Use Policy For Electronic Communications
Access Contro Policy
Business continuity and disaster recovery Policy
Physical and Environmental Security Policy
Risk Management Policy
Privacy Policy
Security Incident Response Policy
Asset Management Policy
Legal and Regulatory Compliance Policy
Policy For Management of Information Systems
Policy For Security Training and Awareness
Data Classification Policy

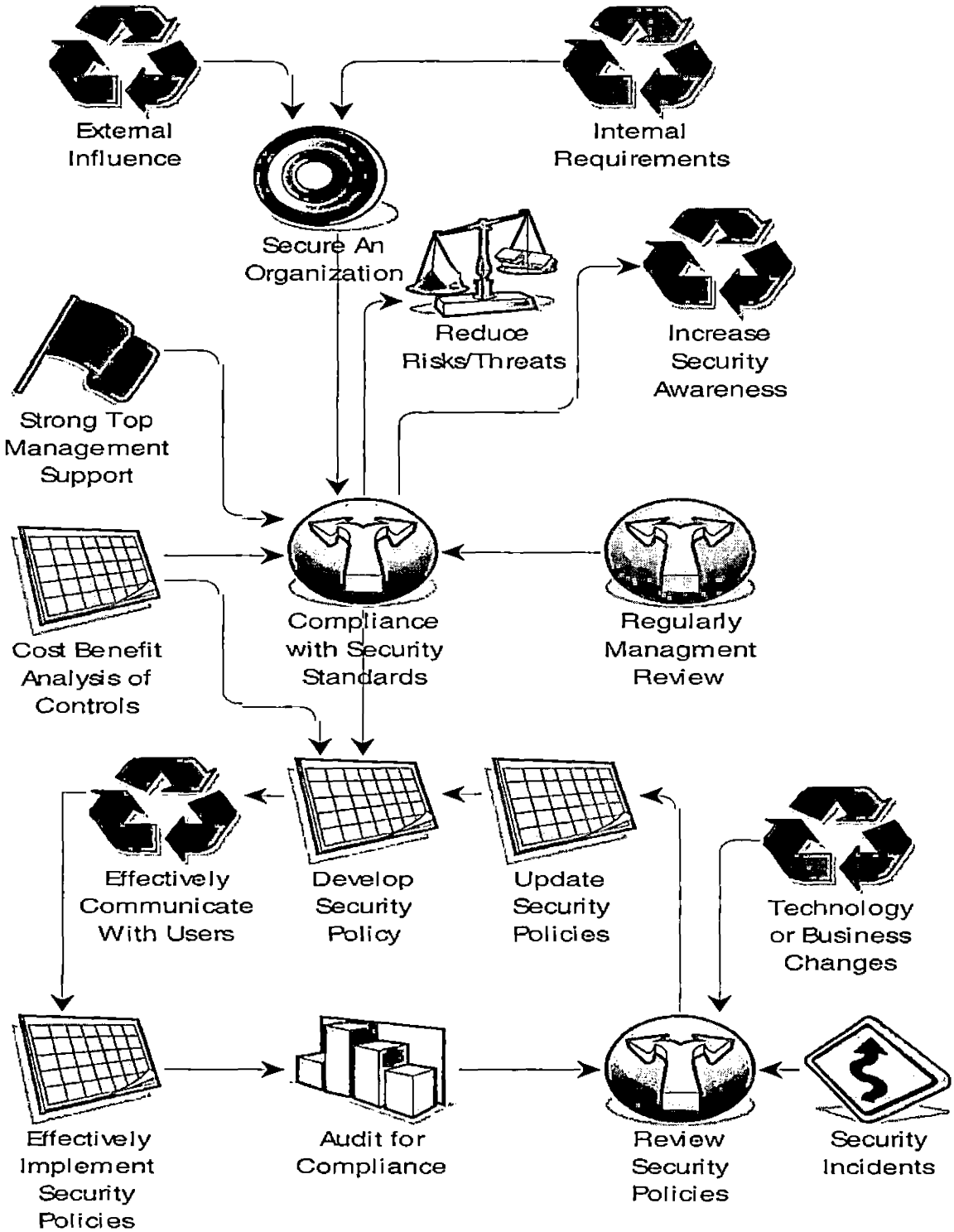
APPENDIX J

THE L SYSTEM - BUSINESS PROCESS


Provide Help /Information / Support
Provide Help /Information / Support
Help Desk Services
Information Security
Provide Security Agreement
Support for the Servers /OS
Data Center
Faculties
Provide Content
Vendors
Provide Technical Support
Authorize Users
L System And Information Resources
Receive Content
Students
Common Management System
Provide Infrastructure
Maintain Applications
Provide Trainning
Provide Trainning
Telecommunications & Network Services
Technical Support (Application)
Training
Other academic organizations

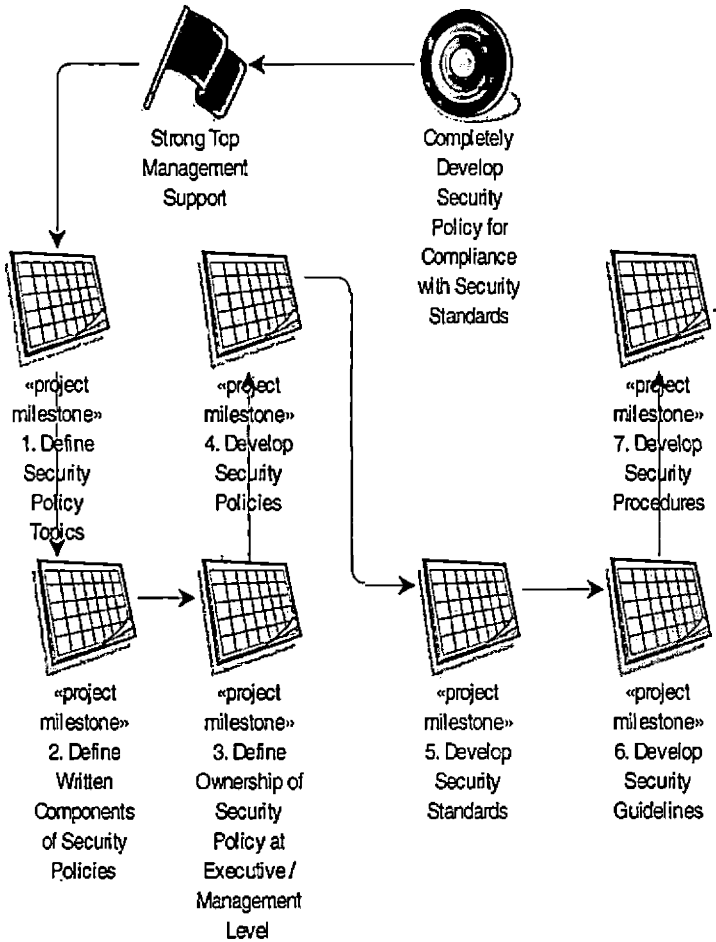
APPENDIX K

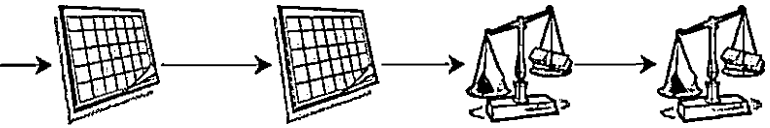
SECURITY FRAMEWORK


External Influence
Internal Requirements
Secure An Organization
Reduce Risks/Threats
Increase Security Awareness
Strong Top Management Support
Cost Benefit Analysis of Controls
Compliance with Security Standards
Regularly Managment Review
Effectively Communicate With Users
Develop Security Policy
Update Security Policies
Technology or Business Changes
Effectively Implement Security Policies
Audit for Compliance
Review Security Policies
Security Incidents

APPENDIX L

DEVELOP SECURITY POLICY


Strong Top Management Support
Completely Develop Security Policy for Compliance with Security Standards
«project milestone» 1. Define Security Policy Topics
«project milestone» 4. Develop Security Policies
«project milestone» 7. Develop Security Procedures
«project milestone» 2. Define Written Components of Security Policies
«project milestone» 3. Define Ownership of Security Policy at Executive / Management Level
«project milestone» 5. Develop Security Standards
«project milestone» 6. Develop Security Guidelines



Feedback From Key Employees and Managers

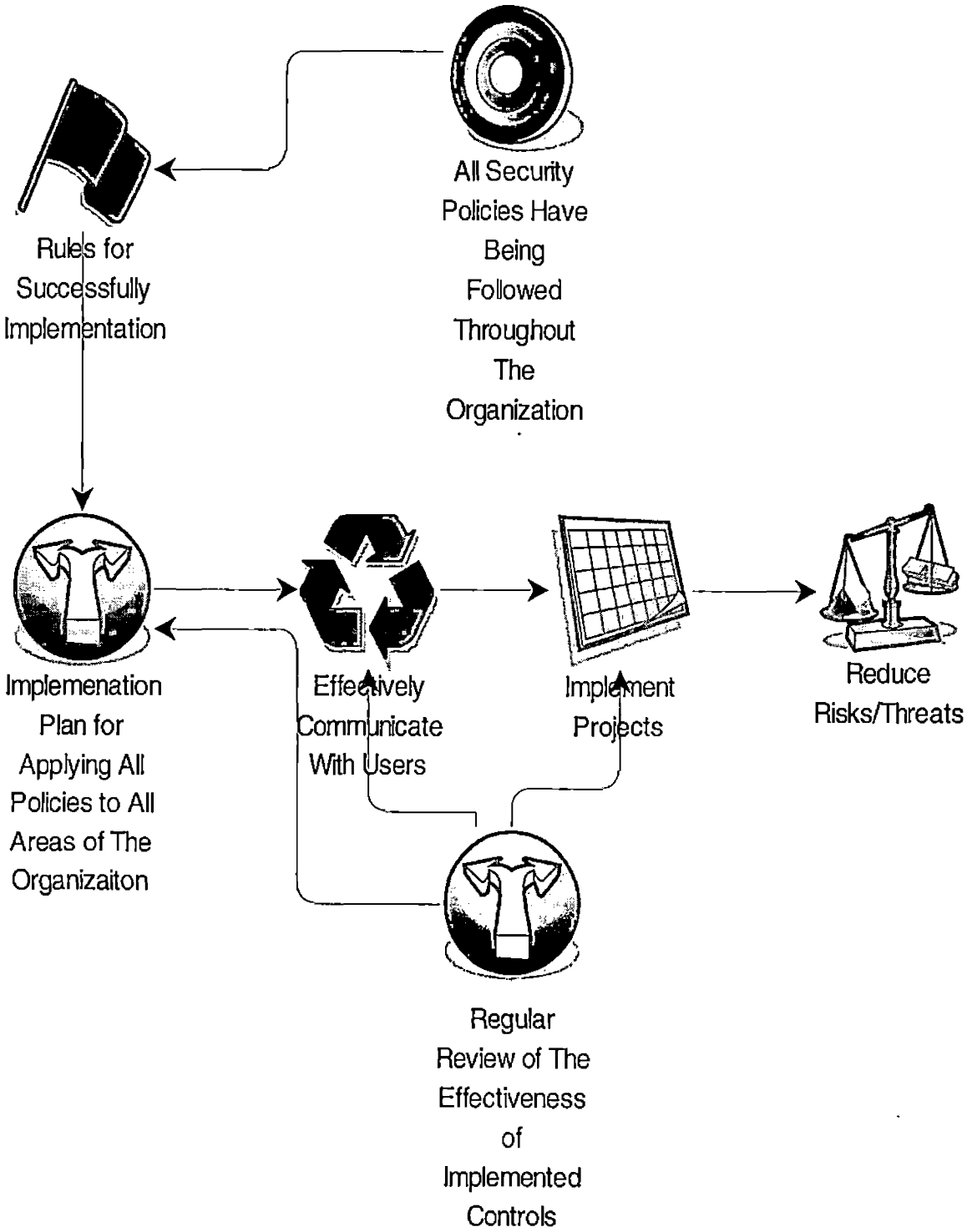
Modify The Entire Security Policy

A Documented Security Policy Is Formally Approved

Distribute Throughout The Organization

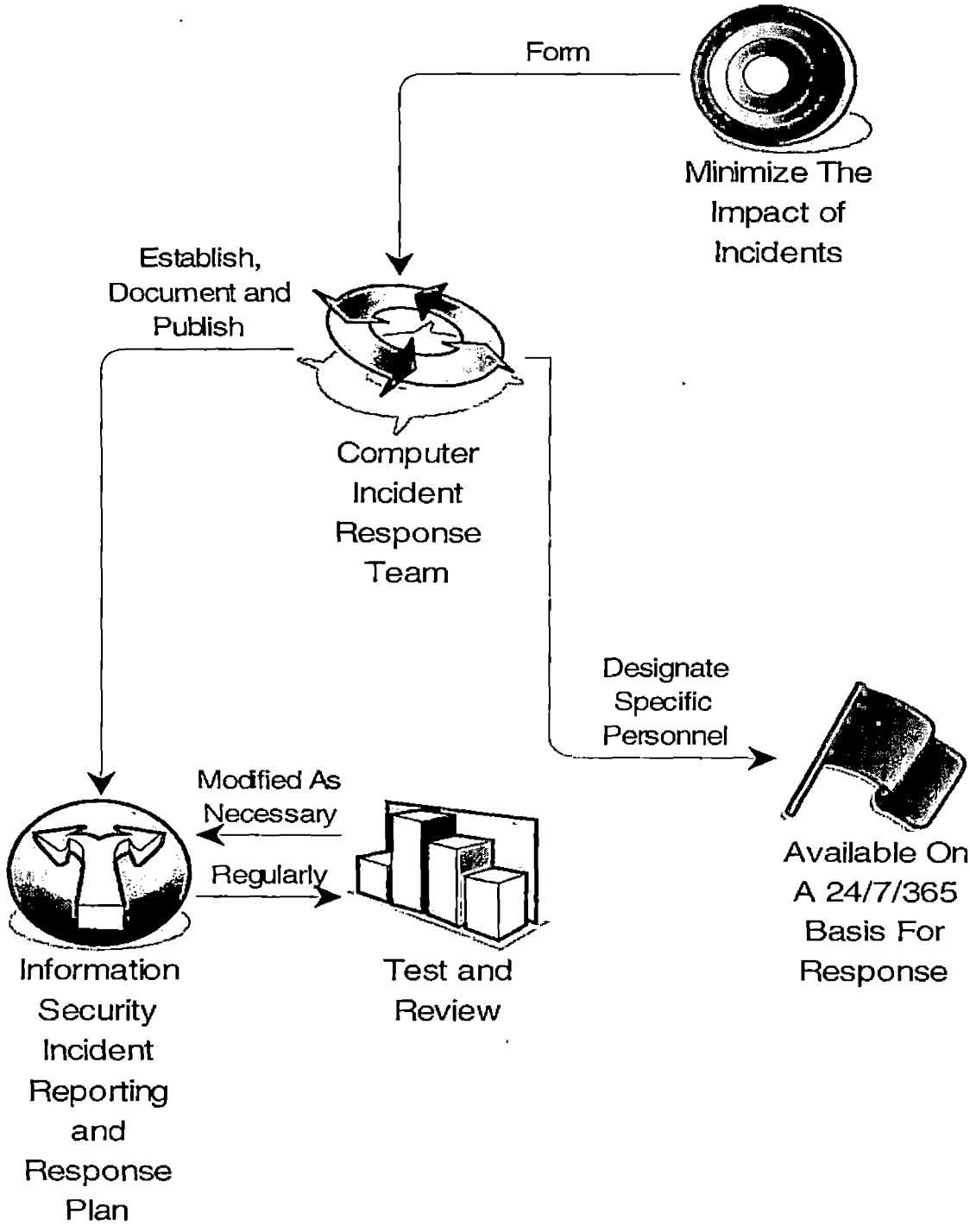
APPENDIX M

EFFECTIVELY IMPLEMENT SECURITY POLICIES


All Security Policies Have Being Followed Throughout The Organization
Rules for Successfully Implementation
Implemenation Plan for Applying All Policies to All Areas of The Organizaiton
Effectively Communicate With Users
Implement Projects
Reduce Risks/Threats
Regular Review of The Effectiveness of Implemented Controls

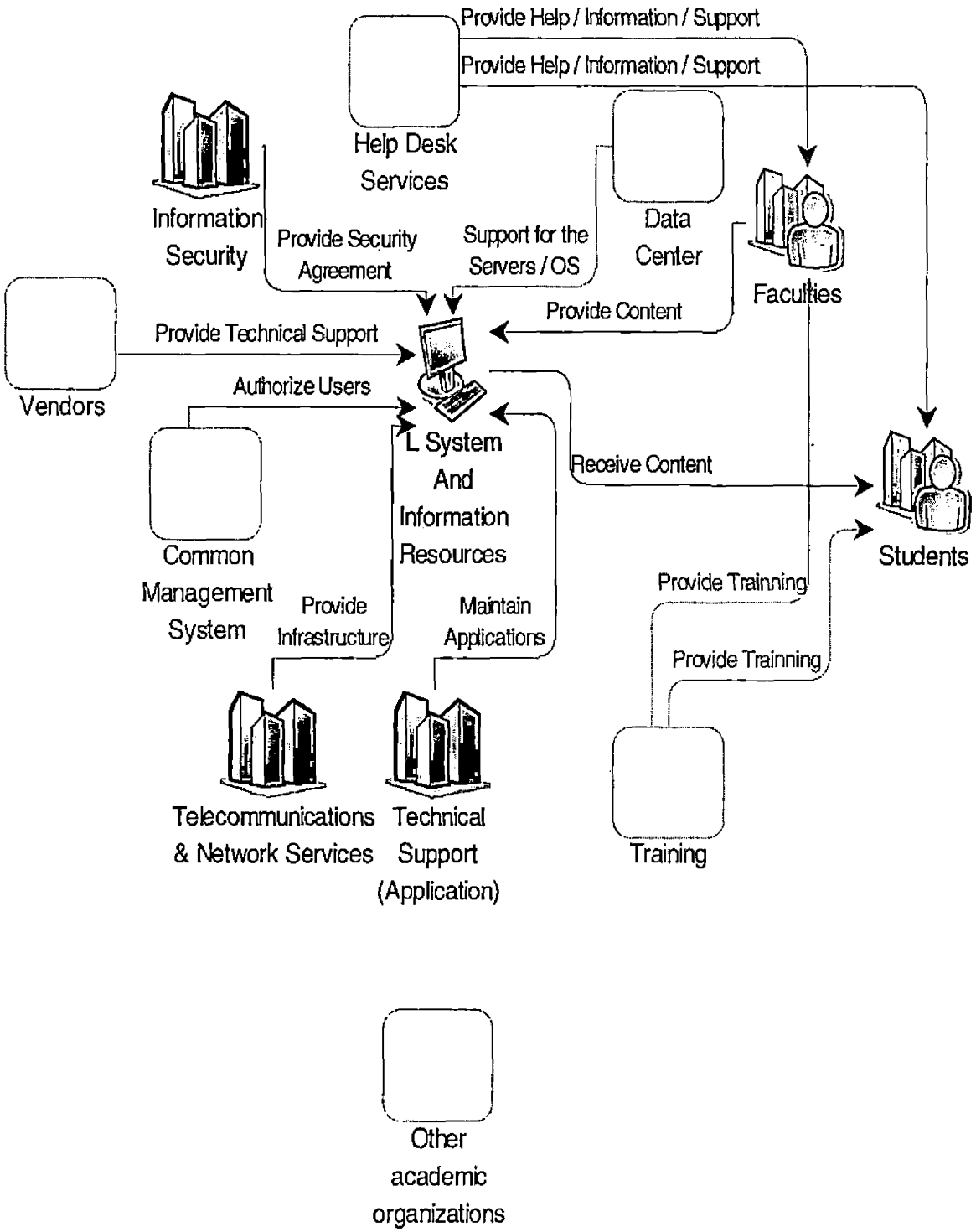
APPENDIX N

STRATEGY FOR SECURITY INCIDENT RESPONSE POLICY


Form
Minimize The Impact of Incidents
Establish, Document and Publish
Computer Incident Response Team
Designate Specific Personnel
Available On A 24/7/365 Basis For Response
Modified As Necessary
Regularly
Information Security Incident Reporting and Response Plan
Test and Review

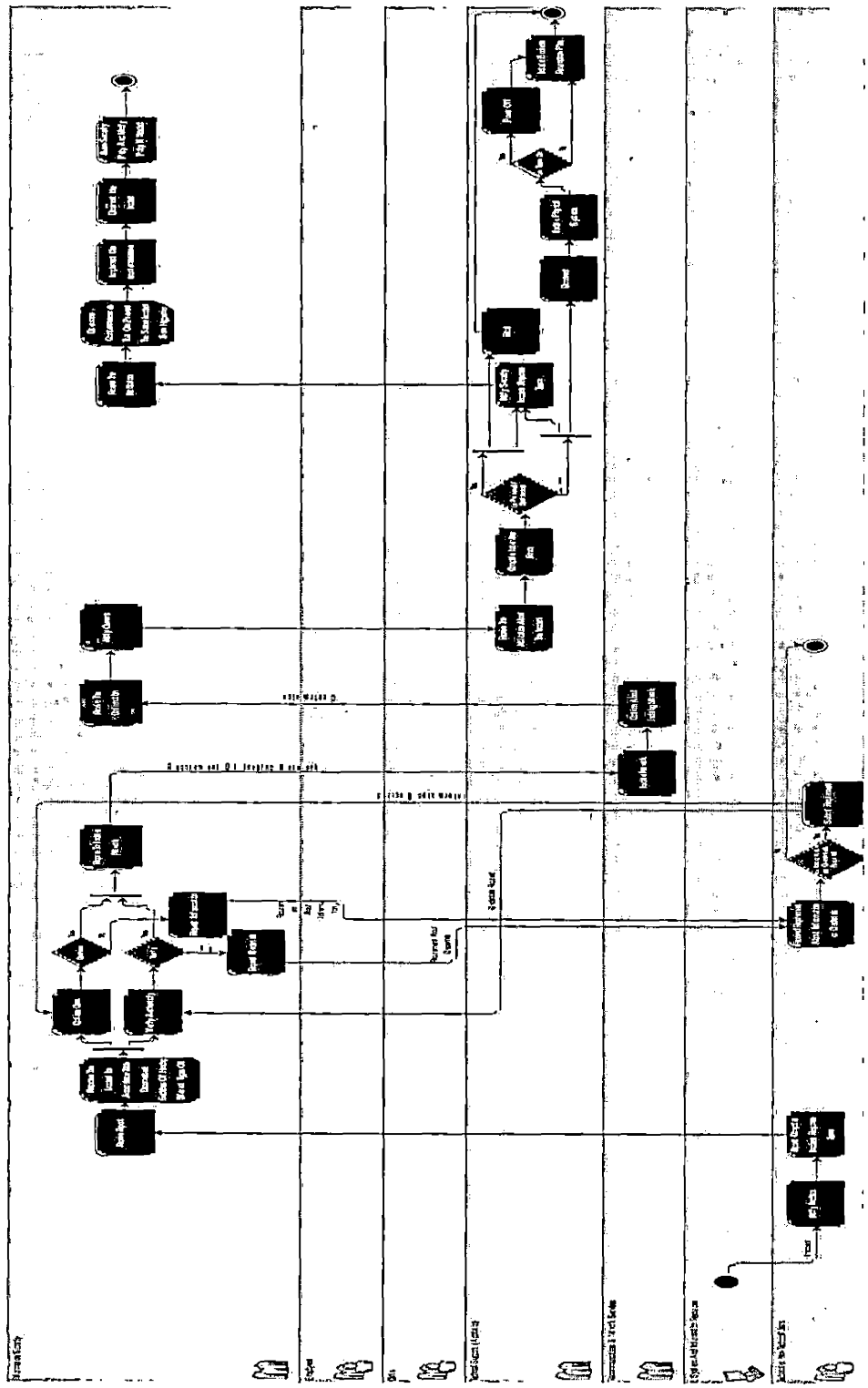
APPENDIX O

SECURITY INCIDENT RESPONSE (L SYSTEM)


Provide Help / Information / Support
Provide Help / Information / Support
Help Desk Services
Information Security
Provide Security Agreement
Support for the Servers / OS
Data Center
Faculties
Provide Content
Vendors
Provide Technical Support
Authorize Users
L System And Information Resources
Receive Content
Students
Common Management System
Provide Infrastructure
Maintain Applications
Provide Trainning
Provide Trainning
Telecommunications & Network Services
Technical Support (Application)
Training
Other academic organizations

APPENDIX P

WORKFLOW OF SECURITY INCIDENT RESPONSE (L SYSTEM)



APPENDIX Q

ESSENTIAL COLLECTION RESOURCES AND COLLECTION APPROACHES

(Carbone, 2004)

Information Needed

- Organizational mission statements and security mission statements
- Organizational goals and security goals
- Organizational structures
- Organizational size in annual revenue, expenses, and number of employees
- List of organizational products and services and quantity sold
- Number and types of organizational customers
- Organizational business units and their objectives
- Flows of organizational processes
- Organizational business strategic plan
- 5 Ws (what, when, who, why, where) and 1 H (how):
  - What do organizations do?
  - When did key essential events or historical changes, which impacted organizations' daily operations, take place? Or when will key essential events, which will affect on the way organizations operate, take place?

- Who are organizations' key customers, suppliers, vendors, partners, government agencies (external interfaces) or potential business sponsors?
- Why do things not turn out right?
- Where (locations) did organizations serve and where are organizations serving?
- How do organizations conduct business (sales channels)?

- Organizational strengths, weaknesses, opportunities, and threats (SWOT), including organizations' stress / risks, challenges, environmental changes, growth/cost containment opportunities
- Organizational key constraints from regulatory, legislative, and shareholder considerations about how to manage organizations
- Organizational major themes, motivational, or cultural forces that impact the behavior of the organization and business direction

- Organizations current IT and security technology, such as enterprise-wide IT and security infrastructures

Essential Collection Resources

- The statement of organizational mission or goals
- Strategic business plans
- Organizational charts for business and IT
- Documentation about major programs of key business units and their objectives
- Security police if in existence
- Annual IT plan if in existence
- IT process flowchart if in existence
- Target function flowchart, target information flowchart, target process requirements, and process descriptions if in existence
- Key reports or indices, such as the annual report, the report of assessment about current organizations, and measurement result reports
- Research and trade publications
- Supplier agreements
- Documentation about execution, operations, tools, and development environments

- This type of resource is useful when establishing current architecture.

- Information source reports / forms / memos, file descriptions, data volume, data location, and existing data architectures and conceptual data models if in existence
  - This type of resource is useful when establishing data architecture.
- Application system and data flow, a report containing security evaluation, the function improvement opportunities, descriptions of current applications, and the findings about user-satisfaction ratings
  - This type of resource is useful when establishing application architecture.
- IT architecture, model, design, infrastructure documentation if in existence
  - This type of resource is useful when establishing technology architecture.

Essential Collection Approaches

- Conducting interviews or surveys with top business managers, key opinion leaders in the

business, and high-ranking IT managers (Carbone, 2004)

- CEO or CIO strongly supports this activity and can efficiently collect sufficient information from interviews or questionnaires.
- Appendix A is an example of a questionnaire coming from Carbone (Carbone, 2004).

- Ongoing feedback from key organizational stakeholders
- Developing target process flows for the current state and the target state
  - Developing teams can simply translate current and future processes into different functions and information flows. The rule of thumb is to keep these diagrams as simple as possible because simple diagrams can give developing teams the ability to easily capture major problems (Carbone, 2004).

REFERENCES

Anderson, E. E. & Choobineh, J. (2008). Enterprise Information Security Strategies. *Computer & Security, In Press*, Corrected Proof, Available online 3 April 2008. Retrieved April 19, 2008, from ScienceDirect database.

Beauchemin, G. & Dansereau G. (2007). *Harmonized Threat and Risk Assessment Methodology*. Retrieved March 03, 2008 from http://www.rcmp-grc.gc.ca/tsb/pubs/tra/tra-1_e.pdf.

Boh, W. F. & Yellin D. (2006). Using Enterprise Architecture Standards in Managing Information Technology. *Journal of Management Information Systems*, 13 (3), 163-207.

Buecker, A., Carreno, A. V., Field N., Hockings C., Kawer, D., Mohanty, S., & Monteiro G. (2004). *Enterprise security architecture using IBM Tivoli security solutions*. NY: IBM Corporation.

Carbone, J. A. (2004). *IT Architecture Toolkit*. NJ: Prentice-Hall PTR.

Carnegie Mellon Software Engineering Institute. *Risk Management*. Retrieved September 04, 2007 from http://www.sei.cmu.edu/risk/index.html.

Cavusoglu, H. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16 (1), 28-46.

Danielyan, E. (2001) *Solaris 8 security*. NY: New Riders Publishing.

Department of Defense. (2006). *Risk Management Guide for DOD Acquisition*. Retrieved November 27, 2007 from http://www.sei.cmu.edu/risk/dod-risk.pdf.

Farrel, R. J. (1996). ProVision (version 6.0.2) [Computer Software]. Metastorm, MD: Baltimore.

Fedor, D. B., Ghosh, S., Caldwell, S. D., Maurer, T. J., & Singhal, V. R. (2003). The Effects of Knowledge Management on Team Members' Ratings of Project Success and Impact. *Decision Sciences*, 34 (3), 513-539. Retrieved April 19, 2008, from ABI/INFORM Global database.

Fumy, W., & Sauerbrey J. (2006). *Enterprise Security: IT Security Solutions: Concepts, Practical Experiences, Technology*. Berlin: Publics Corporate Publishing.

Hansche, S., John B., and Chris H. (2004). *Official (ISC)^2 Guide to the CISSP Exam*. London: Auerbach.

Harris, S. (2005). *All-In-One: CISSP Exam Guide.* California: McGraw-Hill Companies.

IT Governance and the Political Dimension: The Emergence of IT Governance. Retrieved August 16, 2007 from http://itgovernance.politicalinformation.com/.

IT Governance Institute and the Office of Government Commerce. (2005). *Aligning COBIT, ITIL and ISO17799 for Business Benefit: A Management Briefing From ITGI and OGC.* Retrieved October 06, 2007 from http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=22493&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

Jackson, C. M., Chow, S., & Leitch, R. A. (1997). Toward an Understanding of the Behavioral Intentiion to Use an Information System. *Decision Sciences,* 28 (2), 357-389. Retrieved April 19, 2008, from Business Source Premier database.

Kearns, G. S., & Sabherwal, R. (2006). Strategic alignment between business and information technology: a knowledge-based view of behaviors, outcome, and consequences. *Journal of Management Information Systems.* 23 (3), 129-162.

Kent, K., Chevalier S., Grance T., & Dang H. (2006). *Guide to Integrating Forensic Techniques into Incident.* Retrieved October 16, 2007 from http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Killcrece, G., Kossakowski K. P., Ruefle R., & Zajicek M. (2003). *State of the Practice of Computer Security Incident Response Teams (CSIRTs).* Retrieved Novermber 03, 2007 from www.cert.org/archive/pdf/03tr001.pdf.

Lam, W. (2005) Investigating success factors in enterprise application integration: A case-driven analysis. *European Journal of Information* systems, 14(2), 175-187. Retrieved April 21, 2008, from ABI/INFORM Global database.

McGee, A. R., Vasireddy S. R., Xie C., Picklesimer D. D., Chandrashekhar U., & Richman S. H. (2004). A framework for Ensuring Network Security. *Bell Labs Technical Journal*, 8 (4): 7-27.

Martin, N. L., Pearson, M., & Furumo, K. (2007). IS Project Management: Size, Practices and The Project Management Office1,2. *The Journal of computer Information Systems,* 47(4), 52-60.Retrieved April 20, 2008, from ABI/INFORM Global database.

Mealy, M. (2005). *ROI Comparison Paper*. Retrieved May 04, 2007 from http://www.ybsecure.com/downloads/ROI%20Comparison%20paper.pdf.

Meritt, J. W. (1998). *Risk Management*. Retrieved May 16, 2007 from http://csrc.nist.gov/nissc/1998/proceedings/paperE5.pdf.

Poole V. (2006). *A governance framework*. Retrieved October 01, 2007 from http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_195169.

Ross, J. W. (2003). Creating a strategic IT architecture competency: learning in stages. *MIS Quarterly Executive*. 2 (1), 31-43.

The SANS Institute. (n.d.). *The SANS Security Policy Project*. Retrieved January 22, 2008 from http://www.sans.org/resources/policies/.

Sherwood, J. (2005). *Enterprise security architecture: a business-driven approach*. San Francisco: CMP Books.

Spewak, S. H. & Hill, S. C. (1993). *Enterprise architecture planning: developing a blueprint for data, applications, and technology*. New York: Wiley.

Shoniregun, C. A. (2005). *Impact and risk assessment of technology for internet security.* New York: Springer Science+Business Media, Inc.

Stoneburner, G., Goguen1 A., & Feringa A. (2002). *Risk Management Guide for Information Technology Systems.* Retrieved August 24, 2007 from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Tallon, P. P. (2007). A Process-Oriented Perspective on the Alignment of Information Technology and Business Strategy. *Journal of Management Information Systems,* 24 (3), 227-268.

The Information Security Policies & Standards Group. (n.d.) *The Information Security Policies / Computer Security Policies Directory.* Retrieved June 14, 2007 from http://www.information-security-policies-and-standards.com/.

Threat and Risk Assessment Working Guide. Retrieved September 17, 2007 from http://www.cse-cst.gc.ca/en/documents/publications/gov pubs/itsg/itsg04.pdf.

Walker, K. M. & Cavanaugh, L. C. (1998). *Computer Security Policies.* Palo Alto: Sun Microsystems, Inc.

Weise, J. & Martin C. R. (2001). *Developing a Security Policy*. Retrieved January 10, 2008 from http://www.sun.com/blueprints/1201/secpolicy.pdf.

William R. K. (2006) Developing Global IT Capabilities. *Information Systems Management*. 23 (4), 78.

Zachman Framework. Retrieved July 14, 2007 from http://www.zifa.com/.

Zachman, J. A. (1987). A Framework for Information Systems Architecture. IBM Systems Journal. 26 (3) : 276-292